M진 Sidel'nikov 수열의 서로 다른 자기 상관 분포의 개수

정회원 정 정 수*, 김 영 식**, 종신회원 노 종 선*, 정 하 봉***

On the Number of Distinct Autocorrelation Distributions of M-ary Sidel'nikov Sequences

Jung-Soo Chung*, Young-Sik Kim** ***Regular Members***
Jong-Seon No*, Ha-Bong Chung*** ***Lifelong Members***

요 약

이 논문에서는 M진 Sidel'nikov 수열을 생성하는 원시원을 바꾸었을 때, 생성된 수열의 서로 다른 자기 상관 분포의 개수를 계산한다. p는 소수이고 M은 p^n-1의 약수일 때 M진 Sidel'nikov 수열의 서로 다른 자기 상관 분포는 $M=2$일 때, 유일하다. M은 2보다 크고 어떤 $k(1\le k<n)$에 대해서 p^k+1의 약수일 때, M진 Sidel'nikov 수열의 자기 상관 분포는 1개이다. M은 2보다 크고 어떤 $k(1\le k<n)$에 대해서 p^k+1의 약수가 아닐 때, 서로 다른 자기 상관 분포의 개수는 $\phi(M)/k'$(혹은 $\phi(M)/2k'$)보다 작거나 같다. 여기서 k'는 $M|p^{k'}-1$를 만족하는 가장 작은 정수이다.

Key Words : Autocorrelation, Autocorrelation Distributions, Cyclotomic Number, M-ary Sequences, Sidel'nikov Sequences

ABSTRACT

In this paper, we enumerate the number of distinct autocorrelation distributions that M-ary Sidel'nikov sequences can have, while we change the primitive element for generating the sequence. Let p be a prime and $M|p^n-1$. For $M=2$, there is a unique autocorrelation distribution. If $M>2$ and $M|p^k+1$ for some k, $1\le k<n$, then the autocorrelation distribution of M-ary Sidel'nikov sequences is unique. If $M>2$ and $M\nmid p^k+1$ for any k, $1\le k<n$, then the autocorrelation distribution of M-ary Sidel'nikov sequences is less than or equal to $\phi(M)/k'$(or $\phi(M)/2k'$), where k' is the smallest integer satisfying $M|p^{k'}-1$.

Ⅰ. 서 론

$M|p^n-1$를 만족하는 소수 p, 양의 정수 M, n에 대해서, Sidel'nikov는 주기가 p^n-1인 M진 수열(Sidel'nikov 수열이라 부름)을 제안하였다[1]. 이 수열의 자기 상관 값은 위상이 맞지 않을 경우 상한 값이 4이다. 최근, Kim, Chung, No, 그리고 Chung는 위수 M인 원분의 수(cyclotomic number)를 이용해서 M진 Sidel'nikov sequence의 자기 상관 분포를 유도하였고 서로 다른 자기 상관 값의 최대

※ 본 연구는 교육인적자원부, 산업자원부, 노동부의 출연금으로 수행한 최우수실험실지원사업의 연구결과입니다.
* 서울대학교 전기·컴퓨터공학부 및 뉴미디어통신공동연구소(integer@ccl.snu.ac.kr, jsno@snu.ac.kr)
** 삼성전자(kingsi@ccl.snu.ac.kr), *** 홍익대학교 전자전기공학부(habchung@hongik.ac.kr)
논문번호 : KICS2007-06-252, 접수일자 : 2007년 6월 9일, 최종논문접수일자 : 2007년 10월 2일

개수는 M과 수열의 주기와 관련 있다고 언급하였다[4]. 이 때, 최대 개수는 $\binom{M}{2}+1$보다 작거나 같다.

일반적으로 주기가 p^n-1인 수열을 생성하는데 사용하는 원시원(primitive element)이 다르면 각각의 M진 Sidel'nikov 수열도 서로 다르다. 논문에서는 두 M진 Sidel'nikov 수열의 관계를 살펴보고, 서로 다른 원시원으로 생성된 M진 Sidel'nikov 수열의 서로 다른 자기 상관 분포의 개수를 계산한다.

Ⅱ. 배경지식

주기가 N인 M진 수열 $s(t)$에 대해서, 자기 상관 함수 $R(\tau)$는 다음과 같이 정의된다.

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

여기서 $\omega_M=e^{j2\pi/M}$이다.

정의 1. [1] p를 소수라고 하고 α는 유한체(finite field) F_{p^n}의 원시원이라고 하자. M은 p^n-1의 약수이며 2보다 큰 수이다. F_{p^n}의 공통 원소를 가지지 않는 부분 집합(disjoint subsets)을 S_k, $k=0,1,\cdots,M-1$, 라 하고 다음과 같이 정의한다.

$$S_k=\left\{\alpha^{Mi+k}-1 \mid 0\le i<\frac{p^n-1}{M}\right\} \tag{2}$$

주기가 p^n-1인 M진 Sidel'nikov 수열은 다음과 같이 정의한다.

$$s(t)=\begin{cases}k, & \text{if } \alpha^t\in S_k,\ 0\le k\le M-1\\ k_0, & \text{if } \alpha^t=-1\end{cases} \tag{3}$$

여기서 $0\le k_0\le M-1$이다.

식 (3)에서 M진 Sidel'nikov 수열 $s(t)$는 유한체 F_{p^n}상에서 위수(order)가 M인 multiplicative character $\psi_M(\cdot)$와 지시 함수 $I(\cdot)$로 표현할 수 있다.

$$\omega_M^{s(t)}=\omega_M^{k_0}I(\alpha^t+1)+\psi_M(\alpha^t+1). \tag{4}$$

여기서 지시 함수는 다음과 같다.

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

Multiplicative character ψ_M은 $\psi_M(\alpha^t)=e^{j2\pi t/M}$이고 $\psi_M(0)=0$이다.

[4]에서 M진 Sidel'nikov 수열의 자기 상관 분포를 위수가 M인 원분의 수로 표현하였다. 원분의 수는 다음과 같이 정의된다.

정의 2. [6] α는 유한체 F_{p^n}의 원시원이라 하고, p^n-1의 약수이며 2보다 큰 M을 생각하자. 원분의 집합(cyclotomic classes) C_u, $0\le u\le M-1$는 다음과 같이 정의된다.

$$C_u=\left\{\alpha^{Ml+u} \mid 0\le l<\frac{p^n-1}{M}\right\}$$

고정된 양수 u,v에 대해서, 원분의 수 $(u,v)_M$은 $1+z_u\in C_v$를 만족하는 $z_u\in C_u$의 개수를 의미한다. □

논문에서 사용하는 원분의 수의 유용한 성질은 다음과 같다.

보조 정리 3. [6]

1) 임의의 l_1와 l_2에 대해서
$(i+Ml_1,j+Ml_2)_M=(i,j)_M$
2) $(i,j)_M=(M-i,j-i)_M$
3) $(i,j)_M=(\pi,pj)_M$
4)
$$(i,j)_M=\begin{cases}(j,i)_M, & \text{if } \frac{p^n-1}{M} \text{ is even}\\ & \text{or } p=2\\ (j+\frac{M}{2},i+\frac{M}{2})_M, & \text{if } \frac{p^n-1}{M} \text{ is odd}\end{cases}$$
5) $(i,j)_{M'}=\sum_{t=0}^{m-1}\sum_{s=0}^{m-1}(i+tM',j+sM')_M$, for $M=mM'$. □

Baumert와 Mills, Ward는 F_{p^n}에서 위수 M의 원분의 수가 일정함을 다음과 같이 보였다.

정리 4. [7] p는 소수, $q=p^{2ms}$라 하고 M은 p^s+1의 약수라고 하자. 이 때 $M\ge 3$이어야 한다. 그러면 F_q 상의 위수가 M인 원분의 수는 항상 일정하고 다음과 같다.

$(0,0)=\eta^2-(M-3)\eta-1$
$(0,i)=(i,0)=(i,i)=\eta^2+\eta, \quad \text{for} \quad i\neq 0$
$(i,j)=\eta^2, \quad \text{otherwise}$
여기서

$$\eta=\begin{cases}(\sqrt{q}-1)/M, & \text{if } m \text{ is even}\\ (-\sqrt{q}-1)/M, & \text{if } m \text{ is odd.}\end{cases}$$

Ⅲ. Sidel'nikov 수열의 서로 다른 자기 상관 분포의 개수

이번 장에서는, 수열을 생성하는 원시원을 변경한 M진 Sidel'nikov 수열 $s^{(c)}(t)$의 서로 다른 자기 상관 분포의 개수를 유도한다. 이 때, c는 주기와 서로 소이다.

정의 1로부터 수열을 생성하는 원시원을 바꾸면, M진 Sidel'nikov 수열은 달라진다. 원시원 α를 $\beta(=\alpha^c)$로 바꾸었을 때, $S_k^{(c)}$는 식 (2)와 같이 정의되는 공통 원소를 가지지 않는 부분 집합이고 $s^{(c)}(t)$는 식 (3)에서의 수열이다. 명백하게, $S_k^{(c)}=S_{ck}$이다. 다음 보조 정리는 $s(t)$와 $s^{(c)}(t)$사이의 관계를 보여 준다.

보조 정리 5. [10]

$$s^{(c)}(t)\equiv\begin{cases}s(ct)=k_0, & \text{if } \alpha^{ct}=-1\\ c^{-1}s(ct), & \text{otherwise}\end{cases}$$

여기서 c와 p^n-1은 서로 소이다. □

보조 정리 5로부터, $s^{(c)}(t)$의 자기 상관 함수인 $R_c(\tau)$는 [4]에서 유도한 것처럼, $s(t)$의 자기 상관 함수인 $R(\tau)$와 비슷하게 구할 수 있다.

정리 6. [10] $s^{(c)}(t)$의 자기 상관 함수인 $R_c(\tau)$ (이 때,$\tau\neq 0 \bmod p^n-1$라 가정한다.)는 다음과 같다.

$$R_c(\tau)=\omega_M^{k_0}\overline{\psi_M^{c^{-1}}}(1-\alpha^{c\tau})+\omega_M^{-k_0}\psi_M^{c^{-1}}(1-\alpha^{-c\tau})-\psi_M^{c^{-1}}(\alpha^{-c\tau})-1$$

여기서 $\overline{\psi_M}$은 ψ_M의 복소 공액이다.

□

[4],[10]의 결과를 이용하면, $R_c(\tau)$는 다음과 같다.
$\psi_M(-1)=1$이거나 $(p^n-1)/M$이 짝수일 때,

$$R_{i,j}=-(\omega_M^i-1)(\omega_M^j-1) \tag{5}$$

이고,
$\psi_M(-1)=-1$이거나 $(p^n-1)/M$이 홀수일 때,

$$Q_{i,j}=(\omega_M^i+1)(\omega_M^j+1)-2 \tag{6}$$

이다.

$s^{(c)}(t)$의 자기 상관 분포는 $s(t)$의 자기 상관 분포의 일반화로 생각할 수 있다.

정리 7. [10] $N_c(R_{i,j})$와 $N_c(Q_{i,j})$는 각각 $R_c(\tau)=R_{i,j}$이고 $R_c(\tau)=Q_{i,j}$를 만족하는 개수이다. (여기서 $\tau\neq 0 \bmod p^n-1$) 그러면 M진 Sidel'nikov 수열 $s^{(c)}(t)$의 위상이 일치하지 않는 자기 상관 분포는 다음과 같다.

Case 1. $\psi_M(-1)=1$;

1) $N_c(0)=\sum_{i=1}^{M-1}\{(ci,ci+ck_0)_M+(ci,ck_0)_M\}+(0,ck_0)_M$
2) $N_c(R_{i,i})=(2ci,ci+ck_0)_M,\ 1\le i\le M-1$
3) $N_c(R_{i,j})=(ci+cj,ci+ck_0)_M+(ci+cj,cj+ck_0)_M,\ 1\le i<j\le M-1$

Case 2. $\psi_M(-1)=-1$;

1) $N_c(-2)=\sum_{i=0,i\neq\frac{M}{2}}^{M-1}\{(\frac{Mc}{2}+ci,ci+ck_0)_M+(\frac{Mc}{2}+ci,\frac{Mc}{2}+ck_0)_M\}+(0,\frac{Mc}{2}+ck_0)_M$
2) $N_c(Q_{i,i})=(2ci,ci+ck_0)_M,\ 0\le i\le M-1 \text{ and } i\neq\frac{M}{2}$
3) $N_c(Q_{i,j})=(ci+cj,ci+ck_0)_M+(ci+cj,cj+ck_0)_M,\ 0\le i<j\le M-1, i\neq\frac{M}{2}, \text{ and } j\neq\frac{M}{2}$

□

위의 정리를 이용하여, 다음 정리는 Sidel'nikov 수열의 서로 다른 자기 상관 분포의 개수를 구하는 것을 보여준다.

정리 8. p는 소수이고 M은 p^n-1의 약수이다. ψ_M은 F_{p^n}의 nontrivial multiplicative character이다. 주기 p^n-1과 c가 서로 소일 때, M진 Sidel'nikov 수열 $s^{(c)}(t)$의 서로 다른 자기 상관 분포는 다음과 같다.

Case 1) $M=2$일 때, 자기 상관 분포는 유일하다.

Case 2) M은 2보다 크고 어떤 $k(1 \le k < n)$에 대해서 p^k+1의 약수일 때, M진 Sidel'nikov 수열의 자기 상관 분포는 1개이다.

Case 3) M은 2보다 크고 어떤 $k(1 \le k < n)$에 대해서 p^k+1의 약수가 아닐 때, 서로 다른 자기 상관 분포의 개수는 k_0가 0, $M/2$가 아닌 경우 $\phi(M)/k'$보다 작거나 같다. k_0가 0또는 $M/2$인 경우 $\phi(M)/2k'$보다 작거나 같다. 여기서 k'는 $M|p^{k'}-1$를 만족하는 가장 작은 정수이다.

증명)

Case 1) $M=2$인 경우, 주기와 서로 소인 임의의 c는 홀수이다. $s^{(c)}(t)$는 $s(t)$의 c-decimation이다. 주기와 서로 소인 상수에 의해 decimation된 수열은 같은 자기 상관 분포를 가지기 때문에, 자기 상관 분포는 유일하다.

Case 2) 이 경우, n은 짝수이고 k는 $n/2$의 약수이다. $\frac{p^n-1}{M}$이 짝수이므로 $\psi_M(-1)=1$이다. 정리 4와 7을 이용하면 다음을 얻을 수 있다.

(1) $k_0=0$인 경우

$$N_c(0)=(2M-1)\eta^2+(M+1)\eta-1$$

$$N_c(R_{i,i})=\begin{cases}\eta^2+\eta, & \text{if } i=M/2\\ \eta^2, & \text{otherwise}\end{cases}$$

$$N_c(R_{i,j})=\begin{cases}2(\eta^2+\eta), & \text{if } i+j=M\\ 2\eta^2, & \text{otherwise.}\end{cases}$$

(2) $k_0=M/2$인 경우

$$N_c(0)=(2M-1)\eta^2+3\eta$$

$$N_c(R_{i,i})=\begin{cases}\eta^2-(M-3)\eta-1, & \text{if } i=M/2\\ \eta^2, & \text{otherwise}\end{cases}$$

$$N_c(R_{i,j})=\begin{cases}2(\eta^2+\eta), & \text{if } i+j=M \text{ or } \ddot{y}\\ & i=\frac{M}{2} \text{ or } j=\frac{M}{2}\\ 2\eta^2, & \text{otherwise.}\end{cases}$$

(3) $k_0 \neq 0$ 이고 $k_0 \neq M/2$인 경우

$$N_c(0)=(2M-1)\eta^2+3\eta$$

$$N_c(R_{i,i})=\begin{cases}\eta^2+\eta, & \text{if } i=k_0,-k_0,M/2\\ \eta^2, & \text{otherwise}\end{cases}$$

$$N_c(R_{i,j})=\begin{cases}2\eta^2-(M-4)\eta-1, & \text{if } i+j=M\\ & \text{and } i=\pm k_0\\ 2(\eta^2+\eta), & \text{if } i+j=M\\ & \text{and } i\neq\pm k_0\\ 2\eta^2+\eta, & \text{if } i+j\neq M\\ & \text{and } i=\pm k_0\\ & (\text{or } j=\pm k_0)\\ 2\eta^2, & \text{otherwise}\end{cases}$$

여기서,

$$\eta=\begin{cases}\frac{\sqrt{p^n}-1}{M}, & \text{if } \frac{n}{2k} \text{ is even}\\ \frac{-\sqrt{p^n}-1}{M}, & \text{if } \frac{n}{2k} \text{ is odd.}\end{cases}$$

위의 결과로부터, 자기 상관 분포가 c와 독립적임을 알 수 있다. 따라서 자기 상관 분포는 유일하다.

Case 3) 서로 다른 자기 상관 분포의 개수를 계산하는 것은 $\gcd(c,p^n-1)=1$의 조건을 만족하는 c의 개수를 계산하는 것과 관련이 있다. c가 변할 때, 주어진 $R_{i,j}$에 대해서 $N_c(R_{i,j})$ 값이 변한다. 이 변하는 값을 계산하면 자기 상관 분포

표 1. 5진 Sidel'nikov 수열의 자기 상관 분포

	$R(\tau)$의 발생횟수									
$R(\tau)$	$k_0=0$		$k_0=1,4$				$k_0=2,3$			
1330	1	1	1	1	1	1	1	1	1	1
$\omega^4-2\omega^2+1$	54	55	55	54	55	54	60	49	42	54
$-2\omega^3+\omega+1$	54	55	55	54	55	54	60	49	42	54
$-\omega^3-\omega^2+2$	103	102	91	96	114	109	102	114	120	109
$-\omega^4-\omega^3+\omega^2+1$	108	110	108	115	103	97	109	114	104	96
$\omega^3-\omega^2-\omega+1$	108	110	108	115	103	97	109	114	104	96
$-\omega^4-\omega^2+\omega+1$	110	108	114	104	96	109	97	108	115	103
$\omega^4-\omega^3-\omega+1$	110	108	114	104	96	109	97	108	115	103
$\omega^2-2\omega+1$	55	54	49	42	54	60	54	55	54	55
$-2\omega^4+\omega^3+1$	55	54	49	42	54	60	54	55	54	55
$-\omega^4-\omega+2$	102	103	114	120	109	102	109	91	96	114
0	470	470	472	483	490	478	478	472	483	490

의 개수를 계산할 수 있다. 정리 7에서는 위수 M인 원분의 수로 $N_c(R_{i,j})$를 나타낼 수 있다. p^n-1와 c가 서로 소라는 것은 M과 c가 서로 소라는 것을 의미하기 때문에, 서로 다른 자기 상관 분포의 개수의 최대값은 $\phi(M)$을 넘지 않을 것이다.

Euler의 정리는 다음과 같다.

$p^{\phi(M)} \equiv 1 \mod M$

k'은 $M|p^{k'}-1$을 만족하는 가장 작은 정수라고 하면, $k'|\phi(M)$이다. $c, cp, cp^2, cp^3, \cdots, cp^{k'-1}$는 M으로 나눈 나머지가 서로 다르다. 보조 정리 3으로부터, 다음을 알 수 있다.

$(cs, ct)_M = (cps, cpt)_M = \cdots = (cp^{k'-1}s, cp^{k'-1}t)_M$

그러므로, 자기 상관 분포의 개수는 $\phi(M)/k'$보다 작거나 같다.

보조 정리 3의 2)에서 임의의 c와 c'이 $c+c'=M$일 때,

$(2ci, ci+ck_0)_M = (2c'i, c'i-c'k_0)_M$

이고

$(c(i+j), c(i+k_0))_M + (c(i+j), c(j+k_0))_M$
$= (c'(i+j), c'(i-k_0))_M + (c'(i+j), c'(j-k_0))_M$

이다.

그러므로, k_0가 0 또는 $M/2$이면, $N_c(R_{i,j}) = N_{c'}(R_{i,j})$이다. $c' \notin \{c, cp, \cdots, cp^{k'-1}\}$는 사실로부터, 서로 다른 자기 상관 분포의 개수의 최대값은 $\phi(M)/2k'$이다. □

M, p, n의 다양한 값에 대해서 수치적 분석을 통해, Case 3)에서 $M=8$, $p \equiv 1 (\mathrm{mod}\, 8)$이고 $k_0 = 0, 4$인 경우는 자기 상관 분포의 개수는 1이지만, 이외의 경우는 자기 상관 분포의 개수는 주어진 상한 값과 같다.

다음 예제는, M진 Sidel'nikov 수열의 서로 다른 자기 상관 분포의 개수가 k_0의 값에 따라 변함을 보여준다.

예제 9. 주기 N을 1330(11^3-1)이라 하고 M을 5라 하자. 5진 Sidel'nikov 수열의 자기 상관 분포는 표 1과 같다.

Ⅳ. 결 론

이 논문에서는 M진 Sidel'nikov 수열을 생성하는 원시원을 바꾸었을 때, 생성된 수열의 서로 다른 자기 상관 분포의 개수를 계산하였다.

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〕 A. Lempel, M. Cohn, and W. L. Eastman, "A class of balanced binary sequences with optimal autocorrelation properties," IEEE Trans. Inform. Theory, vol. 23, no. 1, pp. 38 – 42, Jan. 1977.

〔3〕 T. Helleseth, S.-H. Kim, and J.-S. No, "Linear complexity over F_p and trace representation of Lempel-Cohn-Eastman sequences," IEEE Trans. Inform. Theory, vol. 49, no. 6, pp. 1548 – 1552, June 2003.

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

〔5〕 R. Lidl and H. Niederreiter, Finite Fields, vol. 20 of Encyclopedia of Mathematics and Its Applications Reading, MA: Addison-Wesley, 1983.

〔6〕 T. Storer, Cyclotomy and Difference Sets, Lectures in Advanced Mathematics Chicago, IL: Markham, 1967.

〔7〕 L.D. Baumert, W.H. Mills, and R.L. Ward, "Uniform cyclotomy," J. Number Theory, vol. 14, pp. 67 – 82, 1982.

〔8〕 L. E. Dickson, "Cyclotomy, higher congruences, and Waring's problem," Amer. J. Math., vol. 57, pp. 391 – 424, 1935.

〔9〕 R. J. McEliece and H. C. Rumsey, "Euler products, cyclotomy, and coding," J. Number Theory, vol. 4, pp. 302 – 311, 1972.

〔10〕 Tae-Hyung Lim, Young-Sik Kim, Jung-Soo Chung, Jong-Seon No, and Habong Chung, "On the relationship of Sidel'nikov sequences," ISITA 2006(International Symposium on Information Theory and its Applications, Seoul, Korea), Oct. 29 - Nov. 1, 2006, pp. 934-937.

정 정 수 (Jung-Soo Chung) 정회원

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

김 영 식 (Young-Sik Kim) 정회원

2001년 2월 서울대학교 전기공학부 공학사
2003년 2월 서울대학교 전기컴퓨터공학부 석사
2007년 2월 서울대학교 전기컴퓨터공학부 박사
2007년 3월~현재 삼성전자
<관심분야> 시퀀스, 오류정정부호, 디지털통신

노 종 선 (Jong-Seon No) 종신회원

1981년 2월 서울대학교 전자공학과 공학사
1984년 2월 서울대학교 대학원 전자공학과 석사
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 전기컴퓨터공학부 교수
<관심분야> 시퀀스, 시공간부호, LDPC 부호, OFDM, 이동통신, 암호학

정 하 봉 (Ha-Bong Chung) 종신회원

1981년 2월 서울대학교 전자공학과 졸업 공학학사
1985년 미국 University of Southern California, 전기공학과 공학석사
1988년 미국 University of Southern California, 전기공학과 공학박사
1988년~1991년 미국 뉴욕주립대 전기공학과 조교수
1991년~현재 홍익대학교 전자전기공학부 교수
<관심분야> 부호 이론, 조합수학, 시퀀스 설계