TRACE REPRESENTATION OF

LEGENDRE SEQUENCES

J.-H. KIM
M. SHIN
H.-Y. SONG

YONSEI UNIVERSITY
SEOUL, KOREA
Contents

• Definition and Notation, and *Introduction*

• Existence of some primitive element of $GF(2^n)$

• Trace Representation for $p \equiv \pm 1 \pmod{8}$

• Trace Representation for $p \equiv \pm 3 \pmod{8}$

• Some Historical Remarks

• Some References

Hong-Yeop Song, Dept. of Electrical and Computer Engineering, Yonsei Univ.
INTRODUCTION

• Legendre sequence \( \sigma(t), \ t=0,1,2,\ldots, p-1 \)

\[
\sigma(t) = \begin{cases} 
1 & \text{if } t \equiv 0 \pmod{p} \\
0 & \text{if } t \equiv QR \pmod{p} \\
1 & \text{if } t \equiv QNR \pmod{p} 
\end{cases}
\]

where \( p \) is an odd prime.

• m-sequence \( m(t), \ t=0,1,\ldots, 2^n-2 \)

\[
m(t) = \text{tr}_1^n (\theta, \alpha^t)
\]

where \( \theta \in \text{GF}(2^n) \) and \( \alpha \) is a primitive element of \( \text{GF}(2^n) \).

° WHEN \( p=2^n-1 \) (Mersenne prime), both m-sequence and Legendre sequence are balanced and have optimal 2-level autocorrelation, but they are inequivalent.

° What happens when just \( p \equiv 1 \pmod{4} \)?
Preparation

Goal: Represent Legendre sequences as

\[ s(t) = \sum_{a \in \mathbb{Z}/p} \text{tr}_1^n(\theta_a \cdot \alpha^t) \]

- period: \( p = \text{odd prime} \Rightarrow p \mid 2^n - 1 \).

Smallest such integer \( n \) is indeed the order of \( 2 \mod p \).

Proposition 1. Let \( p \) be an odd prime and \( n \) be the order of \( 2 \mod p \). Then there exists a primitive root \( a \mod p \) such that

\[ a^{(p-1)/n} \equiv 2 \pmod{p} \]

pf. Letting \( R \) be the set of primitive roots \( \mod p \), we try to show that

\[ R^{(p-1)/n} = \{ r^{(p-1)/n} \mid r \in R \} \]

contains \( 2 \).

\( \Box \)

* Fix the notation: \( p, n, a \).
Case $p \equiv \pm 1 \pmod{8}$

(i) $n$ divides not only $p-1$, it divides $\frac{p-1}{2}$.

Hence, \( \left( \frac{2}{p} \right) = (-1)^{\frac{p^2-1}{8}} = +1 \iff 2 \text{ is a QR. mod } p \iff \gamma^2 \equiv 2 \pmod{p} \), some $\gamma$.

Therefore,

\[ 2^{\frac{p-1}{n}} \equiv \gamma^{p-1} \equiv 1 \pmod{p}. \]

Since $n$ is the order of 2 mod $p$, we are done.

(ii) For any $\beta \in GF(2^n)$, if $i \equiv j \pmod{\frac{p-1}{n}}$ then

\[ \text{tr}_i^n(\beta^a^i) = \text{tr}_i^n(\beta^a^j) \]

where $a$ is a prim. root mod $p$ such that $a^{\frac{p-1}{n}} \equiv 2 \pmod{p}$.

Hence, \( \text{tr}(\beta^a^i) = \text{tr}(\beta^{a^\frac{p-1}{n} \cdot k + j}) = \text{tr}(\beta^a^{k \cdot \gamma^j}) \)

\[ = \text{tr}(\beta^a^j) \]
(iii) There exists a primitive $p$-th root of unity $\beta \in GF(2^n)$ such that

$$\sum_{i=0}^{p-1} \text{tr}_1^n(\beta^{a^i}) = 0.$$ 

pf. Let $\eta \in GF(2^n)$ be any primitive $p$-th root of unity, and consider the following:

$$\sum_{i=0}^{p-1} \left[ \text{tr}_1^n(\eta^{a^i}) + \text{tr}_1^n([\eta^{a^i}]) \right]$$

$$= \sum_{i=0}^{n-1} \left[ \sum_{j=0}^{p-1} \left( \eta^{a^i} \right)^{2^j} + \sum_{j=0}^{p-1} \left( \eta^{a^{2i+1}} \right)^{2^j} \right]$$

$$= \sum_{i=0}^{n-1} \left[ \sum_{j=0}^{p-1} \eta^{a^i} + \sum_{j=0}^{p-1} \eta^{a^{2i+1}} \right]^{2^j}$$

$$= \sum_{i=0}^{n-1} \sum_{j=0}^{p-1} \eta^{a^i} \eta^{a^{2i+1}}^{2^j} \quad \text{since} \quad a = \frac{2}{n}$$

$$= \sum_{k=0}^{p-2} \eta^{a^k}$$

$$= \sum_{i=1}^{p-1} \eta^i = 1 \quad \Rightarrow \quad \text{either } \beta = \eta \text{ or } \beta = \eta^a \text{ will work.}$$

Further, for such $\beta$, \( \sum_{i=0}^{p-1} \text{tr}_1^n(\beta^{a^i+1}) = 1 \).
Sub Case: \( p \equiv -1 \pmod{8} \)

Claim: \[
    s(t) = \sum_{i=0}^{\frac{p-1}{2n}-1} tr^n \left( \beta^{a \cdot i^2} \right), \quad t = 0, 1, \ldots, p-1,
\]
is Legendre sequence of period \( p \).

Proof: \[
    s(0) = \sum_{i=0}^{\frac{p-1}{2n}-1} tr(1) = 1 + 1 + \cdots + 1 = \frac{p-1}{2n},
\]
\( \text{times} \)
\[
    s(1) = \sum_{i=0}^{\frac{p-1}{2n}-1} tr(\beta^{a^2}) = 0.
\]

\( \beta \) is so defined in (iii).

(iii) says \( s(1) + s(a) = 1 \) \( \Rightarrow \) \( s(a) = 1 \).

and we have \( s(0) = 0 \)

Remaining steps:

If \( t = QR \pmod{p} \Rightarrow t = a^{2\hat{i}} \) some \( \hat{i} \)

\[
    s(t) = s(a^{2\hat{i}}) = \sum_{i=0}^{\frac{p-1}{2n}-1} tr\left( \beta^{a^{2(i+\hat{i})}} \right) = \sum_{i=0}^{\frac{p-1}{2n}-1} tr\left( \beta^{a^{2\hat{i}}} \right) = s(1).
\]

If \( t = QNR \pmod{p} \Rightarrow t = a^{2\hat{i}+1} \) some \( \hat{i} \)

\[
    s(t) = s(a^{2\hat{i}+1}) = s(a) = 1.
\]
Sub case \( p \equiv 1 \pmod{8} \)

\[
s(t) = 1 + \sum_{i=0}^{p-1} \text{tr}_i \left( \beta^{\frac{2it+1}{p-1}} \right), \quad t=0,1,\ldots,p-1,
\]

is a Legendre sequence of period \( p \).
Theorem 1 for case $p \equiv \pm 1 \pmod{8}$

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

$$
\sum_{i=0}^{\frac{p-1}{2n}-1} \text{tr}(\beta^{a^{2i}t}) = 0,
$$

(2)

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

For $p \equiv -1 \pmod{8}$

$$
s(t) = \sum_{i=0}^{\frac{p-1}{2n}-1} \text{tr}(\beta^{a^{2i}t})
$$

(3)

For $p \equiv 1 \pmod{8}$

$$
s(t) = 1 + \sum_{i=0}^{\frac{p-1}{2n}-1} \text{tr}(\beta^{a^{2i+1}t})
$$

(4)

Hong-Yeop Song, Dept. of Electrical and Computer Engineering, Yonsei Univ.
Lemma 2 for case \( p \equiv \pm 3 \pmod{8} \)

Let \( p > 3 \) be a prime with \( p \equiv \pm 3 \pmod{8} \), let \( n \) be the order of \( 2 \) mod \( p \). Then \( n \) must be even and we may let \( 2^n - 1 = 3pm \) for some positive integer \( m \). Let \( \alpha \) be a primitive element of \( GF(2^n) \). Then, we have

\[
\text{tr}(\alpha^{pm}) = \begin{cases} 
1 & \text{for } p \equiv 3 \pmod{8} \\
0 & \text{for } p \equiv -3 \pmod{8}
\end{cases} \quad (7)
\]

Proof:

When \( p \equiv \pm 3 \pmod{8} \), \( 2 \) is a quadratic non-residue mod \( p \). If the order \( n \) of \( 2 \) mod \( p \) is odd, then \( 2^{n+1} \equiv 2 \pmod{p} \) is a contradiction. Therefore, \( n \) must be even and we may let \( 2^n - 1 = 3pm \) for some positive integer \( m \).

Let \( \alpha \) be a primitive element in \( GF(2^n) \) where \( 2^n - 1 = 3pm \). Then, \( \alpha^{pm} \) is a primitive 3rd root of unity,

---

Hong-Yeop Song, Dept. of Electrical and Computer Engineering, Yonsei Univ.
and we have
\[ \text{tr} (\alpha^{pm}) = \sum_{i=0}^{n-1} (\alpha^{pm}) 2^i = \sum_{i=0}^{n/2-1} (\alpha^{pm} + \alpha^{2pm}) 2^{2i} = \frac{n}{2}. \]

If \( p \equiv 3 \pmod{8} \) \( \Rightarrow p = 8k + 3 \) for some \( k \)
\( \Rightarrow (p - 1)/n = (8k + 2)/n = (4k + 1)/(n/2). \)
Therefore, \( n/2 \) must be odd.

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.

This proves (7).

\[ 2^2 = \frac{a}{b} + (p - 1)/k \]

Hong-Yeop Song, Dept. of Electrical and Computer Engineering, Yonsei Univ.
Theorem 2 for case $p \equiv \pm 3 \pmod{8}$

Let $p > 3$ be a prime with $p \equiv \pm 3 \pmod{8}$, $n$ be the order of 2 mod $p$, and $a$ be a primitive root mod $p$ such that $\alpha^{\frac{n-1}{2}} \equiv 2 \pmod{p}$. 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

$$\sum_{i=0}^{n-1} \text{tr}\left((\alpha^{pm})^{2^i} \beta^{a_i}\right) = 0,$$

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

For $p \equiv 3 \pmod{8}$

$$s(t) = \sum_{i=0}^{n-1} \text{tr}\left((\alpha^{pm})^{2^i} (\beta^{a_i})^t\right)$$

For $p \equiv -3 \pmod{8}$

$$s(t) = 1 + \sum_{i=0}^{n-1} \text{tr}\left((\alpha^{2pm})^{2^i} (\beta^{a_i})^t\right)$$

Hong-Yeop Song, Dept. of Electrical and Computer Engineering, Yonsei Univ.
Proof of Theorem 2

We first show the existence of such a primitive element $\alpha$ in $GF(2^n)$ in exactly similar method in the proof of Theorem 1. If we let $\gamma$ be a primitive element in $GF(2^n)$, then it is easy to check that

$$\sum_{i=0}^{\frac{p-1}{n}-1} \text{tr} \left( (\gamma^{pm})^{2^i} \beta^{a^i} \right) + \sum_{i=0}^{\frac{p-1}{n}-1} \text{tr} \left( (\gamma^{2pm})^{2^i} \beta^{a^i} \right) = 1.$$ (11)

Therefore, either $\alpha = \gamma$ or $\alpha = \gamma^2$ is the primitive element satisfying (8). We would like to note that for such $\alpha$ we have

$$\sum_{i=0}^{\frac{p-1}{n}-1} \text{tr} \left( (\alpha^{2pm})^{2^i} \beta^{a^i} \right) = 1.$$ (12)

Consider the case $p \equiv 3 \pmod{8}$. Since $(p - 1)/n$ is odd in this case by Lemma 2, we have

$$s(0) = \sum_{i=0}^{\frac{p-1}{n}-1} \text{tr}(\alpha^{pm}) = \text{tr}(\alpha^{pm}) = 1.$$ by (7)

Hong-Yeop Song, Dept. of Electrical and Computer Engineering, Yonsei Univ.
From (8), (11), and (12), we also have \( s(1) = 0 \) and \( s(2) = 1 \).

Define \( X_{i,j} \) as

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

If \( t \) is a quadratic residue mod \( p \), then

\[
s(t) = s(a^{2^j}) = \sum_{i=0}^{p-1} \frac{1}{n-1} \cdot \text{tr} \left( X_{i,j} \right) = \left( \sum_{i=2}^{p-1} \text{tr} \left( X_{i,j-1} \right) \right) + \text{tr} \left( X_{2,j-1}^2 \right) + \text{tr} \left( X_{1,j-1}^2 \right) \]

\[
= \sum_{i=0}^{p-1} \text{tr} \left( X_{i,j-1} \right) = s(a^{2(j-1)}).
\]

Therefore, we have \( s(a^{2^j}) = s(1) = 0 \) for all \( j \).
Similarly, \( s(a^{2^j+1}) = s(2) = 1 \) for all \( j \). Therefore, done.

Hong-Yeop Song, Dept. of Electrical and Computer Engineering, Yonsei Univ.

* Similarly, for the case \( p \equiv -3 \pmod{8} \).
Some Historical Remarks

A binary sequence \( \{b(t)\} \) of period \( N \), where \( b(t) \in \{0, 1\} \), is called balanced if the number of 1's and the number of 0's in one period differ by one.

It is said to have optimal autocorrelation if, when \( N \equiv 3 \pmod{4} \), its periodic autocorrelation function \( R(\tau) \) satisfies the following:

\[
R(\tau) \triangleq \sum_{i=0}^{N-1} (-1)^{b(t)+b(t+\tau)}
\]

\[
= \begin{cases} 
N & \text{for } \tau \equiv 0 \pmod{N}, \\
-1 & \text{otherwise}.
\end{cases}
\]  

(13)

(14)

Balanced binary sequences with optimal autocorrelation have been widely used in spread-spectrum CDMA communication systems, position/location systems, and many other systems due to their randomness properties and ease of generation.

Hong-Yeop Song, Dept. of Electrical and Computer Engineering, Yonsei Univ.
Every known example of a balanced binary sequence with optimal autocorrelation has a period \( N \equiv 3 \pmod{4} \) that belongs to one of the following three categories:

1. \( N \equiv 3 \pmod{4} \) is a prime;

2. \( N = p(p + 2) \) is a product of twin primes; or

3. \( N = 2^t - 1 \), for \( t = 2, 3, 4, \ldots \) "LFSR"

Based upon some extensive computation, Song and Golomb (IEEE IT 1994 and JSPI 1997) conjectured that the period \( N \) of a balanced binary sequence with the optimal autocorrelation must be one of the above three types.

Most recently, Kim and Song (JCN 1999) reported that the conjecture is confirmed for all \( N \equiv 3 \pmod{4} \) up to 3435, and \( N = 3439 \) is the smallest unsettled case.

Hong-Yeop Song, Dept. of Electrical and Computer Engineering, Yonsei Univ.

\( \bigstar \) Up to 10,000, only 13 cases remain unsettled.