Existence of Cyclic Hadamard Difference Sets and its Relation to Binary Sequences with Ideal Autocorrelation

Jeong-Heon Kim and Hong-Yeop Song

Abstract: Balanced binary sequences with ideal autocorrelation are equivalent to (v, k, λ)-cyclic Hadamard difference sets with $v = 4n - 1,\ k = 2n - 1,\ \lambda = n - 1$ for some positive integer n. Every known cyclic Hadamard difference set has one of the following three types of v : (1) $v = 4n - 1$ is a prime. (2) v is a product of twin primes. (3) $v = 2^n - 1$ for $n = 2,\ 3, \cdots$. It is conjectured that all cyclic Hadamard difference sets have parameter v which falls into one of the three types. The conjecture has been previously confirmed for $n < 10000$ except for 17 cases not fully investigated. In this paper, four smallest cases among these 17 cases are examined and the conjecture is confirmed for all $v \leq 3435$. In addition, all the inequivalent cyclic Hadamard difference sets with $v = 2^n - 1$ for $n \leq 10$ are listed and classified according to known construction methods.

Index Terms: Pseudorandom Binary Sequences, Ideal Autocorrelation, Cyclic Hadamard Difference Sets.

I. INTRODUCTION

A binary sequence $\{a(t)\}$ of period N is said to have the two-level ideal autocorrelation property if its autocorrelation function $R_a(\tau)$ satisfies the following:

$$R_a(\tau) = \begin{cases} N, & \text{if } \tau = 0 \bmod N, \\ -1, & \text{otherwise,} \end{cases}$$

where $R_a(\tau)$ is defined as

$$R_a(\tau) = \sum_{t=0}^{N-1} (-1)^{a_t + a_{t+\tau}}.$$

Binary sequences with the ideal autocorrelation are important because of their various applications to digital communication systems such as spread spectrum communication systems and code division multiple access (CDMA) systems [1].

It is well known that if a binary sequence has the two-level ideal autocorrelation, it must have a period N with $N = -1 (\text{mod } 4)$ and the numbers of ones and zeros differ by 1. Such a binary sequence is called a Hadamard sequence, and is equivalent to a cyclic Hadamard difference set with parameters $v = 4n - 1,\ k = 2n - 1,\ \lambda = n - 1$ for some integer $n \geq 2$. All known Hadamard sequences have periods of the following three types [2], [3]:

1. $N = 4n - 1$ is a prime number.
2. $N = p(p + 2)$ is a product of twin primes.
3. $N = 2^t - 1$, for $t = 2,\ 3,\ 4, \cdots$.

There is a conjecture that if a Hadamard sequence exists, the period N must be one of the above three types [4]. In [2], it is reported that there are no other values of $N < 1000$ with Hadamard sequences of period other than those listed above, except for the six cases $N = 399,\ 495,\ 627,\ 783$, and 975, which were not fully investigated. In [3], Song and Golomb reconfirmed the conjecture for all $N < 1000$ including these six cases. Furthermore, it was verified up to $N < 10000$, except for the following 17 cases: 1295, 1599, 1935, 3135, 3439, 4355, 4623, 5775, 7395, 7743, 8227, 8463, 8591, 8835, 9135, 9215, 9423. The conjecture becomes more and more interesting since there seems to be no immediate common property among the three types of v listed above and no counterexample has yet been discovered. In this paper, the four smallest previously unknown cases $v = 1295, 1599, 1935, 3135$ are examined and the conjecture is confirmed for all $v \leq 3435$.

Of three types of the period N, the case of $N = 2^n - 1$ owes its popularity to simple implementation. There has been a lot of effort to determine how many inequivalent Hadamard sequences of period $N = 2^n - 1$ there exist and to figure out how to construct them systematically. So far, full search for these sequences is completed up to $n = 10$.

II. NON-EXISTENCE OF SOME HADAMARD SEQUENCES

A Hadamard sequence of period $n = 4N - 1$ is known to be equivalent to a (v, k, λ)-cyclic difference set with $v = 4n - 1,\ k = 2n - 1,\ \lambda = n - 1$.

Definition 1: Given a positive integer v, let U denote the set of residues mod v. Let D be a k-subset of U. One calls D a (v, k, λ)-cyclic difference set if for any non-zero $d \in U$, there are exactly λ pairs of $(x,\ y),\ x,\ y \in D$ such that $d = (x - y) \bmod v$.

A (v, k, λ)-cyclic difference set with $v = 4n - 1, k = 2n - 1, \lambda = n - 1$ is called a cyclic Hadamard difference set and it induces a binary sequence of period $v = 4n - 1$ with the ideal

Manuscript received June 27, 1998; approved for publication by Jong S. No, Division I Editor, December 28, 1998.

The authors are with the Electronic Engineering Department of Yonsei University, Seoul, Korea, e-mail: heon@eve.yonsei.ac.kr and hysong@bubble.yonsei.ac.kr.

This work was supported by the Ministry of Information and Communication, Republic of Korea.

autocorrelation, i.e., a Hadamard sequence.

For a cyclic difference set $D = \{d_1, d_2, \cdots, d_k\}$, if there exist some s and t such that $\{td_1, td_2, \cdots, td_k\} = \{s + d_1, s + d_2, \cdots, s + d_k\}$, then the integer t is called a multiplier of D, and if $s = 0$, D is said to be fixed by t. Such a multiplier turns out to be very useful when one wants to exhaustively search for all the cyclic difference sets with a given set of parameters. The following theorem gives a sufficient condition on the existence of a multiplier of cyclic difference sets.

Theorem 1: [2] Let D be a (v, k, λ)-cyclic difference set. Let d be a divisor of $k - \lambda$ and suppose that $(d,\ v) = 1$ and $d > \lambda$. If t is an integer with the property that for each prime divisor p of d there is an integer j such that $p^j = t \bmod v$, then t is a multiplier of D.

Baumert[2] proved the following theorem which can be used to prove the non-existence of some cyclic Hadamard difference sets and can also be used to reduce the computational complexity of an exhaustive search.

Theorem 2: If a (v, k, λ)-cyclic difference set exists, then for every divisor w of v, there exist integers $b_i (i = 0,\ 1,\ 2, \cdots, w-1)$ satisfying the diophantine equations

$$\begin{aligned} &\sum_{i=0}^{w-1} b_i = k, \\ &\sum_{i=0}^{w-1} b_i^2 = k - \lambda + v\lambda/w, \\ &\sum_{i=0}^{w-1} b_i b_{i-j} = v\lambda/w, \qquad \text{for } 1 \le j \le w-1. \end{aligned} \tag{1}$$

Here, the subscript $i - j$ is taken modulo w.

Basic steps to reach the nonexistence is the following. We assume first that a cyclic Hadamard difference set D exists. By Theorem 1, its multiplier m can be determined. For every divisor w of v, its cyclotomic cosets can be determined by the multiplier m. We set some dummy indicators b_i for each cyclotomic coset. There must be some sets of b_i's satisfying the three diophantine equations in Theorem 2 if there exists a cyclic Hadamard difference set D. Thus, if these equations do not possess any solution for some divisor w, the non-existence is guaranteed.

A. Some Computations

If there exists a (1295,647,323)-cyclic Hadamard difference set D, it must have the multiplier 16 by Theorem 1. There are 155 cyclotomic cosets modulo 1295. One needs to consider the cyclotomic cosets modulo each divisor of 1295.

Since $1295 = 5 \times 7 \times 37$, if there exists a (1295, 647, 323)-cyclic Hadamard difference set D, there must be integers satisfying the three diophantine equations in Theorem 2 for each divisor 5, 7, 37, 35, 185, and 259. Otherwise, one can conclude that there is no (1295,647,323)-cyclic Hadamard difference set.

For the divisor $w = 5$, we have the following equations:

$$\begin{aligned} &\sum_{i=0}^{4} b_i = 647, \\ &\sum_{i=0}^{4} b_i^2 = 83981, \\ &\sum_{i=0}^{4} b_i b_{i-j} = 83657, \qquad \text{for } 1 \le j \le 4, \end{aligned} \tag{2}$$

and $0 \le b_i \le 255$. There are two solutions for b_i's satisfying (2), which are

$$(b_0,\ b_1,\ b_2,\ b_3,\ b_4) = \begin{cases} (115,\ 133,\ 133,\ 133,\ 133) \\ (133,\ 115,\ 133,\ 133,\ 133) \end{cases}$$

For the divisor $w = 7$, we have the following equations:

$$\begin{aligned} &\sum_{i=0}^{6} c_i = 647, \\ &\sum_{i=0}^{6} c_i^2 = 60079, \\ &\sum_{i=0}^{6} c_i c_{i-j} = 59755, \qquad \text{for } 1 \le j \le 6, \end{aligned} \tag{3}$$

and $0 \le c_i \le 175$. There are two solutions for c_i's satisfying (3), which are

$(c_0 = 77,\ c_1 = c_2 = c_4 = 95,\ c_3 = c_5 = c_6 = 95)$ and
$(c_0 = 104,\ c_1 = c_2 = c_4 = 86,\ c_3 = c_5 = c_6 = 95)$.

For the divisor $w = 37$, we have the following equations:

$$\begin{aligned} &\sum_{i=0}^{36} d_i = 647, \\ &\sum_{i=0}^{36} d_i^2 = 11629, \\ &\sum_{i=0}^{36} d_i d_{i-j} = 11305, \qquad \text{for } 1 \le j \le 36, \end{aligned} \tag{4}$$

and $0 \le d_0,\ d_1,\ \cdots,\ d_{36} \le 35$. There is only one solution.

$$\begin{aligned} &d_0 = 35, \\ &d_1 = d_7 = \cdots = d_{34} = 17, \\ &d_2 = d_{14} = \cdots = d_{32} = 17, \\ &d_3 = d_4 = \cdots = d_{36} = 17, \\ &d_5 = d_6 = \cdots = d_{35} = 17. \end{aligned}$$

For the divisor $w = 185$, we have the following equations:

$$\begin{aligned}
&\sum_{i=0}^{184} h_i = 647,\\
&\sum_{i=0}^{184} h_i^2 = 2585,\\
&\sum_{i=0}^{184} h_i h_{i-j} = 2261, \qquad \text{for } 1 \le j \le 184.
\end{aligned} \tag{5}$$

Here, we use another dummy indicator g_i which is related to h_i by the following equations:

$$\begin{aligned}
&g_0 = h_0,\\
&g_1 = h_{10} = h_{70} = \cdots = h_{160},\\
&g_2 = h_{15} = h_{20} = \cdots = h_{180},\\
&g_3 = h_{25} = h_{30} = \cdots h_{175},\\
&g_4 = h_5 = h_{35} = \cdots h_{170},\\
&g_5 = h_{111},\\
&g_6 = h_1 = h_{16} = \cdots = h_{181},\\
&g_7 = h_{31} = h_{51} = \cdots = h_{166},\\
&g_8 = h_{11} = h_{21} = \cdots = h_{176},\\
&g_9 = h_6 = h_{56} = \cdots = h_{171},\\
&g_{10} = h_{37},\\
&g_{11} = h_7 = h_{12} = \cdots = h_{182},\\
&g_{12} = h_2 = h_{32} = \cdots = h_{177},\\
&g_{13} = h_{27} = h_{62} = \cdots = h_{152},\\
&g_{14} = h_{17} = h_{22} = \cdots = h_{167},\\
&g_{15} = h_{148},\\
&g_{16} = h_{33} = h_{38} = \cdots = h_{158},\\
&g_{17} = h_{18} = h_{68} = \cdots = h_{168},\\
&g_{18} = h_3 = h_{28} = \cdots = h_{178},\\
&g_{19} = h_8 = h_{13} = \cdots = h_{183},\\
&g_{20} = h_{74},\\
&g_{21} = h_9 = h_{34} = \cdots = h_{174},\\
&g_{22} = h_{14} = h_{24} = \cdots = h_{179},\\
&g_{23} = h_4 = h_{64} = \cdots = h_{184},\\
&g_{24} = h_{19} = h_{54} = \cdots = h_{154},
\end{aligned}$$

and $0 \le g_i \le 7$ for $0 \le i \le 24$. In addition, since $185 = 5 \times 37$, g_i's are related to b_i's as follows:

$$\begin{aligned}
b_0 &= g_0 + 9(g_1 + g_2 + g_3 + g_4),\\
b_1 &= g_5 + 9(g_6 + g_7 + g_8 + g_9),\\
b_2 &= g_{10} + 9(g_{11} + g_{12} + g_{13} + g_{14}),\\
b_3 &= g_{15} + 9(g_{16} + g_{17} + g_{18} + g_{19}),\\
b_4 &= g_{20} + 9(g_{21} + g_{22} + g_{23} + g_{24}),
\end{aligned} \tag{6}$$

$$\begin{aligned}
d_0 &= g_0 + g_5 + g_{10} + g_{15} + g_{20},\\
d_1 &= g_1 + g_6 + g_{11} + g_{16} + g_{21},\\
d_2 &= g_2 + g_7 + g_{12} + g_{17} + g_{22},\\
d_3 &= g_3 + g_8 + g_{13} + g_{18} + g_{23},\\
d_4 &= g_4 + g_9 + g_{14} + g_{19} + g_{24}.
\end{aligned}$$

Recall that $(b_0,\ b_1,\ b_2,\ b_3,\ b_4)$ were already determined as (115, 133, 133, 133, 133) or (133, 115, 133, 133, 133) and $(d_0, d_1, d_2, d_3, d_4)$ were also determined as (35, 17, 17, 17, 17). By executing a series of C programs for a few hours of CPU time (Intel Pentium PC) collectively, we could confirm that there is no solution for g_i's satisfying both the diophantine equations (5) and the above relations (6). Thus, one can conclude that there does not exist a (1295, 647, 323)-cyclic Hadamard difference set.

Similarly, the three cases $v = 1599$, 1935, and 3135 can also be examined and it turns out that no cyclic Hadamard difference set with $v = 1599$, 1935, or 3135 exists. The result may be summarized as follows.

- For $v = 1599$
  1. Multiplier is 25.
  2. Number of cosets is 176.
  3. Number of solutions for $w = 3$ is 2.
  4. Number of solutions for $w = 41$ is 1.
  5. Number of solutions for $w = 3 \times 41 = 123$ is 0.
- For $v = 1935$
  1. Multiplier is 16.
  2. Number of cosets is 175.
  3. Number of solutions for $w = 3$ is 1.
  4. Number of solutions for $w = 43$ is 10.
  5. Number of solutions for $w = 3 \times 43 = 129$ is 0.
- For $v = 3135$
  1. Multiplier is 49.
  2. Number of cosets is 189.
  3. Number of solutions for $w = 3$ is 5.
  4. Number of solutions for $w = 5$ is 1.
  5. Number of solutions for $w = 3 \times 5 = 15$ is 0.

From all of the above results, the smallest open case now becomes $v = 3439$ which is very special. The above analysis of the four cases basically depends on the existence of a multiplier. For the case $v = 3439$, we do not have any method to determine a multiplier. So far, we are not even sure of the existence of a multiplier in this case. The remaining 12 cases up to $v < 10000$ have relatively many cosets and the ranges of the possible solutions to the diophantine equations are much wider than the previous four cases. These result in the huge increase of complexity. It seems impossible to finish the exhaustive search in a reasonable amount of time.

III. CLASSIFICATION OF CYCLIC HADAMARD DIFFERENCE SETS WITH $v = 2^n - 1$

In practical applications, Hadamard sequences of period $2^n - 1$ are most frequently used. Maximal length sequences, (m-sequences, in short) also belong to this family [5]. To describe Hadamard sequences of period $2^n - 1$, one can use the well-known trace function which is defined as follows [6]:

Definition 2: The trace function ${Tr_m}^n(\cdot)$ is a linear mapping from $GF(2^n)$ to $GF(2^m)$, with $m|n$, defined as

$${Tr_m}^n(\alpha) = \alpha + \alpha^{2^m} + \alpha^{2^{2m}} + \cdots + \alpha^{2^{m(n/m-1)}},$$

where $\alpha \in GF(2^n)$.

Any two Hadamard sequences $a(i)$ and $b(i)$ of the same period N are said to be equivalent if one can find integers d and s such that $a(i) = b(di+s)$ where $(d, N) = 1$ and $0 \le s \le N-1$.

Otherwise, we say that they are inequivalent. There have been some effort to determine the number of inequivalent Hadamard sequences of period $2^n - 1$ for each n, which implies the classification of cyclic Hadamard difference sets (CHDS) with $v = 2^n - 1$, since every CHDS with $v = 2^n - 1$ is equivalent to a Hadamard sequence of period $2^n - 1$ by the well-known correspondence that, for each $i = 0, 1, 2, \cdots, 2^n - 2$, $a(i) = 0$ if and only if $i \in D$. In this section, all the Hadamard sequences of period $2^n - 1$ for $n = 3, 4, \cdots, 10$ are classified and listed according to the known construction methods.

(7,3,1)-CHDS

There is only one (7,3,1)-CHDS. It is equivalent to an m-sequence which can be expressed as

$$s(t) = {Tr_1}^3(\alpha^t)$$

where α is a primitive element of $GF(2^3)$.

(15,7,3)-CHDS

There is only one (15,7,3)-CHDS. It is an m-sequence and its trace representation is

$$s(t) = {Tr_1}^4(\alpha^t)$$

where α is a primitive element of $GF(2^4)$.

(31,15,7)-CHDS

There are two inequivalent (31,15,7)-CHDS. Since 31 is a prime congruent to 3 mod 4, there must be a Legendre sequence of period 31. Let α be a primitive element of $GF(2^5)$.

☐ m31(m-sequence): $s(t) = {Tr_1}^5(\alpha^t)$.

☐ L31(Legendre sequence) [7]: $s(t) = {Tr_1}^5(\alpha^t + \alpha^{5t} + \alpha^{7t})$.

(63,31,15)-CHDS

There are two (63,31,15)-CHDS. Let α be a primitive element of $GF(2^6)$.

☐ m63(m-sequence): $s(t) = {Tr_1}^6(\alpha^t)$.

☐ G63(GMW-sequence) [8]: $s(t) = {Tr_1}^6(\alpha^t + \alpha^{15t})$.

(127,63,31)-CHDS

There are six (127,63,31)-CHDS [9]. Their trace representations are as follows where α is a primitive element of $GF(2^7)$.

☐ m127(m-sequence): $s(t) = {Tr_1}^7(\alpha^t)$.

☐ L127(Legendre sequence) [7]:

$$\begin{aligned} s(t) =& {Tr_1}^7(\alpha^t + \alpha^{9t} + \alpha^{11t} + \alpha^{13t} \\ &+ \alpha^{15t} + \alpha^{19t} + \alpha^{21t} + \alpha^{31t} + \alpha^{47t}). \end{aligned}$$

☐ H127(Hall's sextic residue sequence) [10]:

$$s(t) = {Tr_1}^7(\alpha^t + \alpha^{19t} + \alpha^{47t}).$$

☐ Miscellaneous sequences [11]–[13]:

- M127-1: $s(t) = {Tr_1}^7(\alpha^t + \alpha^{11t} + \alpha^{15t})$.
- M127-2: $s(t) = {Tr_1}^7(\alpha^t + \alpha^{3t} + \alpha^{7t} + \alpha^{19t} + \alpha^{29t})$.
- M127-3: $s(t) = {Tr_1}^7(\alpha^t + \alpha^{5t} + \alpha^{13t} + \alpha^{21t} + \alpha^{29t})$.

(255,127,63)-CHDS

There are four (255,127,63)-CHDS [14]. Their trace representations are as follows where α is a primitive element of $GF(2^8)$.

☐ m255 (m-sequence): $s(t) = {Tr_1}^8(\alpha^t)$.

☐ G255 (GMW-sequence) [8]:

$$s(t) = {Tr_1}^8(\alpha^t + \alpha^{19t} + \alpha^{53t} + \alpha^{91t}).$$

☐ Miscellaneous sequences [11]–[13]:

- M255-1: $s(t) = {Tr_1}^8(\alpha^t + \alpha^{11t} + \alpha^{19t} + \alpha^{27t} + \alpha^{87t})$.
- M255-2: $s(t) = {Tr_1}^8(\alpha^t + \alpha^{3t} + \alpha^{43t} + \alpha^{91t} + \alpha^{111t})$.

(511,255,127)-CHDS

There are five (511,255,127)-CHDS [15], [16]. Let α be a primitive element of $GF(2^9)$. Then the corresponding 5 binary sequences can be written as follows.

☐ m511(m-sequence): $s(t) = {Tr_1}^9(\alpha^t)$.

☐ G511(GMW-sequence) [8]:

$$s(t) = {Tr_1}^9(\alpha^t + \alpha^{11t} + \alpha^{43t}).$$

☐ Miscellaneous sequences [11]–[13], [16]:

- M511-1: $s(t) = {Tr_1}^9(\alpha^t + \alpha^{23t} + \alpha^{31t})$.
- M511-2:

$$\begin{aligned} s(t) =& {Tr_1}^9(\alpha^t + \alpha^{51t} + \alpha^{57t} \\ &+ \alpha^{83t} + \alpha^{111t} + \alpha^{125t} + \alpha^{183t}). \end{aligned}$$

- M511-3:

$$\begin{aligned} s(t) =& {Tr_1}^9(\alpha^t + \alpha^{7t} + \alpha^{57t} + \alpha^{77t} \\ &+ \alpha^{83t} + \alpha^{103t} + \alpha^{111t} + \alpha^{127t} + \alpha^{183t}). \end{aligned}$$

(1023,511,255)-CHDS

There are ten (1023,511,255)-CHDS [17], [18]. Let α be a primitive element of $GF(2^{10})$.

☐ m1023(m-sequence): $s(t) = {Tr_1}^{10}(\alpha^t)$.

☐ GMW-sequences [8]:

- G1023-1: $s(t) = {Tr_1}^{10}(\alpha^t + \alpha^{63t})$.
- G1023-2: $s(t) = {Tr_1}^{10}(\alpha^t + \alpha^{219t})$.
- G1023-3: $s(t) = {Tr_1}^{10}(\alpha^t + \alpha^{101t} + \alpha^{159t} + \alpha^{221t})$.
- G1023-4: $s(t) = {Tr_1}^{10}(\alpha^t + \alpha^{39t} + \alpha^{157t} + \alpha^{221t})$.
- G1023-5:

$$\begin{aligned} s(t) =& {Tr_1}^{10}(\alpha^t + \alpha^{39t} + \alpha^{47t} + \alpha^{63t} \\ &+ \alpha^{109t} + \alpha^{125t} + \alpha^{159t} + \alpha^{187t}). \end{aligned}$$

☐ Miscellaneous sequences [11]–[13]:

- M1023-1:

$$s(t) = {Tr_1}^{10}(\alpha^t + \alpha^{11t} + \alpha^{15t} + \alpha^{39t} + \alpha^{127t}).$$

- M1023-2:

$$\begin{aligned} s(t) =& {Tr_1}^{10}(\alpha^t + \alpha^{39t} + \alpha^{47t} + \alpha^{63t} \\ &+ \alpha^{109t} + \alpha^{125t} + \alpha^{159t} + \alpha^{187t}). \end{aligned}$$

- M1023-3:

$$s(t) = {Tr_1}^{10}(\alpha^t + \alpha^{41t} + \alpha^{47t} + \alpha^{63t} + \alpha^{87t} + \alpha^{125t} + \alpha^{205t}).$$

- M1023-4:

$$s(t) = {Tr_1}^{10}(\alpha^t + \alpha^{5t} + \alpha^{9t} + \alpha^{49t} + \alpha^{63t} + \alpha^{71t} + \alpha^{111t} + \alpha^{121t} + \alpha^{253t} + \alpha^{237t} + \alpha^{191t} + \alpha^{183t} + \alpha^{205t} + \alpha^{245t}).$$

REFERENCES

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

[2] L. D. Baumert, *Cyclic Difference Sets*, Springer-Verlag, New York, 1971.

[3] H.-Y. Song and S. W. Golomb, "On the existence of cyclic Hadamard difference sets," *IEEE Trans. Inform. Theory*, vol. 40, no. 4, pp. 1266–1268, July 1994.

[4] S. W. Golomb and H.-Y. Song, "A conjecture on the existence of cyclic Hadamard difference sets," *Journal of Statistical Planning and Inference*, vol. 62, pp. 39–41, 1997.

[5] S. W. Golomb, *Shift Register Sequences*, Holden-Day, San Francisco, CA(Revised Edition, Aegean Park Press, Laguna Hills, CA, 1982), 1967.

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

[7] J.-S. No, H.-K. Lee, H.-Y. Song, and K. Yang, "Trace representation of Legendre sequences of Mersenne prime period," *IEEE Trans. Inform. Theory*, vol. 42, no. 6, pp. 2254–2255, Nov. 1996.

[8] B. Gorden, W. H. Mills, and L. R. Welch, "Some new difference sets," *Canadian J. Math.*, vol. 14, pp. 614-625, 1962.

[9] L. D. Baumert and H. Fredricksen, "The cyclotomic numbers of order eighteen with applications to difference sets," *Math. Computation*, vol. 21, no. 98, pp. 204–219, 1967.

[10] H.-K. Lee, J.-S. No, H. Chung, K. Yang, J.-H. Kim, and H.-Y. Song, "Trace function representation of Hall's sextic residue sequences and some new sequences with ideal autocorrelation," in *Proceedings of APCC'97*, Dec. 1997, pp. 536–540.

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

[12] J.-S. No, H.-K. Lee, H. Chung, K. Yang, and H.-Y. Song, "On the classification of binary sequences of period $2^n - 1$ with ideal autocorrelation," in *Proceedings of ISIT*, 1997, p.42.

[13] 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*, vol. 44, no. 2, pp. 814–817, Mar. 1998.

[14] U. Cheng, "Exhaustive construction of (255,127,63)-cyclic difference sets," *J. Combinatorial Theory, Series A*, vol. 35, no. 2, pp. 115–125, Sep. 1983.

[15] R. Dreier, "(511,255,127)-cyclic difference sets," in *IDA Talk*, 1992.

[16] J.-H. Kim, *On the Binary Sequences of Period 511 with Ideal Autocorrelation*, M.S. thesis, Yonsei University, Korea, 1998.

[17] P. Gaal and S. W. Golomb, "Exhaustive determination of (1023,511,255)-cyclic difference sets," preprint, 1997.

[18] J.-H. Kim and H.-Y. Song, "Existence of Hadamard difference sets and its relation to binary sequences with ideal autocorrelation," in *Mathematical Theory of Networks and Systems*, Padova, Italy, July 1998, invited for presentation.

Jeong-Heon Kim was born in Gwang-Ju, Korea, in 1973. He received his B.S. and M.S. degrees from Yonsei University in 1996 and 1998, respectively. He is currently a Ph.D. candidate in the Department of Electronic Engineering, Yonsei University. His area of research interest includes application of pseudorandom sequences to mobile telecommunication systems and cryptographic systems.

Hong-Yeop Song received his BS 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, where he is currently an associate professor. His area of research interest includes application of discrete mathematics to various communication and coding problems. He is a member of IEEE, MAA(Mathematical Association of America), IEEK, KICS, and KIISC.