On the 3-Ranks and Characteristic Polynomials of HKM and Lin Difference Sets

Jong-Seon No*, Dong-Joon Shin** *Regular Members*

ABSTRACT

In this paper, the p-ranks and characteristic polynomials of cyclic difference sets are derived by expanding the trace expression of their characteristic sequences. By using this method, it is shown that the 3-ranks and characteristic polynomials of Helleseth-Kumar-Martinsen (HKM) difference set and Lin difference set can be easily obtained.

Ⅰ. Introduction

It is well-known that a cyclic difference set with Singer parameter $(2^n-1, 2^{n-1}-1, 2^{n-2}-1)$ [2], [3] is equivalent to the binary sequences of period 2^n-1 with ideal autocorrelation property [4], [5], [9], [10], [11]. Recently, nonbinary sequences with ideal autocorrelation property have been investigated and some research results are introduced. Helleseth, Kumar and Martinsen [8] found ternary sequences with ideal autocorrelation and it turned out to be a cyclic difference set with Singer parameter $(\frac{3^{3k}-1}{3-1}, \frac{3^{3k-1}-1}{3-1}, \frac{3^{3k-2}-1}{3-1})$ [13], [14]. Lin has found a new family of ternary sequences of period 3^n-1 and he conjectured that it has the ideal autocorrelation property, when $n=2m+1$ [12]. Under this assumption, a cyclic difference set (Lin difference set) with Singer parameter $(\frac{3^n-1}{3-1}, \frac{3^{n-1}-1}{3-1}, \frac{3^{n-2}-1}{3-1})$ can be obtained [13], [14].

In this paper, the p-ranks and characteristic polynomials of cyclic difference sets are derived by expanding the trace expressions of their characteristic sequences. By using this method, it is shown that the 3-ranks and characteristic polynomials of Helleseth-Kumar-Martinsen (HKM) difference set and Lin difference set can be easily obtained.

Ⅱ. Preliminaries

Let D be a (v, k, λ) difference set [1], [6] defined as a set of k distinct residues modulo v expressed by

$$D=\{c_1, c_2, c_3, \ldots, c_k\}. \tag{1}$$

Then each non-zero residue occurs exactly λ times among the $k(k-1)$ differences $c_i-c_j, i\neq j$ and thus it satisfies

$$\lambda(v-1)=k(k-1).$$

The complementary difference set of D is a $(v, v-k, v-2k+\lambda)$ difference set defined as

$$\overline{D}=Z_v\setminus D,$$

where Z_v is the ring of integers modulo v.

Then for integers a and b, a set $aD+b$ is defined as

$$aD+b=\{a\cdot c_1+b, a\cdot c_2+b, a\cdot c_3+b, \cdots, a\cdot c_k+b\},$$

where $a\cdot c_i+b$ is taken modulo v. For integers a and b, two (v, k, λ) difference sets D_1 and D_2 are said to be *inequivalent* if D_1 is distinct from aD_2+b for any integers a and b, $1\leq a\leq v-1$, $0\leq b\leq v-1$, where a is relatively prime to v. The *characteristic sequence* of a cyclic difference set D in (1) is defined as a

* 서울대학교 전기.컴퓨터공학부 (jsno@snu.ac.kr),
** 한양대학교 전자전기컴퓨터공학부 (djshin@hanyang.ac.kr)

논문번호 : 010005-0216, 접수일자 : 2001년 2월 16일
※ 본 연구는 BK21과 ITRC 지원 및 관리로 수행되었습니다.

binary sequence given by

$$s(t)=\begin{cases} 1, & \text{if } t\in D \\ 0, & \text{if } t\notin D \end{cases}$$

and the characteristic sequence of its complementary difference set $\overline{D}$ is defined as

$$\begin{aligned} s_c(t) &= \begin{cases} 1, & \text{if } t\in \overline{D} \\ 0, & \text{if } t\notin \overline{D} \end{cases} \\ &= 1-s(t). \end{aligned}$$

The c*haracteristic polynomial* of a cyclic difference set D is defined as a least-degree linear recursion equation over F_p of characteristic sequence $s(t)$ of D. The p-rank [7] of cyclic difference set D is defined as a degree of characteristic polynomial of the cyclic difference set D. In order to prove the inequivalence of two cyclic difference sets, the p-rank is often used. However, it is very difficult to find the p-ranks of cyclic difference sets.

Let $n=e\cdot m>1$ for some positive integers e and m. The trace function is a mapping from F_{p^n} to its subfield F_{p^m} defined by

$$tr_m^n(x)=\sum_{i=0}^{e-1} x^{p^{m\cdot i}}, \tag{2}$$

where x is an element in Galois field F_{p^n}.

Ⅲ. p-Ranks and Characteristic Polynomials of Cyclic Difference Sets

As it will be given in the following theorem and lemma, the characteristic sequences of a cyclic difference set and its complementary difference set can be expressed by using the trace expressions and the p-rank can be calculated by counting the number of terms in the trace expression. Moreover, by finding the minimal polynomials corresponding to this trace expression, we can easily obtain the characteristic polynomial. This method will be used to find the 3-ranks and characteristic polynomials of HKM and Lin difference sets in the following sections.

Let $f(t)$ be a function from Galois field F_{p^n} to its subfield F_{p^m}. Then we have the relation as follows:

$$[f(t)]^{p^m-1}=\begin{cases} 1, & \text{if } f(t)\neq 0 \\ 0, & \text{if } f(t)=0. \end{cases}$$

As in the following theorem, therefore, the characteristic sequence of a cyclic difference set is given by using this relationship.

Theorem 1: Assume that (v,k,λ) cyclic difference set D and its complementary difference set $\overline{D}$ are defined as

$$D=\{t\,|f(t)=0,\ 0\le t<v\} \tag{3}$$

$$D=\{t\,|f(t)\neq 0,\ 0\le t<v\}, \tag{4}$$

where $f(t)$ is given as the summation of trace function from a Galois field F_{p^n} to its subfield F_{p^m}, that is

$$f(t)=\sum_{a\in I} tr_m^n(\alpha^{at})$$

for some index set I and $\alpha\in F_{p^n}$.

Then the characteristic sequences of the cyclic difference set D and its complementary difference set $\overline{D}$ can be expressed as

$$s(t)=1-s_c(t),\quad 0\le t<v$$

and

$$s_c(t)=[f(t)]^{p^m-1},\quad 0\le t<v. \tag{5}$$

□

In order to find the p-rank of the cyclic Difference set $\overline{D}$, we have to expand the trace expression in (5) as given in the following lemma.

Lemma 2 : Let D and $\overline{D}$ be a (v,k,λ) cyclic difference set and its complementary difference set defined by equations (3) and (4), respectively. Suppose that the trace expression of the characteristic sequence $s_c(t)$ of $\overline{D}$ can be expanded as

$$\begin{aligned} s_c(t) &= [f(t)]^{p^m-1} \\ &= [\sum_{a\in I} tr_m^n(\alpha^{at})]^{p^m-1}=\sum_{j\in J} c_j\alpha^{jt}, \end{aligned} \tag{6}$$

where J is an index set and $c_j\in F_p^*$. Then the p

-rank of the complementary difference set $\overline{D}$ is given as $|J|$, which means that the degree of characteristic polynomial of $\overline{D}$ is $|J|$. And the p-rank of the cyclic difference set D is also given as $|J|+1$, if $|\overline{D}|=v-k$ is divisible by p.

Proof : Let $g(x)$ and $g_c(x)$ be the characteristic polynomials over F_p of a cyclic difference set D and its complementary difference set $\overline{D}$, respectively. Since there is the relationship between $s_c(t)$ and $s(t)$ as

$$s(t)=1-s_c(t),$$

we have the relationship between their characteristic polynomials as

$$\frac{a(x)}{g(x)}=\frac{1}{x-1}-\frac{b(x)}{g_c(x)}=\frac{g_c(x)-(x-1)b(x)}{(x-1)\cdot g_c(x)},$$

where the polynomials $a(x)$ and $b(x)$ are relatively prime to $g(x)$ and $g_c(x)$, respectively. If $|\overline{D}|=v-k$ is divisible by p, then the number of 1's in one period of the characteristic sequence of the cyclic difference set $\overline{D}$ is a multiple of p. Therefore, the polynomial expression of the characteristic sequence possesses the factor $x-1$ and it removes the factor $x-1$ in the characteristic polynomial, which means that the characteristic polynomial $g_c(x)$ is not divisible by $x-1$. Therefore, the polynomial $g_c(x)-(x-1)b(x)$ is relatively prime to $(x-1)g_c(x)$ and we get the following relationship

$$g(x)=(x-1)g_c(x), \tag{7}$$

if $|\overline{D}|=v-k$ is divisible by p. Therefore, the p-rank of the cyclic difference set D is $|J|+1$, if $|\overline{D}|=v-k$ is divisible by p.

□

If the equation (6) is expressed as a summation of trace functions as

$$[f(t)]^{p^m-1}=\sum_{k|n,k>1}\sum_{a_k\in J_k}c_{a_k}\cdot tr_1^k(\alpha_k^{a_k t}),$$

where $c_{a_k}\in F_p^*$, J_k's are index sets and α_k is a primitive element of F_{p^k}, the characteristic polynomials of the cyclic difference set D and its complementary difference set $\overline{D}$ can be expressed as in the following theorem.

Theorem 3 : If the characteristic sequence of a cyclic difference set $\overline{D}$ is expressed as

$$s_c(t)=\sum_{k|n,k>1}\sum_{a_k\in J_k}c_{a_k}\cdot tr_1^k(\alpha_k^{a_k t}),$$

where $c_{a_k}\in F_p^*$ and if $|\overline{D}|=v-\lambda$ is divisible by p, then the characteristic polynomials $g(x)$ and $g_c(x)$ of the cyclic difference set D and its complementary difference set $\overline{D}$ are given as follows:

$$g(x)=(x-1)\cdot g_c(x) \tag{8}$$

$$g_c(x)=\prod_{k|n,k>1}\prod_{a_k\in J_k}M_{a_k}(x), \tag{9}$$

where $M_{a_k}(x)$ is the minimal polynomial of the element $\alpha_k^{a_k}\in F_{p^k}$.

□

Note that the p-rank of D is one bigger than that of $\overline{D}$. For the cyclic difference set with Singer parameter $(v,k,\lambda)=(\frac{q^n-1}{q-1},\frac{q^{n-1}-1}{q-1},\frac{q^{n-2}-1}{q-1})$, where $q=p^m$, $v-k=q^{n-1}=p^{m(n-1)}$ is divisible by p. Therefore, the above theorem can be applied to find the p-ranks and characteristic polynomials of the cyclic difference set with Singer parameter and its complementary difference set.

Ⅳ. 3-Ranks and Characteristic Polynomials of HKM Difference Sets

Recently, Helleseth, Kumar and Martinsen introduced a new ternary sequence ($p=3$) with ideal autocorrelation. It turned out to be a cyclic difference set (HKM difference set) with Singer parameter and the p-ranks of HKM difference set and its complementary difference set are derived in the following theorem.

Theorem 4: HKM difference set with parameter $(v,k,\lambda)=(\frac{3^n-1}{3-1},\frac{3^{n-1}-1}{3-1},\frac{3^{n-2}-1}{3-1})$ is defined by

$$D=\left\{t \mid tr_1^n(a^t)+tr_1^n(a^{dt})=0,\ 0\le t<\frac{3^n-1}{3-1}\right\},$$

where $n=3k$, $d=3^{2k}-3^k+1$, and a is a primitive element of F_{3^n}. Then the 3-ranks of HKM difference set D and its complementary difference set $\overline{D}$ are given as $2n^2-2n+1$ and $2n^2-2n$, respectively.

Proof: Let $x=a^t$. Then we can expand the square of trace function as

$$\begin{aligned}
&[tr_1^n(a^t)]^2\\
&=[tr_1^n(x)]^2=tr_1^n(x)\cdot tr_1^n(x)\\
&=tr_1^n(x\cdot tr_1^n(x))\\
&=tr_1^n(x\cdot(x+x^3+x^{3^3}+\cdots{}^{3^{n-1}}_{x}))\\
&=\sum_{i=0}^{n-1}tr_1^n(x^{1+3^i})\\
&=tr_1^n(x^{1+1})+\sum_{i=1}^{n-1}tr_1^n(x^{1+3^i})\\
&=\begin{cases}tr_1^n(x^{1+1})+2\cdot\displaystyle\sum_{i=1}^{\frac{n-1}{2}}tr_1^n(x^{1+3^i}), & \text{for } n=odd\\ tr_1^n(x^{1+1})+2\cdot tr_1^{\frac{n}{2}}(x^{1+3^{\frac{n}{2}}}) \\ \quad +2\cdot\displaystyle\sum_{i=1}^{\frac{n-1}{2}}tr_1^n(x^{1+3^i}), & \text{for } n=even.\end{cases}
\end{aligned}$$

The characteristic sequence of the cyclic difference set $\overline{D}$ is given as

$$[tr_1^n(x)+tr_1^n(x^d)]^2. \tag{10}$$

Using the expansion of the square of trace function, we can also expand the equation (10) as in the followings.

(i) $n=2m+1$ (odd case)

$$\begin{aligned}
&[tr_1^n(x)+tr_1^n(x^d)]^2\\
&=[tr_1^n(x)]^2+[tr_1^n(x^d)]^2\\
&\quad+2\cdot tr_1^n(x)\cdot tr_1^n(x^d)\\
&=tr_1^n(x^{1+1})+2\cdot\sum_{i=1}^{\frac{n-1}{2}}tr_1^n(x^{1+3^i})\\
&\quad+tr_1^n(x^{(1+1)d})+2\cdot\sum_{i=1}^{\frac{n-1}{2}}tr_1^n(x^{(1+3^i)d})\\
&\quad+2\cdot tr_1^n(x^d\cdot tr_1^n(x))\\
&=tr_1^n(x^{1+1})+2\cdot\sum_{i=1}^{\frac{n-1}{2}}tr_1^n(x^{1+3^i})\\
&\quad+tr_1^n(x^{(1+1)d})+2\cdot\sum_{i=1}^{\frac{n-1}{2}}tr_1^n(x^{(1+3^i)d}).
\end{aligned}$$

Since

$$\begin{aligned}d\cdot(3^k+1)&=3^{3k}+1=3^{3k}-1+2\\&\equiv 2\ \mathrm{mod}(3^{3k}-1),\end{aligned}$$

we have $tr_1^n(x^{(1+3^k)d})=tr_1^n(x^{1+1})$.

And since $d+3^k=3^{2k}+1$, we have

$$tr_1^n(x^{d+3^k})=tr_1^n(x^{3^{2k}+1})=tr_1^n(x^{x^{3^k+1}}).$$

Therefore,

$$\begin{aligned}
&[tr_1^n(x)+tr_1^n(x^d)]^2\\
&=2\cdot\sum_{i=1,i\neq k}^{m}tr_1^n(x^{1+3^i})+tr_1^n(x^{(1+1)d})\\
&\quad+2\cdot\sum_{i=1,i\neq k}^{m}tr_1^n(x^{(1+3^i)d})\\
&\quad+2\cdot\sum_{i=0,i\neq k}^{n-1}tr_1^n(x^{3^{2k}-3^k+1+3^i})\\
&\quad+tr_1^n(x^{1+3^k}).
\end{aligned}\tag{11}$$

It is easy to prove that all exponents belong to the different cyclotomic coset of size n. Therefore, the 3-rank of $\overline{D}$ is given as

$$\begin{aligned}&(m-1)n+n+(m-1)n+(n-1)n+n\\&=2\cdot n(n-1)\end{aligned}$$

and the 3-rank of HKM difference set D is derived as $2n^2-2n+1$.

(ii) $n=2m$ (even case)

$$\begin{aligned}
&[tr_1^n(x)+tr_1^n(x^d)]^2\\
&=[tr_1^n(x)]^2+[tr_1^n(x^d)]^2+2\cdot tr_1^n(x)\cdot tr_1^n(x^d)\\
&=tr_1^n(x^{1+1})+2\cdot tr_1^m(x^{1+3^m})\\
&\quad+2\cdot\sum_{i=1}^{m-1}tr_1^n(x^{1+3^i})+tr_1^n(x^{(1+1)d})\\
&\quad+2\cdot tr_1^m(x^{(1+3^m)d})+2\cdot\sum_{i=1}^{m-1}tr_1^n(x^{(1+3^i)d})\\
&\quad+2\cdot\sum_{i=0}^{n-1}tr_1^n(x^{3^{2k}-3^k+1+3^i}).
\end{aligned}$$

Since $(1+3^k)\cdot d=2$ mod $(3^{3k}-1)$, we have

$$tr_1^n(x^{(1+3^k)d})=tr_1^n(x^2),$$

and since $3^{2k}-3^k+1+3^k=3^{2k}+1$, we have

$$tr_1^n(x^{d+3^k})=tr_1^n(x^{1+3^{2k}})=tr_1^n(x^{1+3^k}).$$

Adding up the same trace terms, we have

$$\begin{aligned}
&[tr_1^n(x)+tr_1^n(x^d)]^2\\
&=2\cdot tr_1^m(x^{(1+3^m)})+2\cdot\sum_{i=1,i\neq k}^{m-1}tr_1^n(x^{1+3^i})\\
&\quad+tr_1^n(x^{(1+1)d})+2\cdot tr_1^m(x^{(1+3^m)d})\\
&\quad+2\cdot\sum_{i=1,i\neq k}^{m-1}tr_1^n(x^{d(1+3^i)}).\\
&\quad+2\cdot\sum_{i=0,i\neq k}^{n-1}tr_1^n(x^{d+3^i})+tr_1^n(x^{1+3^k}).
\end{aligned}\tag{12}$$

It can be shown that all exponents belong to different cosets of size n or m. Therefore the 3-rank of the difference set $\overline{D}$ is

$$\begin{aligned}&m+(m-2)n+n+m+(m-2)n\\&+(n-1)n+n=2\cdot n(n-1)\end{aligned}$$

and from (8) the 3-rank of HKM difference set D is derived as $2n^2-2n+1$.

□

From the equations (11) and (12), we can derive the characteristic polynomials of HKM difference set and its complementary difference set as in the following theorem.

Theorem 5: HKM difference set with parameter $(v,k,\lambda)=\left(\frac{3^n-1}{3-1},\frac{3^{n-1}-1}{3-1},\frac{3^{n-2}-1}{3-1}\right)$ is defined by

$$D=\left\{t \mid tr_1^n(\alpha^t)+tr_1^n(\alpha^{dt})=0,\ 0\le t<\frac{3^n-1}{3-1}\right\}, \tag{13}$$

where $n=3k$, $d=3^{2k}-3^k+1$ and α is a primitive element of F_{3^n}. Then the characteristic polynomials of the HKM difference set D in (13) and its complementary difference set $\overline{D}$ are given as:

For $n=2m+1$:

$$\begin{aligned} g(x) &= (x-1)g_c(x)\\ g_c(x) &= M_{2d}(x)M_{1+3^k}(x)\prod_{i=1,i\ne k}^{m}M_{1+3^i}(x)\\ &\quad \prod_{i=1,i\ne k}^{m}M_{(1+3^i)d}(x)\prod_{i=0,i\ne k}^{n-1}M_{d+3^i}(x). \end{aligned}$$

For $n=2m$:

$$\begin{aligned} g(x) &= (x-1)g_c(x)\\ g_c(x) &= M_{2d}(x)M_{1+3^m}(x)M_{(1+3^m)d}(x)\\ &\quad M_{1+3^k}(x)\prod_{i=1,i\ne k}^{m-1}M_{1+3^i}(x)\\ &\quad \prod_{i=1,i\ne k}^{m-1}M_{(1+3^i)d}(x)\prod_{i=0,i\ne k}^{n-1}M_{d+3^i}(x). \end{aligned}$$

V. 3-Ranks and Characteristic Polynomials of Lin Difference Sets

Lin has conjectured that the family of ternary sequences $c(t)=tr_1^n(\alpha^t)+tr_1^n(\alpha^{dt})$ has the ideal autocorrelation property, where $n=2m+1$and $d=2\cdot 3^{m+1}$. If it is true, then it gives a cyclic difference set (Lin difference set) with Singer parameter. Under this assumption, we can derive the 3-ranks and characteristic polynomials of Lin difference set and its complementary difference set as in the following theorems.

Theorem 6: Lin difference set with $(v,k,\lambda)=\left(\frac{3^n-1}{3-1},\frac{3^{n-1}-1}{3-1},\frac{3^{n-2}-1}{3-1}\right)$ is defined by

$$D=\left\{t \mid tr_1^n(\alpha^t)+tr_1^n(\alpha^{dt})=0,\ 0\le t<\frac{3^n-1}{3-1}\right\},$$

where $n=2m+1$, $d=2\cdot 3^m+1$ and α is a primitive element of F_{3^n}. Then the 3-ranks of the Lin difference set D and its complementary difference set $\overline{D}$ are given as $2n^2-2n+1$ and $2n^2-2n$, respectively.

Proof: Let $x=\alpha^t$. Then the characteristic sequence of the difference set $\overline{D}$ is given as

$$[tr_1^n(x)+tr_1^n(x^d)]^2. \tag{14}$$

Using the expansion of the square of trace function in the proof of the previous theorem, we can also expand the equation (14) as in the followings.

$$\begin{aligned} &[tr_1^n(\alpha^t)+tr_1^n(\alpha^{dt})]^2\\ &=[tr_1^n(x)]^2+[tr_1^n(x^d)]^2+2\cdot tr_1^n(x)\,tr_1^n(x^d)\\ &=tr_1^n(x^{1+1})+2\cdot\sum_{i=1}^{m}tr_1^n(x^{1+3^i})\\ &\quad +tr_1^n(x^{(1+1)d})+2\cdot\sum_{i=1}^{m}tr_1^n(x^{(1+3^i)d})\\ &\quad +2\cdot\sum_{i=0}^{n-1}tr_1^n(x^{d+3^i}). \end{aligned}$$

Since $d+3^m=2\cdot 3^m+1+3^m=3^{m+1}+1$, we have

$$tr_1^n(x^{d+3^m})=tr_1^n(x^{1+3^m})$$

and since $d+3^{n-1}=3^{n-1}+2\cdot 3^m+1$, we have

$$\begin{aligned} tr_1^n(x^{d+3^{n-1}}) &= tr_1^n(x^{2\cdot 3^{m+1}+3+1})\\ &= tr_1^n(x^{2\cdot(\cdot 3^{m+1}+2)})\\ &= tr_1^n(x^{2\cdot(1+2\cdot 3^m)})\\ &= tr_1^n(x^{(1+1)d}). \end{aligned}$$

Adding up the same trace terms, we have

$$\begin{aligned} &[tr_1^n(x)+tr_1^n(x^d)]^2\\ &=tr_1^n(x^{1+1})+2\cdot\sum_{i=1}^{m-1}tr_1^n(x^{1+3^i})\\ &\quad +tr_1^n(x^{1+3^m})+2\cdot\sum_{i=1}^{m}tr_1^n(x^{(1+3^i)d})\\ &\quad +2\cdot\sum_{i=0,i\ne m}^{n-2}tr_1^n(x^{3^i+d}). \end{aligned} \tag{15}$$

It can be shown that all exponents belong to the different cosets of size n. Therefore, the 3-rank of the difference set $\overline{D}$ is

$$\begin{aligned} &n+(m-1)n+n+m\cdot n+n(n-2)\\ &=2n(n-1) \end{aligned}$$

and from the equation (8), the 3-rank of Lin difference set D is $2n^2-2n+1$.

□

From the equation (15), we can derive the characteristic polynomials of Lin difference set and its complementary difference set as in the following theorem.

Theorem 7: Lin difference set with parameter $(v,k,\lambda)=(\frac{3^n-1}{3-1},\frac{3^{n-1}-1}{3-1},\frac{3^{n-2}-1}{3-1})$ is defined by

$$D=\left\{t \mid tr_1^n(a^t)+tr_1^n(a^{dt})=0,\ 0\le t<\frac{3^n-1}{3-1}\right\}. \qquad (16)$$

where $n=2m+1$, $d=2\cdot 3^m+1$ and a is a primitive element of F_{3^n}. Then the characteristic polynomials of the Lin difference set D and its complementary difference set $\overline{D}$ are given as:

$$g(x)=(x-1)g_c(x)$$
$$g_c(x)=M_2(x)M_{1+3^m}(x)\prod_{i=1}^{m-1}M_{1+3^i}(x)$$
$$\prod_{i=1}^{m}M_{(1+3^i)d}(x)\prod_{i=0,i\neq m}^{n-2}M_{d+3^i}(x).$$

□

References

[1] L.D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics, pp. 71-79, 1971.

[2] J. Singer, "A theorem in finite projective geometry and some applications to number theory," *Trans. Amer. Math. Soc*, 43, pp. 377-385, 1983.

[3] B. Gordon, W.H. Mills and L.R. Welch, "Some new difference sets," *Canad. J. Math.*, 14, pp. 614-625, 1962.

[4] J.F. Dillon, "Multiplicative difference sets via additive character," *Designs, Codes and Cryptography*, 17, pp. 225-235, 1999.

[5] J.F. Dillon and H. Dobbertin, "Cyclic difference sets with Singer parameters," Preprint, 1999.

[6] D. Jungnickel, "Difference sets," *Contemporary Design Theory: A Collection of Surveys*, 1992.

[7] R. Evans, H. Hollmann, C. Krattenthaler and Q. Xiang, "Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets," *Journals of Combin. Theory*, 87, pp. 74-119, 1999.

[8] T. Helleseth, P.V. Kumar, and H.M. Martinsen, "A new family of ternary sequences with ideal two-level autcorrelation," *Proceedings of International Symposium on Information Theory*, pp. 3289, Jun. 2000.

[9] J.S. No, K. Yang, H. Chung and H.Y. Song, "On the construction of binary sequences with ideal autocorrelation property," Proceedings of 1996 IEEE International Symposium on Information Theory and Its Applications, pp. 837-840, Sep. 1996.

[10] J.S. No, H. Chung and M.S. Yun, "Binary pseudorandom sequences of period 2^m-1 with ideal autocorrelation generated by the polynomial $z^d+(z+1)^d$," *IEEE Trans. Inform. Theory*, 44, pp. 1278-1282, 1998.

[11] J.S. No, S.W. Golomb, G. Gong, H.K. Lee and P. Gaal, "Binary pseudorandom sequences of period 2^n-1 with ideal autocorrelation," *IEEE Trans. Inform. Theory*, 44, pp. 814-817, 1998.

[12] H.A. Lin, "From cyclic Hadamard difference Sets to perfectly balanced sequences," Ph.D. Dissertation, University of Southern California, May 1998.

[13] J.S. No, "New cyclic difference sets with Singer parameters constructed from d-homogeneous functions," Preprint, 2000.

[14] T. Helleseth and M. Martinsen, "Open problems in sequence design and correlation," Preprint, 2000.

[15] K. J. C. Smith, "On the p-rank of the incidence matrix of points and hyperplanes in a finite projective geometry," *J. Comb. Theory*, 7, pp. 122-129, 1996.

[16] E. F. Assmus, Jr. and J. D. Key, *Designs and their codes*, *Cambridge Univ. Press*, 1992.

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

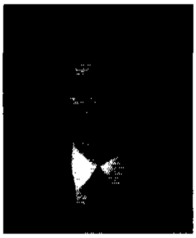
1988년 2월~1990년 7월 : Hughes Network Systems, Senior MTS

1990년 9월~1999년 7월 : 건국대학교 전자공학과 부교수

1999년 8월~현재 : 서울대학교 전기 · 컴퓨터공학부 조교수

<주관심 분야> 시퀀스, 오류정정부호, 암호학, 이동통신

신 동 준(Dong-Joon Shin) 정회원



1990년 2월 : 서울대학교 전자공학과 공학사

1991년 12월 : Northwestern University, 전기공학과 공학석사

1998년 12월 :University of Southern California, 전기공학과 공학박사

1999년 1월~1999년 4월 : Research Associate(USC)

1999년 4월~2000년 8월 : Hughes Network Systems, MTS

2000년 9월~현재 : 한양대학교 전자전기컴퓨터공학부 전임강사

<주관심 분야> 디지털통신, 이산수학, 시퀀스, 오류정정부호, 암호학