Trace Representation of Legendre Sequences of Mersenne Prime Period

Jong-Seon No, Hwan-Keun Lee, Habong Chung, *Member, IEEE*, Hong-Yeop Song, *Member, IEEE*, and Kyeongcheol Yang, *Member, IEEE*

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

***Index Terms*—Legendre sequences, m-sequences, two-level autocorrelation property.**

I. 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 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 (a 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

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

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 $p = 3 (\bmod 4)$. These sequences have only been described as above, and it seems to be meaningful to find any simple connection between the description given in (1) for all primes $p = 3 (\bmod 4)$ and the trace function over a finite field.

In this correspondence, 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 defined on the finite field with 2^n elements.

II. Main Theorem

For the remainder of this correspondence, 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}.

Manuscript received April 11, 1996; revised June 10, 1996. This work was supported in part by the Korea Science and Engineering Foundation (KOSEF) under Grant 951-0913-074-2 and in part by the Korean Ministry of Information and Communications.

J.-S. No and H.-K. Lee are with the Department of Electronic Engineering, Konkuk University, Seoul 143-701, Korea.

H. Chung is with the School of Electronic and Electrical Engineering, Hong-Ik University, Seoul 121-791, Korea.

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

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

Publisher Item Identifier S 0018-9448(96)07293-8.

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

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

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 function 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 nonresidues mod p, since 2 is always a quadratic residue mod p of the form $2^n - 1$ for $n \geq 3$ [1, p. 198].

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 $x^n - 1 = 0 (\bmod p)$ for any integer i from 0 to $n-1$, and there are no other solutions because $p = 2^n - 1$ is prime. Since $(u^{\frac{p-1}{n}})^n = 1 (\bmod p)$, 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 integers mod p. Then, either α or α^u (not both) satisfies the equation in x given by

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

Proof: Let

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

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

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

where QN denotes the set of quadratic nonresidues 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 integers mod p. Let α be a primitive element of F_{2^n} such that

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

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

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

is the Legendre sequence given in (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 (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. In this case

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

This is because, as i runs from 0 to $\frac{p-1}{2n}-1$ in the above summations, both u^{2i} and $u^{2(i+j)}$ run through the same set of cyclotomic cosets, consisting entirely of quadratic residues mod p.

If t is a quadratic nonresidue 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

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

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

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

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

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

is the Legendre sequence of period 127.

Remarks:

1) The characteristic polynomial $h(x)$ of the Legendre sequence $s(t)$ of Mersenne prime period $p = 2^n - 1 > 3$ 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, no. 6, pp. 730–732, Nov. 1980.

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

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

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

[6] 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.

A Characterization of Codes with Extreme Parameters

A. Faldum and W. Willems

***Abstract*— Let C be an $[n, k, d]$-code over GF(q) with $k \geq 2$. Let $s = \mathrm{def}(C) = n+1-k-d$ denote the defect of C. The Griesmer bound implies that $d \leq q(s+1)$. If $d > qs$ and $s \geq 2$, then using a previous result of Faldum and Willems, $k \leq q$. Thus fixing $s \geq 2$ the extreme parameters for a code with def$(C) = s$ are $d = q(s+1)$, $k = q$, and $n = k + d + s - 1 = (q+1)(s+2) - 3$. In this correspondence we characterize the codes with such parameters.**

***Index Terms*— Linear code, elliptic quadric surface, defect of codes, weight distribution.**

I. Introduction

Let C be an $[n, k, d]$-code over the field GF(q) with $k \geq 2$. Furthermore, let $s = \mathrm{def}(C) = n + 1 - k - d$ denote the defect of C. By the Griesmer bound

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$$

we immediately get that $d \leq q(s+1)$. From now on we suppose that d is maximal, i.e., $d = q(s+1)$.

If $s = 0$, then by the same argument as above used for the dual code $C^\perp$, we obtain $k \leq q - 1$. For the extreme parameters $n = 2q - 2$, $k = q - 1$, and $d = q$, codes only exist for $q = 3$ and $q = 4$, by [4, ch. 11, sec. VIII, Theorem 13]. Clearly, these are the ternary

Manuscript received May 9, 1995; revised April 24, 1996. The material in this correspondence was presented in part at the Confernce on Optimal Codes and Related Topics, Sozopol, Bulgaria, May 26–June 1, 1995.

The authors are with Fakultät für Mathematik, Otto-von-Guericke-Universität Magdeburg, 39106 Magdeburg, Germany.

Publisher Item Identifier S 0018-9448(96)06887-3.