Trace Function Representation of Hall's Sextic Residue Sequences of Period $p \equiv 7 \pmod 8$ *

Jeong-Heon Kim
Samsung Electronics, Soowon 442-742, Korea
Email: jeongheon.kim@samsung.com

Hong-Yeop Song
Department of Electrical and Electronics Engineering
Yonsei University, Seoul 120-749, Korea
E-mail: hy.song@coding.yonsei.ac.kr

Guang Gong
Department of Electrical and Computer Engineering
University of Waterloo, Waterloo, Ontario, Canada
Email: ggong@cacr.math.uwaterloo.ca

Abstract

We determine the trace function representation of Hall's sextic residue sequences of period $p \equiv 7 \pmod 8$. Current status of a conjecture regarding the existence of Hadamard sequences is briefly discussed.

Keywords

Hall's Sextic Residue Difference Sets, PN Sequences, Cyclic Hadamard Difference Sets, Trace Functions.

I. INTRODUCTION

It is well known that, for an integer $v \equiv 3 \pmod 4$, a balanced binary sequence of period v with the ideal two-level autocorrelation function [4] exists if and only if a (v, k, λ)-cyclic Hadamard difference set (where $v = 4n - 1$, $k = 2n - 1$, and $\lambda = n - 1$ for some

* This work was performed while J.-H. Kim is with Department of Electrical and Electronics Engineering, Yonsei University, Seoul, Korea. H.-Y. Song is visiting University of Waterloo, Canada, from March 2002 to Feb 2003.

integer n) exists [1], [5]. There are only three types of integers $v \equiv 3 \pmod 4$ such that cyclic Hadamard difference sets are *known* to exist: (A) v is a prime, (B) v is a product of twin primes, and (C) v is one less than a power of 2 [1], [6], [18]. Numerical check for the non-existence of cyclic Hadamard difference sets have been done for all values $v \equiv 3 \pmod 4$ up to 10000 other than those listed above [1], [18], [11], and confirmed that none exists in this range with 13 possible exceptions of $v = 3439$, 4355, 4623, 5775, 7395, 7743, 8227, 8463, 8591, 8835, 9135, 9215, and 9423.

Those sequences of period $2^t - 1$ (belonging to (C) above) can easily be described using trace functions, while those of period v which is a prime or a product of twin primes (belonging to either (A) or (B) above) have been easily described using the construction of cyclic difference sets over the integers mod v. These are "Legendre" sequences, Hall's sextic residue sequences, and twin-prime sequences [1], [5], [8], [19]. Trace function representation of these sequences may enable one to implement the generation of them easily using linear feedback shift registers (LFSR). The minimum degree characteristic polynomials will determine the shortest number of stages (linear complexity) and the connection logic of LFSRs. For the definition and properties of trace functions and finite fields, see [15]. For the application of the sequences with ideal autocorrelation into various communication engineering and streamcipher, see [5], [7], [17].

The linear complexity and the characteristic polynomial of Legendre sequences have been reported in [20], and independently in [3]. Its trace representation for Mersenne prime period was reported in [16], and for the general case including $p \equiv 1 \pmod 4$ in [13]. The linear complexity and the characteristic polynomial of Jacobi sequences (generalization of twin-prime sequences) have been determined in [2].

Hall's sextic residue sequences [8], [1], [5] can be describe as follows. Let p be an odd prime of the form $p = 4x^2 + 27$ for some integer x. Then $p \equiv 1 \pmod 6$ and we may write it as $p = 6f + 1$ for some integer f. Let g be a primitive root modulo p such that $3 \in C_1$ where

$$C_l = \{g^{6i+l} \mid i = 0, 1, \ldots, f-1\}. \tag{1}$$

Then, Hall's sextic residue sequence $\{s(t)\}$ of period p is defined as [5]

$$s(t) = \begin{cases} 0 & \text{if } t \in C_0 \cup C_1 \cup C_3 \\ 1 & \text{otherwise} \end{cases} \tag{2}$$

where $t = 0, 1, 2, \ldots, p-1$. Note that the subset $D = C_0 \cup C_1 \cup C_3$ of the integers mod p is a (v, k, λ)-cyclic difference set with $v = p$, $k = (p-1)/2$, and $\lambda = (p-3)/4$, called Hall's sextic residue difference set [8].

Let

$$S(x) = s(0) + s(1)x + \cdots + s(p-1)x^{p-1} \tag{3}$$

be the polynomial over $GF(2)$ of degree at most $p-1$ whose coefficients are one period of the sequence $\{s(t)\}$, and let n be the order of 2 mod p. Then, there exists a primitive p-th root β of unity in $GF(2^n)$ such that $S(\beta) = 1$ and the minimum degree characteristic polynomial $c(x)$ of $\{s(t)\}$ is given by the following [12]:

$$c(x) = \begin{cases} \prod_{j \in C_0}(x - \beta^j) & \text{for } p \equiv 7 \pmod 8 \\ (x^p - 1)/(x-1) & \text{for } p \equiv 3 \pmod 8, \end{cases} \tag{4}$$

and hence, the linear complexity is given as $(p-1)/6$ and $p-1$ in each case, respectively.

Trace representation of Hall's sextic residue sequences was determined earlier for the Mersenne prime period cases. It is well-known that there are only 3 cases [10] of prime p which are both Mersenne prime and of type $4x^2 + 27$, which are 31, 127, and 131071. For these three cases, the trace representation was determined in [14] as follows: Let $p = 4x^2 + 27 = 6f + 1 = 2^n - 1$ be a prime, α be a primitive element of $GF(2^n)$, and hence a primitive p-th root of unity. Note that n is the order of 2 mod p in this case. Finally, let u be a primitive root mod p. Then, the sequence $\{s(t)\}$ in (2) for these Mersenne prime period can be written as

$$s(t) = \sum_{i=0}^{\frac{p-1}{6n}-1} \mathrm{tr}_1^n(\alpha^{u^{6i}t}), \tag{5}$$

where $\mathrm{tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$ is a trace function from $GF(2^n)$ to $GF(2)$. The above representation was confirmed as [14]

$$s(t) = \begin{cases} \mathrm{tr}_1^5(\alpha^t) & \text{for } p = 31, \\ \mathrm{tr}_1^7(\alpha^t) + \mathrm{tr}_1^7(\alpha^{19t}) + \mathrm{tr}_1^7(\alpha^{47t}) & \text{for } p = 127, \\ \sum_{i=0}^{1284} \mathrm{tr}_1^{17}(\alpha^{3^{6i}t}) & \text{for } p = 131071. \end{cases}$$

In this paper, we determine the trace representation of Hall's sextic residue sequences for $v = p \equiv 7 \pmod 8$. Section 2 describes the main result and its proof. Some brief concluding remarks are given in Section 3.

II. Main Result

Theorem 1 *(main) Let $p = 4x^2 + 27 = 6f + 1 \equiv 7 \pmod 8$ be a prime, g be a primitive root mod p such that $3 \in C_1$ where C_l is given in (1) for $l = 0, 1, ..., 5$. Let $S(x)$ be given in (3), i.e.,*

$$S(x) = C_2(x) + C_4(x) + C_5(x) + 1,$$

where

$$C_l(x) = \sum_{i \in C_l} x^i = \sum_{x=0}^{f-1} x^{g^{6x+l}} \quad \textit{for} \;\; l = 0, 1, 2, 3, 4, 5. \tag{6}$$

Let n be the order of 2 mod p. Then, there exists a primitive p-th root β of unity in $GF(2^n)$ such that $S(\beta^{-1}) = 1$, and the sequence given by

$$s(t) = \sum_{i=0}^{\frac{p-1}{6n}-1} tr_1^n(\beta^{g^{6i}t}), \tag{7}$$

for $t = 0, 1, 2, ..., p-1$ is the Hall's sextic residue sequence of period p given in (2).

To prove the theorem, we first note that the residue 3 belongs to C_1 or C_5 mod p for any primitive root g mod p [9]. If g puts 3 into C_5, then g^{-1} will put 3 into C_1. The residue -1 mod p belongs to C_3 [9]. Now we will present a series of lemmas to prove the theorem. In the following, p is the prime of the form given in the theorem, i.e., $p = 4x^2 + 27 = 6f + 1 \equiv 7 \pmod 8$, α is a primitive p-th root of unity in $GF(2^n)$, and n is the order of 2 mod p. The key idea is to observe the following.

Lemma 1 *The residue 2 mod p belongs to C_0, and we have*

$$C_0(x) = \sum_{i=0}^{\frac{p-1}{6n}-1} tr_1^n(x^{g^{6i}}),$$

where $C_0(x)$ is given in (6).

Proof: The residue 2 is both a quadratic residue and cubic residue mod p [9]. Therefore, $2 \in C_0$. The sextic residue class C_0 is a multiplicative subgroup of the non-zero integers mod p. If we let H_0 be its cyclic subgroup generated by 2, then

$$C_0 = \bigcup_{i=0}^{\frac{p-1}{6n}-1} g^{6i} H_0 = \bigcup_{i=0}^{\frac{p-1}{6n}-1} H_i,$$

is a disjoint union of cosets of H_0 in C_0, where we write $H_i = g^{6i} H_0$. If we write $H_i(x) = \sum_{j \in H_i} x^j$ for $i = 0, 1, ..., \frac{p-1}{6n} - 1$, then $H_0(x) = \sum_{j \in H_0} x^j = \sum_{i=0}^{n-1} x^{2^i} = \mathrm{tr}_1^n(x)$, and $H_i(x) = \mathrm{tr}_1^n(x^{g^{6i}})$. ∎

Therefore, the proof of the main theorem will be completed if we show that

$$C_0(\alpha^t) = 0 \iff t \in C_0 \cup C_1 \cup C_3, \tag{8}$$

for some primitive p-th root α of unity in $GF(2^n)$. To show (8), we need the following.

Lemma 2 *For any $l = 0, 1, ..., 5$, we have $C_l(\alpha^3) = C_{(l+1 \pmod 6)}(\alpha)$. In particular, we have $C_l(\alpha) = C_0(\alpha^{3^l})$ for each $l = 0, 1, 2, ..., 5$.*

Proof: Note that a primitive root g mod p was selected so that $3 \in C_1$. Therefore, $3 = g^{6m+1}$ for some m. Then,

$$C_l(\alpha^3) = \sum_{x=0}^{f-1} \alpha^{3g^{6x+l}} = \sum_{x=0}^{f-1} \alpha^{g^{6(m+x)+l+1}} = C_{(l+1 \pmod 6)}(\alpha).$$

■

Lemma 3 *If $t \in C_l$, then $C_0(\alpha^t) = C_l(\alpha)$.*

Proof: Lemma 2 implies that $C_l(\alpha) = C_0(\alpha^{3^l})$. Since $3 \in C_1$, we have $3^l \in C_l$. Therefore, $C_0(\alpha^{3^l}) = C_0(\alpha^t)$, since $C_l(\alpha^i) = C_l(\alpha^j)$ if i and j belong to the same sextic residue class. This can be seen from the following:

$$\begin{aligned} C_l(\alpha^i) &= \sum_{x=0}^{f-1} (\alpha^{g^{6a+k}})^{g^{6x+l}} \\ &= \sum_{x=0}^{f-1} \alpha^{g^{6(a+x)+k+l}} = \sum_{x=0}^{f-1} \alpha^{g^{6(b+x)+k+l}} = C_l(\alpha^j), \end{aligned}$$

where we use $i = g^{6a+k}$ and $j = g^{6b+k}$ for some a and b. ■

Therefore, the proof of the main theorem will be completed if we show that

$$C_l(\alpha) = 0 \iff l = 0, 1, 3, \tag{9}$$

for some primitive p-th root α of unity in $GF(2^n)$. The rest of the proof will verify (9).

Lemma 4 *For any $l = 0, 1, ..., 5$, we have $C_l(\alpha) \in GF(2)$, and hence, $S(\alpha) \in GF(2)$. Furthermore, we have $S(\alpha)S(\alpha^{-1}) = 0$.*

Proof: Note that it is sufficient to show that $C_l(\alpha)^2 = C_l(\alpha)$. Since $2 \in C_0$, we have $2C_l = C_l$ for any l, and hence

$$C_l(\alpha^2) = \sum_{i \in C_l} \alpha^{2i} = \sum_{i \in C_l} \alpha^i = C_l(\alpha).$$

On the other hand, over the field of characteristic 2, we have $C_l(\alpha^2) = C_l(\alpha)^2$.

For the second part, recall that $D = C_0 \cup C_1 \cup C_3$ is a $(v = p, k = (p-1)/2, \lambda = (p-3)/4)$-cyclic difference set, and its complement $\overline{D} = Z_p \backslash D$ is a $(\overline{v} = p, \overline{k} = (p+1)/2, \overline{\lambda} = (p+1)/4)$-cyclic difference set. Since $S(x) = \sum_{i \in \overline{D}} x^i$, we have [1]

$$S(x)S(x^{-1}) \equiv (\overline{k} - \overline{\lambda}) + \overline{\lambda} \sum_{i=0}^{p-1} x^i \pmod{x^p - 1},$$

or

$$S(\alpha)S(\alpha^{-1}) = \frac{p+1}{4} = 0,$$

since $p \equiv 7 \pmod 8$. ■

To complete the proof of the main theorem, we need the primitive p-th root β of unity in $GF(2^n)$ that will now be shown to exist such that $S(\beta^{-1}) = 1$. In the remaining of the proof after Lemma 5, we use this $\beta \in GF(2^n)$.

Lemma 5 *There exists a primitive p-th root β of unity in $GF(2^n)$ such that $S(\beta^{-1}) = 1$.*

Proof: If we show that $\sum_{i=1}^{p-1} S(\alpha^i) = 1$ for any primitive p-th root α of unity in $GF(2^n)$, then Lemma 4 implies that $S(\alpha^j) = 1$ for at least one j. Since $\alpha^j = \gamma$ is also a primitive p-th root of unity, we have found a primitive p-th root γ such that $S(\gamma) = 1$. Now, $\beta = \gamma^{-1}$ is the desired primitive p-th root of unity in $GF(2^n)$ such that $S(\beta^{-1}) = 1$.

Now, since $f = (p-1)/6$ is odd, we have

$$\begin{aligned}
\sum_{i=1}^{p-1} S(\alpha^i) &= \sum_{l=0}^{5} \sum_{x=0}^{f-1} S(\alpha^{g^{6x+l}}) \\
&= \sum_{l=0}^{5} \sum_{x=0}^{f-1} \left[C_2(\alpha^{g^{6x+l}}) + C_4(\alpha^{g^{6x+l}}) + C_5(\alpha^{g^{6x+l}}) + 1 \right] \\
&= \sum_{l=0}^{5} \left[C_2(\alpha^{g^l}) + C_4(\alpha^{g^l}) + C_5(\alpha^{g^l}) \right],
\end{aligned}$$

where we use the fact that $C_l(\alpha^i) = C_l(\alpha^j)$ if i and j belong to the same sextic residue class. Since g^l and 3^l belong to the same sextic residue class, we have

$$\sum_{i=1}^{p-1} S(\alpha^i) = \sum_{l=0}^{5} \left[C_2(\alpha^{g^l}) + C_4(\alpha^{g^l}) + C_5(\alpha^{g^l}) \right]$$

$$= \sum_{l=0}^{5} \left[C_2(\alpha^{3^l}) + C_4(\alpha^{3^l}) + C_5(\alpha^{3^l}) \right].$$

Note that Lemma 2 implies that, for any k,

$$\sum_{l=0}^{5} C_k(\alpha^{3^l}) = \sum_{x=0}^{5} C_x(\alpha).$$

Therefore,

$$\begin{aligned} \sum_{i=1}^{p-1} S(\alpha^i) &= \sum_{l=0}^{5} \left[C_2(\alpha^{3^l}) + C_4(\alpha^{3^l}) + C_5(\alpha^{3^l}) \right] \\ &= \sum_{x=0}^{5} [C_x(\alpha) + C_x(\alpha) + C_x(\alpha)] \\ &= \sum_{x=0}^{5} C_x(\alpha) = \sum_{i=1}^{p-1} \alpha^i = 1. \end{aligned}$$

■

Lemma 6 *$C_0(\beta) + C_3(\beta)$, $C_1(\beta) + C_4(\beta)$, and $C_2(\beta) + C_5(\beta)$ cannot all be* 1.

Proof: Suppose they all be equal to 1. From Lemma 2, we then have

$$\begin{aligned} 1 &= C_2(\beta) + C_5(\beta) = C_1(\beta^3) + C_4(\beta^3), \\ 1 &= C_0(\beta) + C_3(\beta) = C_4(\beta^{3^2}) + C_1(\beta^{3^2}), \\ 1 &= C_1(\beta) + C_4(\beta). \end{aligned}$$

Furthermore,

$$C_1(\beta^{3^3}) + C_4(\beta^{3^3}) = C_4(\beta) + C_1(\beta) = 1.$$

Therefore, the equation

$$C_1(x) + C_4(x) + 1 = 0 \tag{10}$$

has roots β^{3^i} for $i = 0, 1, 2, \ldots$. Since $3 \in C_1$, it is easy to see that $3^i \in C_i$ for all i, and therefore, the roots of (10) are β^j for $j \in Z_p^* = \bigcup_{l=0}^{5} C_l$, since $C_l(\beta^i) = C_l(\beta^j)$ if i and j belong to the same sextic residue class. But the equation (10) does not have the term x^{p-1} since $-1 \in C_3$, and hence it has degree *strictly* less than $p-1$. ■

Corollary 1 *Exactly one of the three expressions* $C_0(\beta)+C_3(\beta)$, $C_1(\beta)+C_4(\beta)$, *and* $C_2(\beta)+C_5(\beta)$ *is* 1, *and the other two are* 0.

As a final step of computation, we determine the values of $C_l(\beta)$ for $l = 0, 1, ..., 5$, (with β such that $S(\beta^{-1}) = 1$) using Lemma 2, Lemma 4, and Corollary 1.

From Lemma 4, since $S(\beta^{-1}) = 1$, one must have $S(\beta) = 0$. Therefore,

$$\begin{aligned} 0 = S(\beta) &= C_2(\beta) + C_4(\beta) + C_5(\beta) + 1, \quad (11) \\ 1 = S(\beta^{-1}) &= C_2(\beta^{-1}) + C_4(\beta^{-1}) + C_5(\beta^{-1}) + 1 \\ &= C_2(\beta^{3^3}) + C_4(\beta^{3^3}) + C_5(\beta^{3^3}) + 1 \\ &= C_5(\beta) + C_1(\beta) + C_2(\beta) + 1. \quad (12) \end{aligned}$$

From (11) and (12), we have

$$C_1(\beta) + C_4(\beta) = 1. \quad (13)$$

Corollary 1, therefore, implies that

$$\begin{aligned} C_0(\beta) + C_3(\beta) &= 0, \quad (14) \\ C_2(\beta) + C_5(\beta) &= 0. \quad (15) \end{aligned}$$

Substituting (15) into (11) and (12) gives

$$C_1(\beta) = 0 \text{ and } C_4(\beta) = 1.$$

Next, observe that

$$\begin{aligned} S(\beta^3) &= C_1(\beta) + C_3(\beta) + C_4(\beta) + 1 = C_3(\beta), \\ S(\beta^{-3}) = S(\beta^{3^4}) &= C_4(\beta) + C_0(\beta) + C_1(\beta) + 1 = C_0(\beta). \end{aligned}$$

Therefore,

$$0 = S(\beta^3)S(\beta^{-3}) = C_3(\beta)C_0(\beta),$$

and (14) implies therefore that

$$C_0(\beta) = 0 \text{ and } C_3(\beta) = 0.$$

Similarly, we have

$$C_2(\beta) = 1 \text{ and } C_5(\beta) = 1.$$

Finally, for $t = 0$, we have

$$C_0(\beta^0) = C_0(1) = |C_0| = \frac{p-1}{6} = f = 1,$$

since $p = 6f + 1 = 4x^2 + 27$ and f is odd. This completes the proof of the main theorem.

III. Concluding Remarks

Remark 1. It is known that any $d_0 \in C_0$ is a multiplier of the underlying difference set [8]. In fact, it can be confirmed from the trace representation that $s(d_0 t) = s(t)$ for all t if $d_0 \in C_0$. In particular, 2 is a multiplier, since $2 \in C_0$ when $p \equiv 7 \pmod 8$. Note that $2 \in C_3$ when $p \equiv 3 \pmod 8$.

On the other hand, the proof of the main theorem will be simpler if we use two facts that (i) 2 is a multiplier [8] and (ii) the minimal polynomial $c(x)$ of the sequence for $p \equiv 7 \pmod 8$ is given in (4) [12]. Then, Lemma 1 implies that

$$c(x) = \prod_{j \in C_0} (x - \beta^j) = \prod_{i=0}^{f-1} (x - \beta^{g^{6i}}) = \prod_{i=0}^{f/n-1} M_{\beta^{g^{6i}}},$$

where $f = (p-1)/6$, and $M_\alpha(x)$ is the minimal polynomial of α over $GF(2)$. Since $\beta^{g^{6i}}$ has order n for all i from 0 to $f/n - 1$, we have factored $c(x)$ into the product of f/n minimal polynomials all of degree n. Now, the fact that 2 is a multiplier implies the trace representation in the main theorem. The proof in the previous section was done without using these two facts. ■

Remark 2. Observe that $\{s(d_i t)\} = \{s(d_j t)\}$ for all t if and only if d_i and d_j belong to the same sextic residue class. Therefore, there are exactly 6 cyclically distinct decimations of $\{s(t)\}$, each obtained by d_l-decimation where $d_l \in C_l$ for $l = 0, 1, 2, ..., 5$. ■

Remark 3. Trace representation of Hadamard sequences is *not known* only for (1) HSR sequences of period $p \equiv 3 \pmod 8$ and (2) twin-prime sequences of period $p(p+2)$ where both p and $p+2$ are prime. On the other hand, the linear complexity and the minimal polynomial of all the known Hadamard sequences are known. Whether or not a Hadamard sequence of period v exist only for those three types (A), (B), and (C) of v listed in Introduction is still open, with the smallest unsettled case $v = 3439$. ■

References

[1] L. D. Baumert, *Cyclic Difference Sets*, Lecture notes in mathematics, vol. 182, Springer-Verlag, New York, 1971.

[2] C. Ding, "Linear complexity of generalized cyclotomic binary sequences of order 2," *Finite Fields and Their Applications*, vol. 3, no. 2, pp. 159-174, 1997.

[3] C. Ding, T. Helleseth, and W. Shan, "On the Linear Complexity of Legendre Sequences," *IEEE Transactions on Information Theory* vol. 44, no. 3, pp. 1276-1278, 1998.

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

[5] S. W. Golomb, "Construction of Signals with Favourable Correlation Properties," in *Survey in Combinatorics*, A. D. Keedwell, Editor; LMS Lecture Note Series 166, Cambridge University Press, pp. 1-40, 1991.

[6] 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.

[7] G. Gong, *Lecture Notes on Sequence Design and Analysis*, pre-print, http://calliope.uwaterloo.ca/∼ggong, 2000.

[8] M. Hall Jr., "A Survey of Difference Sets," *Proc. Amer. Math. Soc.*, vol. 7, pp. 975-986, 1956.

[9] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, second edition, 1990.

[10] Dieter Jungnickel, "Difference Sets," in *Contemporary Design Theory* edited by J. H. Dinitz and D. R. Stinson, pp. 241-324, John Wiley & Sons, Inc., New York, 1992.

[11] J. -H. Kim and H. -Y. Song, "Existence of Cyclic Hadamard Difference Sets and its Relation to Binary Sequences with Ideal Autocorrelation," Journal of Communications and Networks, vol. 1, no.1, pp. 14-18, March 1999.

[12] J. -H. Kim and H. -Y. Song, "On the linear complexity of hall's sextic residue sequences," *IEEE Transaction on Information Theory*, vol. 47, no. 5, pp. 2094–2096, June 2001.

[13] J. -H. Kim and H. -Y. Song, "Trace Representation of Legendre Sequences," *Designs,Codes and Cryptography*, vol. 24, no. 3, pp. 343-348, December 2001.

[14] 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*. APCC, Dec. 1997, pp. 536–540.

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

[16] J. -S. No, H. -K. Lee, H. Chung, H. -Y. Song and K. Yang, "Trace Representation of Legendre Sequences of Mersenne Prime Period," *IEEE Transactions on Information Theory*, vol. 42, no. 6, pp. 2254-2255, Nov. 1996.

[17] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*, Computer Science Press, Rockville, MD, 1985; revised edition, McGraw-Hill, 1994.

[18] 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.

[19] R. G. Stanton and D. A. Sprott, "A Family of Difference Sets," *Canadian Journal of Mathematics*, vol. 10, pp. 73-77, 1958.

[20] R. Turyn, "The linear generation of the Legendre sequences," *Journal of Soc. Ind. Appl. Math.*, vol. 12, no. 1, pp. 115-117, 1964.