Legendre01.jpg (1602x2234x16M jpeg)

TRACE REPRESENTATION OF LEGENDRE SEQUENCES

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

YONSEI UNIVERSITY
SEOUL, KOREA

Contents

Legendre03.jpg (1618x2301x16M jpeg)

INTRODUCTION

- **Legendre sequence** $b(t)$, $t = 0, 1, 2, \cdots, p-1$

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

where p is an <u>odd</u> prime.

- **m-sequence** $m(t)$, $t = 0, 1, \cdots, 2^n - 2$

$$m(t) = tr_1^n(\theta \cdot \alpha^t)$$

where $\theta \in GF(2^n)$ and α is a primitive element of $GF(2^n)$.

⊙ WHEN $p = 2^n - 1$ (Mersenne prime), both m-sequence and Legendre sequence are <u>balanced</u> and have <u>optimal 2-level autocorrelation</u>, but they are <u>inequivalent</u>.

⊙ What happens when just $p \equiv -1 \pmod 4$?

Legendre04.jpg (1616x2298x16M jpeg)

Preparation

Goal: Represent Legendre sequences as

$$s(t) = \sum_{a \in I} tr_1^n\left(\theta_a \cdot \alpha^{at}\right)$$

- period $= p =$ 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

$$a^{\frac{p-1}{n}} \equiv 2 \pmod{p}.$$

pf. Letting R be the set of prim. roots mod p, we try to show that

$$R^{\frac{p-1}{n}} = \{ r^{\frac{p-1}{n}} \mid r \in R \}$$

contains 2. ∎

◎ Fix the notation: p, n, a.

Legendre05.jpg (1618x2273x16M jpeg)

Case $p \equiv \pm 1 \pmod 8$

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

Pf. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = +1 \Leftrightarrow 2$ is a QR. mod p

$\Leftrightarrow x^2 \equiv 2 \pmod p$, some x.

Therefore,

$$2^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p.$$

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

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

$$tr_1^n\left(\beta^{a^i}\right) = tr_1^n\left(\beta^{a^j}\right)$$

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

Pf. $tr\left(\beta^{a^i}\right) = tr\left(\beta^{a^{\frac{p-1}{n}k+j}}\right) = tr\left(\beta^{2^k \cdot a^j}\right)$

$= tr\left(\beta^{a^j}\right)$

Legendre06.jpg (1621x2286x16M jpeg)

(iii) There exists a primitive p-th root of unity $\beta \in GF(2^n)$ such that

$$\sum_{i=0}^{\frac{p-1}{2n}-1} tr_1^n\left(\beta^{a^{2i}}\right) = 0.$$

pf.

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

$$\sum_{i=0}^{\frac{p-1}{2n}-1} \left[tr_1^n\left(\gamma^{a^{2i}}\right) + tr_1^n\left([\gamma^a]^{a^{2i}}\right) \right]$$

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

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

$$= \sum_{j=0}^{n-1} \sum_{i=0}^{\frac{p-1}{n}-1} \left(\gamma^{a^i}\right)^{a^{j\cdot\frac{p-1}{n}}} \qquad \text{since } 2 = a^{\frac{p-1}{n}}$$

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

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

Further, for such β, $\displaystyle\sum_{i=0}^{\frac{p-1}{2n}-1} tr_1^n\left(\beta^{a^{2i+1}}\right) = 1$.

Legendre07.jpg (1621x2300x16M jpeg)

Sub Case: $p \equiv -1 \pmod 8$

claim:

$$s(t) = \sum_{i=0}^{\frac{p-1}{2n}-1} tr_1^n\left(\beta^{a^{2i}\cdot t}\right), \quad t = 0, 1, \cdots, p-1,$$

is Legendre sequence of period p.

pf.

$$s(0) = \sum_{i=0}^{\frac{p-1}{2n}-1} tr(1) = \underbrace{1+1+\cdots+1}_{\frac{p-1}{2n}\text{ times}} = \frac{p-1}{2n} = 1.$$

observe:

$p = 8K+7$

$\frac{p-1}{2} = 4K+3 = \text{odd}$

$n = \text{odd}$

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

β is so defined in (iii).

(iii) says $s(1) + s(a) = 1$
and we have $s(1) = 0$ $\Big\} \Rightarrow s(a) = 1.$

Remaining steps:

if $t = QR \bmod p \Rightarrow t = a^{2j}$ some j

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

if $t = QNR \bmod p \Rightarrow t = a^{2j+1}$ some j

$$\therefore\ s(t) = s(a^{2j+1}) = s(a) = 1. \quad \blacksquare$$

Legendre08.jpg (1542x2136x16M jpeg)

<u>Sub case</u> $p \equiv 1 \pmod 8$

$$s(t) = 1 + \sum_{i=0}^{\frac{p-1}{2n}-1} tr_1^n\left(\beta^{a^{2i+1} \cdot t}\right), \quad t = 0, 1, \cdots, p-1,$$

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 β in $GF(2^n)$ such that

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

and the following sequence $\{s(t)\}$ is the Legendre sequence of period p for $0 \le t \le p-1$:
For $p \equiv -1 \pmod 8$

$$s(t) = \sum_{i=0}^{\frac{p-1}{2n}-1} \text{tr}\left(\beta^{a^{2i}t}\right) \tag{3}$$

For $p \equiv 1 \pmod 8$

$$s(t) = 1 + \sum_{i=0}^{\frac{p-1}{2n}-1} \text{tr}\left(\beta^{a^{2i+1}t}\right) \tag{4}$$

Legendre10.jpg (1607x2282x16M jpeg)

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 α be a primitive element of $GF(2^n)$. Then, we have

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

Proof: (2 = QNR mod p)

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 α be a primitive element in $GF(2^n)$ where $2^n - 1 = 3pm$. Then, α^{pm} is a primitive 3rd root of unity, and we have

$$
\begin{aligned}
\operatorname{tr}(\alpha^{pm}) &= \sum_{i=0}^{n-1} (\alpha^{pm})^{2^i} \\
&= \sum_{i=0}^{n/2-1} (\underbrace{\alpha^{pm} + \alpha^{2pm}}_{= 1 \;\because\; \alpha^{pm} \text{ is a primi. 3rd root of 1.}})^{2^{2i}} = \frac{n}{2}.
\end{aligned}
$$

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. & $\frac{p-1}{n}$ = 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.

Since
$-1 \equiv x^2 \equiv \alpha^{2j}$ if $x = \alpha^{j}$
$-1 \equiv 2^{\frac{n}{2}} \equiv \alpha^{i \cdot \frac{n}{2}}$ if $2 = \alpha^{i}$

This proves (7). ∎

$\Rightarrow \boxed{2j = i \cdot \frac{n}{2} + (p-1) \cdot k}$

2 = QNR mod p $\Rightarrow$ i = odd $\Rightarrow$ $\frac{n}{2}$ = even.

$p \equiv -3\ (8) \Rightarrow \frac{p-1}{n} = \frac{8k-4}{n} = \frac{4k-2}{(n/2)}$ = odd, since $\frac{n}{2}$ = even.

Legendre12.jpg (1602x2286x16M jpeg)

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 $a^{\frac{p-1}{n}} \equiv 2 \pmod p$. Let $2^n - 1 = 3pm$ for some m, and β be a primitive p-th root of unity in $GF(2^n)$. Then, there exists a primitive element α in $GF(2^n)$ such that

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

and the following sequence $\{s(t)\}$ for $0 \le t \le p-1$ is the Legendre sequence of period p:
For $p \equiv 3 \pmod 8$

$$s(t) = \sum_{i=0}^{\frac{p-1}{n}-1} \mathrm{tr}\left((\alpha^{pm})^{2^i} (\beta^{a^i})^t\right) \tag{9}$$

For $p \equiv -3 \pmod 8$

$$s(t) = 1 + \sum_{i=0}^{\frac{p-1}{n}-1} \mathrm{tr}\left((\alpha^{2pm})^{2^i} (\beta^{a^i})^t\right) \tag{10}$$

Proof of Theorem 2

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

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

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

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

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

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

by (7)

$p-1 = 8k+2 = 2(4k+1)$

$\frac{p-1}{n} = \frac{2(4k+1)}{n}$ = odd since n = even.

Legendre14.jpg (1612x2259x16M jpeg)

From (8), (11), and (12), we also have $s(1) = 0$ and $s(2) = 1$.

Define $X_{i,j}$ as

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

If t is a quadratic residue mod p, then

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

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

· Similarly, for the case $p \equiv -3 \pmod 8$.

Legendre15.jpg (1604x2270x16M jpeg)

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:

$$R(\tau) \triangleq \sum_{i=0}^{N-1} (-1)^{b(t)+b(t+\tau)} \tag{13}$$

$$= \begin{cases} N & \text{for } \tau \equiv 0 \pmod N, \\ -1 & \text{otherwise.} \end{cases} \tag{14}$$

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.

* 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; → Legendre symbols

(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.

* Up to 10,000, only 13 cases remain unsettled.