Designs, Codes and Cryptography, 24, 343–348, 2001


# Trace Representation of Legendre Sequences

JEONG-HEON KIM heon@calab.yonsei.ac.kr
*School of Electrical and Electronic Engineering, Yonsei University, Seoul Korea*

HONG-YEOP SONG hysong@yonsei.ac.kr
*School of Electrical and Electronic Engineering, Yonsei University, Seoul Korea*

**Communicated by:** A. Pott

*Received April 21, 2000; Revised December 8, 2000; Accepted January 12, 2001*

**Abstract.** In this paper, a Legendre sequence of period $p$ for any odd prime $p$ is explicitely represented as a sum of trace functions from $GF(2^n)$ to $GF(2)$, where $n$ is the order of 2 mod $p$.

**Keywords:** Legendre sequences, quadratic residue, trace function

## 1. Introduction

Legendre sequence $\{b(t)\}$ of period $p$ is defined as [1,3,2]

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

If $p \equiv \pm 3 \pmod 8$, the corresponding Legendre sequence is not only balanced but also has optimal autocorrelation property. Because of the usefulness of balanced binary sequences with optimal autocorrelation in communication systems area, many researchers have studied the properties of such sequences to which Legendre sequences belong. In [2], the linear complexity of a Legendre sequence is determined, which was in fact already found in [6]. In [5], J.-S. No, et al. have found the trace representation of Legendre sequences of Mersenne prime period. In this paper, we found a general trace representation of Lengendre sequences of any prime period. For this, we consider two separate cases. The first case is when the period $p$ of a sequence is $\pm 1 \pmod 8$ and the second case is when $p \equiv \pm 3 \pmod 8$. For a prime $p \equiv \pm 1 \pmod 8$, the result in this paper is a straightforward generalization of the result in [5].

For convenience, we use the following notation in this paper. $GF(q)$ is the finite field of $q$ elements, $p$ is an odd prime, $n$ is the order of 2 mod $p$, and $Z_p$ is the integers mod $p$. For integers $i$ and $j$, we use $(i, j)$ as the gcd of $i$ and $j$. We use $\alpha, \beta, \gamma, \ldots$ as elements of $GF(2^n)$, and the trace function from $GF(2^n)$ to $GF(2)$ is denoted by $\mathrm{tr}(x)$ instead of $\mathrm{tr}_1^n(x)$ for any $x \in GF(2^n)$ unless it is necessary to specify those subscripts and superscripts. It is

defined as

$$\mathrm{tr}(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}}.$$

One can easily check that $\mathrm{tr}(x) + \mathrm{tr}(y) = \mathrm{tr}(x + y)$ and $\mathrm{tr}(x) = \mathrm{tr}(x^{2^i})$ for all $i$. Refer to [4] for comprehensive treatment of trace functions.

## 2. Trace Representation of Legendre Sequences

Let $p$ be an odd prime and $n$ be the order of 2 mod $p$. Then it is easy to show that there exists a primitive root $u$ mod $p$ such that $u^{(p-1)/n} \equiv 2 \pmod{p}$. In the remaining of this paper, we use $u$ as a primitive root mod $p$ such that $u^{(p-1)/n} \equiv 2 \pmod{p}$.

Now, we consider the case where $p \equiv \pm 1 \pmod 8$. In this case, note that 2 is a quadratic residue mod $p$, and hence, $x^2 \equiv 2 \pmod{p}$ for some $x$, and $2^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$. Therefore, $n$ divides $(p-1)/2$. Furthermore, if $i \equiv j \pmod{\frac{p-1}{n}}$, then we have $\mathrm{tr}(\beta^{u^i}) = \mathrm{tr}(\beta^{u^{\frac{p-1}{n}k+j}}) = \mathrm{tr}(\beta^{2^k u^j}) = \mathrm{tr}(\beta^{u^j})$ for any $p$-th root of unity $\beta \in GF(2^n)$. All of these are summarized in the following:

LEMMA 1. *Let $p$ be a prime with $p \equiv \pm 1 \pmod 8$ and 2 has order $n$ mod $p$. Then, $n$ divides $(p-1)/2$. If $i \equiv j \pmod{\frac{p-1}{n}}$, then $\mathrm{tr}(\beta^{u^i}) = \mathrm{tr}(\beta^{u^j})$ for any $p$th root of unity $\beta \in GF(2^n)$.*

Following is the first part of our main result.

THEOREM 2. *Let $p$ be a prime with $p \equiv \pm 1 \pmod 8$, $n$ be the order of 2 mod $p$, and $u$ be a primitive root mod $p$ such that $u^{\frac{p-1}{n}} \equiv 2 \pmod{p}$. Then, there exists a primitive $p$th root of unity $\beta$ in $GF(2^n)$ such that*

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

*and the following sequence $\{s(t)\}$ for $0 \le t \le p-1$ is the Legendre sequence of period $p$:*

$$s(t) = \begin{cases} \sum_{i=0}^{\frac{p-1}{2n}-1} \mathrm{tr}\left(\beta^{u^{2i}t}\right) & \text{for } p \equiv -1 \pmod 8, \\ 1 + \sum_{i=0}^{\frac{p-1}{2n}-1} \mathrm{tr}\left(\beta^{u^{2i+1}t}\right) & \text{for } p \equiv 1 \pmod 8. \end{cases}$$

*Proof.* Let $\gamma$ be a primitive $p$th root of unity in $GF(2^n)$ and consider the following:

$$\begin{aligned} \sum_{i=0}^{\frac{p-1}{2n}-1} \mathrm{tr}\left(\gamma^{u^{2i}}\right) + \sum_{i=0}^{\frac{p-1}{2n}-1} \mathrm{tr}\left((\gamma^u)^{u^{2i}}\right) &= \sum_{j=0}^{n-1} \left( \sum_{i=0}^{\frac{p-1}{2n}-1} \left(\gamma^{u^{2i}} + \gamma^{u^{2i+1}}\right) \right)^{2^j} \\ &= \sum_{j=0}^{n-1} \left( \sum_{i=0}^{\frac{p-1}{n}-1} \left(\gamma^{u^i}\right) \right)^{2^j} \end{aligned} \tag{3}$$

$$= \sum_{j=0}^{n-1} \sum_{i=0}^{\frac{p-1}{n}-1} \left(\gamma^{u^{i+\frac{p-1}{n}j}}\right)$$

$$= \sum_{k=0}^{p-2} \gamma^{u^k} = 1. \tag{4}$$

Since one of the two summands in the left-hand side of (3) is 0 and the other is 1, either $\beta = \gamma$ or $\beta = \gamma^u$ is the primitive $p$th root of unity satisfying (2).

Consider the case $p \equiv -1 \pmod 8$. Since $\frac{p-1}{2}$ is odd, we have $s(0) = \frac{p-1}{2} \cdot 1 = 1$. If $t$ is a quadratic residue mod $p$, then

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

Note that as $i$ runs from 0 to $\frac{p-1}{2n} - 1$, both $2i$ and $2(i + j)$ for any $j$ run through the same set of values modulo $\frac{p-1}{n}$ possibly in different order. By Lemma 1 and (2), therefore, we have

$$s(u^{2j}) = \sum_{k=0}^{\frac{p-1}{2n}-1} \operatorname{tr}\left(\beta^{u^{2k}}\right) = s(1) = 0.$$

Similarly for $t$ a quadratic non-residue, we have

$$s(t) = \sum_{k=0}^{\frac{p-1}{2n}-1} \operatorname{tr}\left(\beta^{u^{2k+1}}\right) = s(u).$$

Since $\beta$ also satisfies the relation given from (3) up to (4), we have $s(1) + s(u) = 1$ and consequently $s(u) = 1$, which proves that $\{s(t)\}$ is the Legendre sequence of period $p$.

For $p \equiv 1 \pmod 8$, similarly, it can be shown that $\{s(t)\}$ is the Legendre sequence given in (1). ■

Now, we will take care of the other case that $p \equiv \pm 3 \pmod 8$. We assume that $p > 3$ in the remaining of this section in order to avoid certain triviality. We know that there exists a primitive root $u$ of $GF(p)$ such that $u^{(p-1)/n} = 2$. Since 2 is a quadratic non-residue mod $p$ where $p \equiv \pm 3 \pmod 8$, $(p - 1)/n$ must be odd, which implies $n$ is even. Therefore, we can let $2^n - 1 = 3pm$ for some positive integer $m$. Let $\alpha$ be a primitive element in $GF(2^n)$. Then, $\alpha^{pm}$ is a primitive 3rd root of unity, and we have

$$\operatorname{tr}(\alpha^{pm}) = \sum_{i=0}^{n-1} (\alpha^{pm})^{2^i} = \sum_{i=0}^{n/2-1} (\alpha^{pm} + \alpha^{2pm})^{2^{2i}} = \frac{n}{2} \cdot 1.$$

If $p \equiv 3 \pmod 8$, then $n/2$ must be odd. On the other hand, if $p \equiv -3 \pmod 8$, since $-1$ is a quadratic residue, there exists some $x$ such that $x^2 \equiv -1 \equiv 2^{n/2} \pmod p$. This

implies that $n/2$ must be even. Therefore, we conclude that

$$\mathrm{tr}(\alpha^{pm}) = \begin{cases} 1 & \text{for } p \equiv 3 \pmod 8 \\ 0 & \text{for } p \equiv -3 \pmod 8 \end{cases} \tag{5}$$

All of these are summarized in the following:

LEMMA 3. *Let $p > 3$ be a prime with $p \equiv \pm 3 \pmod 8$, let $n$ be the order of 2 mod $p$, and $\alpha$ be a primitive element of $GF(2^n)$. Then, $\mathrm{tr}(\alpha^{pm})$ is given as (5).*

Following is the second part of our main result.

THEOREM 4. *Let $p > 3$ be a prime with $p \equiv \pm 3 \pmod 8$, $n$ be the order of 2 mod $p$, and $u$ be a primitive root mod $p$ such that $u^{\frac{p-1}{n}} \equiv 2 \pmod p$. Let $2^n - 1 = 3pm$ for some $m$, and $\beta$ be a primitive $p$th root of unity in $GF(2^n)$. Then, there exists a primitive element $\alpha$ in $GF(2^n)$ such that*

$$\sum_{i=0}^{\frac{p-1}{n}-1} \mathrm{tr}\left((\alpha^{pm})^{2^i} \beta^{u^i}\right) = 0, \tag{6}$$

*and the following sequence $\{s(t)\}$ for $0 \le t \le p-1$ is the Legendre sequence of period $p$:*

$$s(t) = \begin{cases} \sum_{i=0}^{\frac{p-1}{n}-1} \mathrm{tr}\left((\alpha^{pm})^{2^i} \left(\beta^{u^i}\right)^t\right) & \text{for } p \equiv 3 \pmod 8, \\ 1 + \sum_{i=0}^{\frac{p-1}{n}-1} \mathrm{tr}\left((\alpha^{2pm})^{2^i} \left(\beta^{u^i}\right)^t\right) & \text{for } p \equiv -3 \pmod 8. \end{cases}$$

*Proof.* If we let $\gamma$ be a primitive element in $GF(2^n)$, one can easily check in a similar manner in Theorem 2 that

$$\sum_{i=0}^{\frac{p-1}{n}-1} \mathrm{tr}\left((\gamma^{pm})^{2^i} \beta^{u^i}\right) + \sum_{i=0}^{\frac{p-1}{n}-1} \mathrm{tr}\left((\gamma^{2pm})^{2^i} \beta^{u^i}\right) = 1. \tag{7}$$

Therefore, either $\alpha = \gamma$ or $\alpha = \gamma^2$ is the primitive element satisfying (6). We would like to note that for such $\alpha$ we have

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

Consider the case $p \equiv 3 \pmod 8$. Since $(p-1)/n$ is odd in this case, by Lemma 3, we have

$$s(0) = \sum_{i=0}^{\frac{p-1}{n}-1} \mathrm{tr}(\alpha^{pm}) = \mathrm{tr}(\alpha^{pm}) = 1.$$

From (6), (7), and (8), we also have $s(1) = 0$ and $s(2) = 1$.

Define $X_{i,j}$ as

$$X_{i,j} \triangleq \alpha^{pm2^i} \beta^{u^{i+2j}} = \begin{cases} \alpha^{pm} \beta^{u^{i+2j}} & \text{if } i \text{ is even}, \\ \alpha^{2pm} \beta^{u^{i+2j}} & \text{if } i \text{ is odd}. \end{cases}$$

If $t$ is a quadratic residue mod $p$, then

$$\begin{aligned} s(t) = s(u^{2j}) &= \sum_{i=0}^{\frac{p-1}{n}-1} \mathrm{tr}(X_{i,j}) \\ &= \left( \sum_{i=2}^{\frac{p-1}{n}-1} \mathrm{tr}\,(X_{i,j-1}) \right) + \mathrm{tr}\big(X_{0,j-1}^2\big) + \mathrm{tr}\big(X_{1,j-1}^2\big) \\ &= \sum_{i=0}^{\frac{p-1}{n}-1} \mathrm{tr}(X_{i,j-1}) \\ &= s\big(u^{2(j-1)}\big). \end{aligned}$$

Therefore, we have $s(u^{2j}) = s(1) = 0$ for all $j$. Similarly, $s(u^{2j+1}) = s(2) = 1$ for all $j$. Therefore, $\{s(t)\}$ for $0 \le t \le p-1$ is the Legendre sequence given in (1). The other case where $p \equiv -3 \pmod 8$ can be proved similarly. ■

## 3. Concluding Remarks

The linear complexity and the characteristic polynomial of Legendre sequences were already determined in [2] and [6]. Nonetheless, we would like to note that the characteristic polynomial and the linear complexity of Legendre sequences of period $p$ can also be obtained from the trace representations in the previous section as following:

| Case | Char. Polynomial | Linear Complexity |
|---|---|---|
| $p \equiv -1 \pmod 8$ | $Q(x)$ | $(p-1)/2$ |
| $p \equiv 11 \pmod 8$ | $(x+1)N(x)$ | $(p+1)/2$ |
| $p \equiv 31 \pmod 8$ | $(x^p+1)/(x+1)$ | $p-1$ |
| $p \equiv -31 \pmod 8$ | $x^p+1$ | $p$ |

Here, $Q(x) = \Pi_{i \in QR}(x + \beta^i)$ and $N(x) = \Pi_{i \in NR}(x + \beta^i)$ where $QR$ and $NR$ are the set of quadratic residues and non-residues mod $p$, respectively, and $\beta$ is a primitive $p$-th root of unity satisfying (2).

## Acknowledgments

The authors would like to thank the referees for their valuable comments and suggestions. This work was supported by the University Research Program supported by Ministry of Information and Communication in South Korea in the Program Year 1999 and the Brain Korea 21 project.

## References

1. L. D. Baumert, *Cyclic Difference Sets,* New York: Springer-Verlag (1971).
2. C. Ding, T. Helleseth and W. Shan, On the linear complexity of Legendre sequences, *IEEE Trans. Inform. Theory,* Vol. 44, No. 3 (1998) pp. 1276–1278.
3. S. W. Golomb, *Shift Register Sequences,* San Francisco, CA (Revised Edition, Aegean Park Press, Laguna Hills, CA, 1982), Holden-Day (1967).
4. R. Lidl and H. Niederreiter, *Finite fields, Encyclopedia of Mathematics and Its Applications,* Addison-Wesley, Reading, MA, Vol. 20 (1983).
5. 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 (1996) pp. 2254–2255.
6. R. Turyn, The linear generation of the Legendre sequences, *J. Soc. Ind. Appl. Math,* Vol. 12, No. 1 (1964) pp. 115–117.