Trace Representation of Legendre Sequences of Mersenne Prime Period

Jong-Seon No*, Hwan-Keun Lee*, Habong Chung**,
Hong-Yeop Song***, and Kyeongcheol Yang****
* Dept. of Electronic Engineering, Konkuk University
** Dept. of Electronic Engineering, Hong-Ik University
*** Dept. of Electronic Engineering, Yonsei University
**** Dept. of Electronic Comm. Eng., Hanyang University

머센 소수의 주기를 가지는 르장드르 수열의 트레이스 표현

노 종 선*, 이 환 근*, 정 하 봉**, 송 홍 엽***, 양 경 철****
* 건국대학교 전자공학과
** 홍익대학교 전자공학과
*** 연세대학교 전자공학과
**** 한양대학교 전자통신공학과

ABSTRACT

In this paper, it is shown that "Legendre" sequences of period p In this paper, it is shown that "Legendre" sequences of period p can be explicitly represented using the trace function over the finite field with 2^n elements, whenever $p = 2^n - 1$ is prime for some $n \geq 3$.

1. INTRODUCTION

Balanced binary sequences of period $2^n - 1$ [2, 3] for some integer n having the two-level autocorrelation function [6] find many applications in digital spread spectrum communication systems [5]. Some of the well-known families of these sequences include: (1) m-sequences of period $2^n - 1$ for all $n = 1, 2, \cdots$; (2) GMW sequences of period $2^n - 1$ for composite values of n; and (3) "Legendre" sequences of period $2^n - 1$ whenever $2^n - 1$ is a prime (so called, Mersenne prime). The m-sequences and the GMW sequences are best described in terms of the trace function over a finite field [5].

In fact, "Legendre" sequences of period p for any prime p are defined as

$$b(t) = \begin{cases} 1 & \text{if } t = 0 \mod p, \\ 0 & \text{if } t \text{ is a quadratic residue mod } p, \\ 1 & \text{if } t \text{ is a quadratic non-residue mod } p, \end{cases} \quad (1)$$

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

and it is not difficult to show that $b(t)$ for $t = 0, 1, 2, \cdots, p-1$ has the two-level autocorrelation function if and only if $p = 3 \pmod 4$. These sequences have only been described as above, and it seems to be quite hard to find any simple connection between the description given in Eq.(1) for all primes $p = 3 \pmod 4$ and the trace function over a finite field.

In this paper, we show that, whenever $2^n - 1 = p$ is prime for some $n \geq 3$, "Legendre" sequences of period $2^n - 1$ can be explicitly described using the trace function over the finite field with 2^n elements.

2. MAIN THEOREM

For the remaining of this paper, we use the convention that $2^n - 1 = p$ is a prime for some $n \geq 3$, u is a primitive element of Z_p which is the set of integers mod p, F_{2^n} is the finite field with 2^n elements, and α is a primitive element of F_{2^n}.

The trace function $\mathrm{tr}_1^n(\cdot)$ is a mapping from F_{2^n} to its subfield $F_2 = \{0, 1\}$ given by

$$\mathrm{tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}. \qquad (2)$$

When $2^n - 1 = p$ is a prime, the cyclotomic coset C_t containing a nonzero $t \in Z_p$ consists of n elements and is given as $\{t, 2t, 2^2t, \cdots, 2^{n-1}t\}$ [3]. Thus, there are $(p-1)/n$ distinct cyclotomic cosets mod p of size n, and $\mathrm{tr}_1^n(x^t)$ is nothing but the sum of x^i over $i \in C_t$ for any $x \in F_{2^n} \backslash \{0, 1\}$ and any nonzero $t \in Z_p$. From the definition of the trace funtion above, it is easy to check that $\mathrm{tr}_1^n(\beta) = \mathrm{tr}_1^n(\beta^2)$ for any $\beta \in F_{2^n}$ [4]. Therefore, we conclude that $\mathrm{tr}_1^n(x^i) = \mathrm{tr}_1^n(x^t)$ if and only if $i \in C_t$. We also have that C_t consists entirely of either quadratic residues or non-residues mod p, since 2 is always a quadratic residue mod p of the form $2^n - 1$ for $n \geq 3$ [1].

Since $2^n - 1 = p$ is a prime for some $n \geq 3$, n must also be a prime and hence it is necessarily an odd integer. Therefore, we note that $\frac{(p-1)}{n}$ is an even integer. It is not hard to show that if u is primitive in Z_p, then u^i for each i from 0 to $\frac{(p-1)}{n} - 1$ runs through all the $(p-1)/n$ cyclotomic cosets of size n mod p. Furthermore, we need the following lemma saying that $u^{\frac{p-1}{n}}$ belongs to C_1 for any primitive element u in Z_p.

Lemma 1 *Let $p = 2^n - 1$ be prime and u be a primitive element in Z_p. Then we have $u^{\frac{p-1}{n}} = 2^i$ for some integer i.*

Proof: Note that 2^i is a solution to $x^n - 1 = 0 \pmod p$ for any integer i from 0 to $n-1$, and there are no other solutions because $p = 2^n - 1$ is prime. Since $(u^{\frac{p-1}{n}})^n = 1 \pmod p$, we have that $u^{\frac{p-1}{n}}$ must be of the form 2^i for some integer i. □

Lemma 2 *Let $2^n - 1 = p$ be a prime for some integer $n \geq 3$ and u be a primitive element of Z_p, the set of intgers mod p. Then, either α or α^u (not both) satisfies the equation in x given by*

$$\sum_{i=0}^{\frac{p-1}{2n}-1} \mathrm{tr}_1^n(x^{u^{2i}}) = 0.$$

Proof: Let

$$f(x) = \sum_{i=0}^{\frac{p-1}{2n}-1} \mathrm{tr}_1^n(x^{u^{2i}}) = \sum_{j \in \mathrm{QR}} x^j$$

where QR denotes the set of quadratic residues mod p. Then

$$f(x^u) = \sum_{i=0}^{\frac{p-1}{2n}-1} \mathrm{tr}_1^n(x^{u^{2i+1}}) = \sum_{j \in \mathrm{QN}} x^j$$

where QN denotes the set of quadratic non-residues mod p. Therefore,

$$f(x) + f(x^u) = \sum_{j=1}^{2^n-2} x^j = 1 + \sum_{j=0}^{2^n-2} x^j = 1$$

for all the nonzero elements $x \in F_{2^n}$ except for 1. Therefore, we have $f(\alpha) + f(\alpha^u) = 1$ for any primitive α in F_{2^n}. This implies that either $f(\alpha) = 0$ or $f(\alpha^u) = 0$. □

Now, we are in a position to state and prove our main theorem:

Main Theorem *Let $p = 2^n - 1$ be a prime for some integer $n \geq 3$ and u be a primitive element of Z_p, the set of intgers mod p. Let α be a primitive element of F_{2^n} such that*

$$\sum_{i=0}^{\frac{p-1}{2n}-1} \mathrm{tr}_1^n(\alpha^{u^{2i}}) = 0. \tag{3}$$

Then the sequence $s(t)$ for $t = 0, 1, 2, \ldots, p-1$ of period p given by

$$s(t) = \sum_{i=0}^{\frac{p-1}{2n}-1} \mathrm{tr}_1^n(\alpha^{u^{2i}t}) \tag{4}$$

is the "Legendre" sequence given in Eq.(1).

Proof: Since $2^n - 1 = p > 3$ is a prime, if $\alpha \in F_{2^n}$ is primitive, then α^j for every j from 1 to $p-2$ is also primitive. Therefore, by changing the name if necessary, the existence of a primitive element $\alpha \in F_{2^n}$ satisfying Eq.(3) is guaranteed by Lemma 2. This, in turn, gives $s(1) = 0$.

Since both n and $\frac{p-1}{2n}$ are odd, we have $\mathrm{tr}_1^n(1) = 1$, and hence, $s(0) = 1$.

If t is a quadratic residue mod p, we get $t = u^{2j}$ for some integer j. Therefore,

$$s(t) = s(u^{2j}) = \sum_{i=0}^{\frac{p-1}{2n}-1} \mathrm{tr}_1^n(\alpha^{u^{2(i+j)}}).$$

Since $\frac{p-1}{2n} = 2^l$ for some integer l by Lemma 1 and $\mathrm{tr}_1^n(\beta) = \mathrm{tr}_1^n(\beta^2)$ for any $\beta \in F_{2^n}$, it is easily checked that as i runs 0 to $\frac{p-1}{2n} - 1$, so does $i+j$. This implies that for any quadratic residue t mod p

$$s(t) = \sum_{k=0}^{\frac{p-1}{2n}-1} \mathrm{tr}_1^n(\alpha^{u^{2k}}) = s(1) = 0,$$

where the last equality comes from the choice of α.

If t is a quadratic non-residue mod p, we get $t = u^{2j+1}$ for some integer j. In this case, similarly, we have $s(t) = s(u)$ where u is a primitive element of Z_p. Since

$$s(1) + s(u) = \sum_{i=1}^{2^m-2} \alpha^j = 1,$$

we get $s(u) = 1$. □

Example: Let $n = 7$ and thus $p = 127 (= 2^7 - 1)$. It is easy to check that $u = 3$ is a primitive element in Z_{127}. Let α be the primitive element of F_{2^7} satisfying $\alpha^7 + \alpha^4 + 1 = 0$. Then we have

$$\sum_{i=0}^{\frac{p-1}{2n}-1} \mathrm{tr}_1^n(\alpha^{u^{2i}}) = \sum_{i=0}^{8} \mathrm{tr}_1^7(\alpha^{3^{2i}}) = 0.$$

The sequence $s(t)$ for t from 0 to 126 given by

$$s(t) = \sum_{i=0}^{8} \mathrm{tr}_1^7(\alpha^{3^{2i}t}) = \sum_{i=0}^{8} \mathrm{tr}_1^7(\alpha^{9^i t})$$

is the Legendre sequence of period 127.

Remark (1) The characteristic polynomial $h(x)$ of the Legendre sequence $s(t)$ of Mersenne prime priod $p = 2^n - 1 > 3$ is

$$h(x) = \prod_{i=0}^{\frac{p-1}{2n}-1} m_{\alpha^{u^{2i}}}(x)$$

where $m_{\alpha^j}(x)$ is the minimal polynomial of α^j over F_2.

(2) The linear span of $s(t)$ is exactly $\frac{p-1}{2} = 2^{n-1} - 1$.

(3) The sequence $s(t)$ is invariant under the decimation by u^{2i}, that is,

$$s(t) = s(u^{2i}t)$$

for any integer i.

References

[1] D. M. Burton, *Elementary Number Theory*, Allyn and Bacon, Inc., 1980.

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

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

[6] 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.