A Theory on the Construction of Binary Sequences with Ideal Autocorrelation

Jong-Seon No, Kyeong-Cheol Yang, Ha-Bong Chung, and Hong-Yeop Song

Abstract

In this paper, we present a closed-form expression of binary sequences of longer period with ideal autocorrelation property in a trace representation, if a given binary sequence with ideal autocorrelation property is described using the trace function. We also enumerate the number of cyclically distinct binary sequences of a longer period with ideal autocorrelation property, which are extended from a given binary sequence with ideal autocorrelation property.

I. Introduction

A binary (0 or 1) sequence $\{b(t), t=0,1,\ldots,N-1\}$ of period $N=2^n-1$ is called *balanced* if the number of 1's is one more than the number of 0's. It is said to have the *ideal autocorrelation property* if its periodic autocorrelation function $R(\tau)$ is given by

$$R(\tau) = \begin{cases} N, & \text{for } \tau\equiv 0 \mod N, \\ -1, & \text{for } \tau\not\equiv 0 \mod N, \end{cases}$$

where $R(\tau)$ is defined as

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

and $t+\tau$ is computed mod N. Note that $R(\tau)$ is the number of agreements between $\{b(t)\}$ and $\{b(t+\tau)\}$ minus the number of disagreements for any $\tau \not\equiv 0 \ (\mod N)$ as t runs from 0 to N-1 [2, 3, 16].

Balanced binary sequences of period 2^n-1 having the ideal autocorrelation function find many applications in spread spectrum communication systems[2, 3, 10, 12, 13, 15, 16, 17]. Some of the well-known binary sequences of period 2^n-1 include m-sequences, GMW sequences, Legendre sequences, etc.

Let $\{b(t)\}$ and $\{c(t)\}$ be two binary sequences of period N. Two sequences $\{b(t)\}$ and $\{c(t)\}$ are defined to be *cyclically equivalent* if there exists an integer τ such that $c(t) = b(t+\tau)$ for all t. Otherwise, they are said to be *cyclically distinct.* For an integer r, the sequence $\{c(t)\}$ is called the *decimation* by r of the sequence $\{b(t)\}$ if $c(t) = b(rt)$ for any integer t. It is easily checked that the period of $\{c(t) = b(rt)\}$ is given by N divided by gcd(r, N). Two sequences $\{b(t)\}$ and $\{c(t)\}$ are said to be *inequivalent* if there are no integers r and τ such that $c(t) = b(r[t+\tau])$ for all t.

In this paper, we present a generalization method of extending binary sequences with ideal autocorrelation property as a closed-form expression. We also enumerate the number of cyclically distinct binary sequences of a longer period with ideal autocorrelation property, which are extended from a given binary sequence with ideal autocorrelation property.

This paper is organized as follows. In Section II, we present the main theorems to extend binary sequences with ideal autocorrelation property. We also enumerate the number of cyclically distinct extensions of a given binary sequence with ideal autocorrelation property. We mention an important question on linear span of the extended sequences in Concluding Remarks.

II. Extension of Binary Sequences with Ideal Autocorrelation

It has been known that binary sequences of longer period with ideal autocorrelation property can be constructed from a binary sequence of shorter period with ideal autocorrelation property, but an explicit construction method has not been well described except for the GMW sequences. Our main result is to give a closed-form expression of binary sequences of longer period with

Manuscript received September 15, 1997; accepted November 20, 1997.

J.-S. No is with Dept. of Electronic Engineering, Konkuk University, Seoul 143-701, Korea.

K. Yang is with Dept. of Electronic Communication Engineering, Hanyang University, Seoul 133-791, Korea.

H. Chung is with Dept. of Electronic Engineering, Hong-Ik University, Seoul 121-791, Korea.

H.-Y Song is with Dept. of Electronic Engineering, Yonsei University, Seoul 120-749, Korea.

ideal autocorrelation property in their trace representation.

The new binary sequences of longer period constructed in this method will be referred to as *extensions* of a given sequence.

Let q be a prime power and let F_q be the finite field with q elements. Let $n = em > 1$ for some positive integers e and m. Then the trace function $tr_m^n(\cdot)$ is a mapping from F_{2^n} to its subfield F_{2^m} given by

$$tr_m^n(x) = \sum_{i=0}^{e-1} x^{2^{mi}}.$$

It is easy to check that the trace function satisfies the following:

(i) $tr_m^n(ax+by) = a\,tr_m^n(x) + b\,tr_m^n(y)$, for all $a, b \in F_{2^m}$, $x, y \in F_{2^n}$.

(ii) $tr_m^n(x^{2^m}) = tr_m^n(x)$, for all $x \in F_{2^n}$.

(iii) $tr_1^n(x) = tr_1^m(tr_m^n(x))$, for all $x \in F_{2^n}$.

See[6, 7] for the detailed properties of the trace function.

For the remaining, we are interested in the case where $n = em$ for integers $m > 1$ and $e > 1$. We use the following notation:

- $N = 2^n - 1, M = 2^m - 1$, and $T = \frac{N}{M} = \frac{2^n - 1}{2^m - 1}$.
- α, β : primitive elements of F_{2^m}, F_{2^n}, respectively.
- $\{b(t_1),\ t_1 = 0, 1, \ldots, M-1\}$
  = a binary sequence of period M with ideal autocorrelation property.
- $\{c(t),\ t = 0, 1, \ldots, N-1\}$
  = binary sequence of period N as an extension of $\{b(t_1)\}$.

It is well-known that the ideal autocorrelation property of a sequence of period N is invariant under the decimation by r, if r is an integer relatively prime to N. The statement is restated in the following proposition.

Proposition 1 : Let r, $1 \le r \le N$-1, be an integer relatively prime to N. If a sequence $\{c(t),\ t = 0, 1, \ldots, N\text{-}1\}$ of period N has the ideal autocorrelation property, so does its decimation $\{c(rt),\ t = 0, 1, \ldots, N\text{-}1\}$

Theorem 2 : Let m and n be positive integers such that m | n. Let β be a primitive element of F_{2^n} and set $\alpha = \beta^T$ where $T = (2^n\text{-}1)/(2^m\text{-}1)$. Assume that for an index set I, the sequence $\{b(t_1),\ t_1 = 0, 1, \ldots, M-1\}$ of period $M = 2^n$-1 given by

$$b(t_1) = \sum_{a \in I} tr_1^m(\alpha^{at_1})$$

has the ideal autocorrelation property. For an integer r, $1 \le r \le M$-1, relatively prime to M, the sequence $\{c(t),\ t = 0, 1, \ldots, N\text{-}1\}$ of period $N = 2^n$-1 defined by

$$c(t) = \sum_{a \in I} tr_1^m\{[tr_m^n(\beta^t)]^{ar}\}$$

also has the ideal autocorrelation property.

Proof : Consider an m-sequence $\{v(t) = tr_1^n(\beta^t),\ t = 0, 1, \ldots, N-1\}$, of period $N = 2^n$-1. Arrange it in the $M \times T$ rectangular array $X_0 = [x_{t_1 t_2}^{(0)}]$ such that $x_{t_1 t_2}^{(0)} = v(t_1 T + t_2)$, where $t_1 = 0, 1, \ldots, 2^m - 2$, and $t_2 = 0, 1, \ldots, T-1$. Since

$$\begin{aligned} v(t) &= v(t_{1T+t_2}) \\ &= tr_1^m\{tr_m^n(\beta^{t_1 T + t_2})\} \\ &= tr_1^m\{\alpha^{t_1} \cdot tr_m^n(\beta^{t_2})\}, \end{aligned}$$

the t_2-th column $\{x_{t_1 t_2}^{(0)},\ t_1 = 0, 1, \ldots, M-1\}$ of X_0 is either a cyclic shift of an m-sequence $\{tr_1^m(\alpha^{t_1}),\ t_1 = 0, 1, \ldots, M-1\}$ of period $M = 2^n$-1 or the all-zero sequence. That is,

$$x_{t_1 t_2}^{(0)} = \begin{cases} tr_1^m(\alpha^{t_1 + l}) & \text{if } tr_m^n(\beta^{t_2}) = \alpha^l, \\ 0 & \text{if } tr_m^n(\beta^{t_2}) = 0, \end{cases} \tag{1}$$

where l, $0 \le l \le M$-1, is an integer. Similarly, if we arrange $\{v(t+\tau),\ t = 0, 1, \ldots, N-1\}$ for $\tau \not\equiv 0 (\mathrm{mod}\ N)$ in the $M \times T$ rectangular array $X_\tau = [x_{t_1 t_2}^{(\tau)}]$ such that $x_{t_1 t_2}^{(\tau)} = v(t_1 T + t_2 + \tau)$, where $t_1 = 0, 1, \ldots, M-1$, and $t_2 = 0, 1, \ldots, T-1$, then the t_2-th column $\{x_{t_1 t_2}^{(\tau)},\ t_1 = 0, 1, \ldots, M-1\}$ of X_0 is also either a cyclic shift of an m-sequence $\{tr_1^m(\alpha^{t_1}),\ t_1 = 0, 1, \ldots, M-1\}$ of period M or the all-zero sequence. That is,

$$x_{t_1 t_2}^{(\tau)} = \begin{cases} tr_1^m(\alpha^{t_1' + l}) & \text{if } tr_m^n(\beta^{t_2'}) = \alpha^l, \\ 0 & \text{if } tr_m^n(\beta^{t_2'}) = 0, \end{cases} \tag{2}$$

where $t + \tau = t_1' T + t_2'$, $0 \le t_1' \le M$-1, $0 \le t_2' \le T$-1. Expressing τ into

$$\tau = \tau_1 T + \tau_2, \quad 0 \le \tau_1 \le M-1,\ 0 \le \tau_2 \le T-1,$$

it is easy to check that

$$t_2' = t_2 + \tau_2 \mod T \tag{3}$$

$$t_1' = t_1 + \tau_1 + (t_2 + \tau_2 - t_2')/T. \tag{4}$$

Since $\{v(t)\}$ has the ideal autocorrelation property, we have

$$\begin{aligned} -1 &= \sum_{t=0}^{N-1} (-1)^{v(t) + v(t+\tau)} \\ &= \sum_{t_2=0}^{T-1} \Big[\sum_{t_1=0}^{M-1} (-1)^{x_{t_1 t_2}^{(0)} + x_{t_1 t_2}^{(\tau)}} \Big] \end{aligned} \tag{5}$$

for any integer $\tau \not\equiv 0 (\mathrm{mod}\ N)$. Note that the inner sum can yield the value 2^m-1 when both $\{x_{t_1 t_2}^{(0)},\ 0 \le t_1 \le M-1\}$ and $\{x_{t_1 t_2}^{(\tau)},\ 0 \le t_1 \le M-1\}$ are identical as an m-sequence of the same phase or as the all-zero sequence, and the value -1 when either of them is the all-zero sequence or both are the distinct cyclic shifts of an m-sequence. In order to satisfy Equation (5), the inner sum gives the value 2^m-1 with $(T\text{-}1)/2^m$ times, and the value -1 with $T\text{-}(T\text{-}1)/2^m$ times as t_2 runs from 0 to T-1.

Now consider the sequence $\{c(t), t = 0, 1, \ldots, N-1\}$ and arrange it in the $M \times T$ rectangular array $Y_0 = [y_{t_1t_2}^{(0)}]$ in the same manner as the previous case. Since

$$\begin{aligned} c(t) &= c(t_1T+t_2) \\ &= \sum_{a\in I} tr_1^m\{[tr_m^n(\beta^{t_1T+t_2})]^{ar}\} \\ &= \sum_{a\in I} tr_1^m\{\alpha^{art_1}[tr_m^n(\beta^{t_2})]^{ar}\}, \end{aligned}$$

we know that the t_2-th column $\{y_{t_1t_2}^{(0)}, t_1=0,1,\ldots,M-1\}$ of Y_0 is either a decimation $\{b(r[t_1+l]), t_1=0,1,\ldots,M-1\}$ by r of $\{b(t_1)\}$ when $tr_m^n(\beta^{t_2})=\alpha^l$, or the all-zero sequence when $tr_m^n(\beta^{t_2})=0$. That is,

$$y_{t_1t_2}^{(0)} = \begin{cases} b(r[t_1+l]) & \text{if } tr_m^n(\beta^{t_2})=\alpha^l, \\ 0 & \text{if } tr_m^n(\beta^{t_2})=0, \end{cases} \tag{6}$$

where l, $0 \le l \le M-1$, is an integer. Similarly, if we arrange $\{c(t+\tau), t = 0, 1, \ldots, N-1\}$ for $\tau \not\equiv 0 (\mathrm{mod}\ N)$ in the $M \times T$ rectangular array $Y_\tau = [y_{t_1t_2}^{(\tau)}]$ such that $y_{t_1t_2}^{(\tau)} = c(t_1T+t_2+\tau)$, where $t_1 = 0, 1, \ldots, M-1$ and $t_2 = 0, 1, \ldots, M-1$, then the t_2-th column $\{y_{t_1t_2}^{(\tau)}, t_1=0,1,\ldots,M-1\}$ of Y_0 is also either a cyclic shift of the decimation $\{b(rt_1), t_1=0,1,\ldots,M-1\}$ by r of $\{b(t_1), t_1=0,1,\ldots,M-1\}$ of period M or the all-zero sequence. That is,

$$y_{t_1t_2}^{(\tau)} = \begin{cases} b(r[t_1'+l]) & \text{if } tr_m^n(\beta^{t_2'})=\alpha^l, \\ 0 & \text{if } tr_m^n(\beta^{t_2'})=0, \end{cases} \tag{7}$$

where t_1' and t_2' are defined in Eq. (3) and (4), respectively. Since $\{b(t_1), t_1=0,1,\ldots,M-1\}$ has the ideal autocorrelation property, so does $\{b(rt_1)\}$ by Proposition 1. Comparing Eq. (1) and (2) with Eq. (6) and (7), we observe that the all-zero sequence and an m-sequence $\{tr_1^m(\alpha^{t_1})\}$ in the array X_0 and X_τ are replaced by the all-zero sequence and a decimation $\{b(rt_1)\}$ by r of a given sequence $\{b(t_1)\}$ in the array Y_0 and X_τ with *the same phases*, respectively. This implies that the sum

$$\sum_{t_1=0}^{2^m-2}(-1)^{y_{t_1t_2}^{(0)}+y_{t_1t_2}^{(\tau)}}$$

will yield the values 2^m-1 and -1 with the same number of times as the m-sequence, respectively. Therefore, we have

$$\begin{aligned} \sum_{t=0}^{2^n-2}(-1)^{c(t)+c(t+\tau)} &= \sum_{t_2=0}^{T-1}\sum_{t_1=0}^{2^m-2}(-1)^{y_{t_1t_2}^{(0)}+y_{t_1t_2}^{(\tau)}} \\ &= (2^m-1)\cdot\frac{T-1}{2^m}+(-1)\cdot\left(T-\frac{T-1}{2^m}\right) \\ &= -1 \end{aligned}$$

for any integer $\tau \not\equiv 0 (\mathrm{mod}\ N)$.

In order to extend the binary sequences with ideal autocorrelation property using Theorem 2, we need to express them in a trace representation. On the other hand, it is easily shown that any binary sequence of period $M = 2^m$-1 can be expressed using the trace function over F_2. Hence, Theorem 2 may be very powerful in extending binary sequences with ideal autocorrelation property. We will prove another generalization method in the following.

Theorem 3 : Let m, n and k be positive integers such that $m \mid n \mid k$. Let γ be a primitive element of F_{2^k} and set $\alpha=\gamma^{(2^k-1)/(2^m-1)}$. Let r, $1\le r\le M-1$, be an integer relatively prime to M, and let s, $1\le s\le N-1$, be an integer relatively prime to $N = 2^m$-1. Assume that for an index set I, the sequence $\{b(t_1), t_1=0,1,\ldots,M-1\}$ of period $M = 2^m$-1 given by

$$b(t_1) = \sum_{a\in I} tr_1^m(\alpha^{at_1})$$

has the ideal autocorrelation property. Then the sequence $\{d(t), t=0,1,\ldots,K-1\}$ of period $K = 2^k$-1 defined by

$$d(t) = \sum_{a\in I} tr_1^m\{[tr_m^n\{[tr_n^k(\gamma^t)]^s\}]^{ar}\}$$

also has the ideal autocorrelation property.

Proof : Note that the sequence $\{g(t), t=0,1,\ldots,K-1\}$ defined by

$$g(t) = tr_1^m\{[tr_m^k(\gamma^t)]^r\} \tag{8}$$

is a GMW sequence of period $K = 2^k$-1. It is well-known that it has the ideal autocorrelation property. Obviously, it is also easily checked by applying Theorem 2 to an m-sequence. Applying Theorem 2 to the sequence $\{b(t_1)\}$, it can be extended to a sequence $\{c(t_2), t_2=0,1,\ldots,N-1\}$ of period $N = 2^n$-1 with ideal autocorrelation property defined by

$$c(t_2) = \sum_{a\in I} tr_1^m\{[tr_m^n(\beta^{t_2})]^{ar}\} \tag{9}$$

where $\beta=\gamma^{(2^k-1)/(2^n-1)}$. Let $T=(2^k-1)/(2^n-1)$ and let $t=t_2T+t_3$, $t_2=0,1,\ldots,N-1$; $t_3=0,1,\ldots,T-1$.

The same arguments as in the proof of Theorem 2 complete the proof, except that the m-sequence $\{v(t)\}$, $\{b(t_1)\}$, and $\{c(t)\}$ are replaced by the GMW sequence $\{g(t)\}$ in Eq. (8), $\{c(t_2)\}$ in Eq. (9), and $\{d(t)\}$, respectively.

Remark 4 : Extending further as in Theorem 3 is essentially the same as applying Theorem 2 successively. It can be inductively shown by proving that the sequence $\{d(t)\}$ in Theorem 3 can be obtained by applying Theorem 2 to $\{b(t_1)\}$ consecutively. Consider the sequence $\{b(t_1), t_1=0,1,\ldots,M-1\}$ of period $M = 2^m$-1 with ideal autocorrelation property, given by $[b(t_1) = \sum_{a\in I} tr_1^m(\alpha^{at_1})]$ for an index set I. It can be extended to a sequence $\{c(t_2), t_2=0,1,\ldots,N-1\}$ of period $N = 2^n$-1 with ideal autocorrelation property, defined by

$$c(t_2) = \sum_{a\in I} tr_1^m\{[tr_m^n(\beta^{t_2})]^{ar}\}$$

where $\beta=\gamma^{(2^k-1)/(2^n-1)}$ and r, $1\leq r\leq M-1$, is an integer relatively prime to M. Writing each trace term in $c(t_2)$ as

$$tr_1^m\{[tr_m^n(\beta^{t_2})]^{ar}\} = \sum_{j\in J(a)} tr_1^n(\beta^{jt_2}) \tag{10}$$

for some index set $J(a)$, the sequence $\{c(t_2)\}$ can be expressed as

$$c(t_2) = \sum_{a\in I}\sum_{j\in J(a)} tr_1^n(\beta^{jt_2}).$$

Applying Theorem 2 to $\{c(t_2)\}$, we have an extension $\{d'(t), t=0,1,\ldots,K-1\}$ of period $K=2^k-1$ with ideal autocorrelation property, given by

$$d'(t) = \sum_{a\in I}\sum_{j\in J(a)} tr_1^n([tr_n^k(\gamma^t)]^{js})$$

for an integer s, $1\leq s\leq N-1$, relatively prime to N. On the other hand, $d(t)$ can be expressed as

$$\begin{aligned} d(t) &= \sum_{a\in I} tr_1^m([tr_m^n\{[tr_n^k(\gamma^t)]^s\}]^{ar}) \\ &= \sum_{a\in I}\sum_{j\in J(a)} tr_1^n\{([tr_n^k(\gamma^t)]^s)^j\} \end{aligned}$$

using the relation in Eq. (10). Hence, $d(t)$ is exactly the same as $d(t)$.

It is interesting to find the number of cyclically distinct binary sequences of longer period with ideal autocorrelation property obtained by using Theorem 2. It is easily counted by considering cyclotomic cosets.

For an integer $M=2^m$-1, define the cyclotomic coset C_2 of an integer i, $0\leq i\leq M-1$, by $C_i=\{j \mid 0\leq j\leq M-1,$ and $j\equiv i2^l \bmod M$ for some integer $l\geq 0\}$.

For the sake of convenience, the cyclotomic coset representative of C_2 is often defined as the least integer of C_2. It is easily checked that either $C_i=C_j$ or $C_i\cap C_j=\phi$. Hence the set $\{0,1,\ldots,M-1\}$ is partitioned into pairwise disjoint cyclotomic cosets, that is,

$$\{0,1,\ldots,M-1\} = \bigcup_{i\in A} C_i$$

where A is the set of all the cyclotomic coset representatives. Note that

$$tr_1^m(x^j) = tr_1^m(x^i)$$

for any integer $j\in C_i$.

For an integer r and an index set I, define rI as

$$rI=\{j \mid 0\leq j\leq M-1, \text{and } j\equiv ri \bmod M \text{ for } i\in I\},$$

and define the set T_I of cyclotomic cosets associated with I as

$$T_I=\{C_a \mid a\in I\}.$$

Let N_I be the number of r's relatively prime to M such that $T_I\neq T_{rI}$, i.e.,

$$N_I=|\ \{r \mid \gcd(r,M)=1, \text{and } T_I\neq T_{rI}\}\ |. \tag{11}$$

Theorem 4 : Let m and n be positive integers such that $m \mid n$. Let α and β be primitive elements of F_{2^m} and F_{2^n}, respectively. Assume that for an index set I, the sequence $\{b(t_1), t_1=0,1,\ldots,M-1\}$ of period $M=2^m$-1 given by

$$b(t_1) = \sum_{a\in I} tr_1^m(\alpha^{at_1})$$

has the ideal autocorrelation property. Let N_{seq} be the number of cyclically distinct extensions $\{c(t), t=0,1,\ldots,N-1\}$ of period $N=2^n$-1 with ideal autocorrelation property, given by

$$c(t) = \sum_{a\in I} tr_1^m\{[tr_m^n(\beta^t)]^{ar}\},$$

where r, $1\leq r\leq M-1$, is relatively prime to M. Then we have

$$N_{seq} = N_I\,\frac{\varphi(N)}{n},$$

where $\varphi(\cdot)$ is the Euler's phi function and N_I is given in Eq. (11).

Proof : In order to evaluate the number of cyclically distinct extensions of period 2^m-1 constructed from $\{b(t_1)\}$, we need to count the number of choices for γ and r. The number of choices for γ is $\varphi(N)/n$, since γ^2 and γ^i give the same extension for any j in the cyclotomic coset mod N containing i. If $r_1I=r_2I$, then the extension associated with $r=r_1$ is exactly the same as the extension associated with $r=r_2$. Thus the number of choices for r is N_I, given by Eq. (11). Therefore, the number of cyclically distinct extensions of period N constructed from $\{b(t_1)\}$ is given by $N_{seq}=N_I\cdot\varphi(N)/n$.

Concluding Remarks : It is very important to find the linear span of a binary sequence in both theory and practice. So we have a very natural question: *What is the exact linear span of an extension of period $N=2^n$-1 with ideal autocorrelation property, if a binary sequence of period $M=2^m$-1 with ideal autocorrelation property has linear span L?* There is an answer for the m-sequences and the GMW sequences [14], but no others to the best knowledge of the authors.

Acknowledgement

This work was supported in part by the Korea Ministry of Information and Communications.

References

[1] L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics, Springer-Verlag, 1971.

[2] S. W. Golomb, "On the classification of balanced binary sequences of period 2^n-1," *IEEE Trans. Inform. Theory*, Vol. IT-26, pp. 730-732, Nov. 1980.

[3] S. W. Golomb, *Shift-Register Sequences*, Holden-Day, San Francisco, CA, 1967; Aegean Park Press, Laguna Hills, CA 1982.

[4] D. Jungnickel, "Difference sets," in Contemporary Design Theory, J. H. Dinitz and D. R. Stinson, Eds., John Wiley and Sons, Inc., pp. 241-324, 1992.

[5] A. Klapper, A. H. Chan, and M. Goresky, "Cascaded GMW sequences," IEEE Trans. Inform. Theory, Vol. IT-39, pp. 177-183, Jan. 1989.

[6] R. Lidl and H. Niederreiter, *Finite Fields*, Vol. 20 of Encyclopedia of Mathematics and Its Applications, Addison-Wesley, Reading, MA, 1983.

[7] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, 1977.

[8] J. -S. No, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," Ph.D. dissertation, Univ. of Southern California, Los Angeles, CA, May 1988.

[9] J.-S. No, "Generalization of GMW sequences and No sequences," IEEE Trans. Inform. Theory. Vol. 42, No. 1, pp. 260-262, Jan. 1996.

[10] J. -S. No and P. V. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," IEEE Trans. Inform. Theory, Vol. IT-35, pp. 371-379, Mar. 1989.

[11] J. -S. No, H. -K. Lee, H. Chung, H. -Y. Song, and K. Yang, "Trace representation of Legendre sequences of Mersenne prime period," IEEE Trans. Inform. Theory, Vol. 42, No. 6, Nov., 1996.

[12] Hyun-Seo Oh, Chae-Min Park, Seon-Ho Hwang, Chang-Eon Kang, and Jung-Young Son, "Coherent demodulation performance of pilot aided QPSK modulation in wideband CDMA reverse channel," J. of Elec. Engin. and Inform. Sci., A joint publication of KIEE, KITE, KISS, KICS, KEES, KIISC, and IEEE Korea, Vol. 2, No. 1, pp. 28-33, Feb. 1997.

[13] D. V. Sarwate and M. B. Pursley, "Crosscorrelation Properties of Pseudorandom and Related Sequences," Proc. IEEE, Vol. IT-68, pp. 593-619, May 1980.

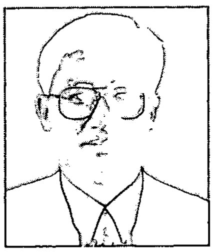
[14] R. A. Scholtz and L. R. Welch, "GMW sequences," IEEE Trans. Inform. Theory, Vol. IT-30, pp. 548-553, May 1984.

[15] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, Spread Spectrum Communications, Vol. 1, Computer Science Press, Rockville, MD, 1985.

[16] H. Y. Song and S. W. Golomb, "On the existence of cyclic Hadamard difference sets," IEEE Trans. Inform. Theory, Vol. IT-40, pp. 1266-1268, July 1994.

[17] Won Sik Yoon, "Concatenated orthogonal/PN spreading scheme for a multitone CDMA system," J. of Elec. Engin. and Inform. Sci., A joint publication of KIEE, KITE, KISS, KICS, KEES, KIISC, and IEEE Korea, Vol. 2, No. 4, pp. 19-22, August 1997.

Jong-Seon No was born in January 1, 1959, received his BS and MSEE degrees in Electronic Engineering from Seoul National University in 1981 and 1984, respectively, and Ph.D. degree from University of Southern California, Los Angeles, CA in 1988. He was a senior MTS at Hughes Network Systems from 1988 to 1990, and he joined the faculty members of the Dept. of Electronic Engineering, Konkuk University, Seoul, Korea in the september of 1990, where he is currently working as an associate professor. His area of research interest includes Error Correcting Codes, PN Sequences, Mobile Radio Communication, IMT-2000, Spread Spectrum Communication Systems.



Kyeong-Cheol Yang received the B.S. and M.S. degrees in Electronic Engineering from Seoul National University, Seoul, Korea, in 1986 and 1988, respectively, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, CA, in 1992. During the summer of 1990, he was with Bellcore, Morristown, NJ as an intern. Since 1993 he has been on the faculty of Hanyang University, Seoul, Korea, where he is currently an Assistant Professor in the Department of Electronic Communication Engineering. His research interests include Error-control Coding, Signal design for CDMA systems, and Cryptology.

Ha-Bong Chung received his B.S. degree in Electronic Engineering from Seoul National University in 1981, MSEE and Ph.D. degrees from University of Southern California, Los Angeles, CA in 1985 and 1988, respectively. He was an Assistant Professor in the Dept. ECE, State University of New York at Buffalo, from August 1988 to August 1991, and then he joined the faculty members of the Dept. of Electronic Engineering, Hong Ik University, Seoul, Korea in 1991. Since 1995, he is teaching and researching as an associate professor in Hong Ik University. His area of research interest includes Information Theory, Error- Correcting Codes, and Communication Theory.

Hong-Yeop Song received his B.S. degree in Electronic Engineering from Yonsei University in 1984, MSEE and Ph.D. degrees from University of Southern California, Los Angeles, CA in 1986 and 1991, respectively, specializing in the area of communication theory and coding. After spending 2 years as a research staff in the Communication Sciences Institute at USC working with Dr. Solomon W. Golomb, he joined Qualcomm Inc., San Diego, CA in 1994 as a senior engineer and worked in a team researching and developing North American CDMA Standards for PCS and cellular air-interface. He joined the Dept. of Electronic Engineering at Yonsei University, Seoul, Korea in 1995, and is currently working as an assistant professor. His area of research interest includes the application of discrete mathematics into various communication and coding problems. He is a member of IEEE, MAA(Mathematical Association of America), KITE, KICS, and KIISC.