On the Legendre Sequences of Mersenne Prime Period

J.S.No, H.K.Lee, H.Chung,
H.Y.Song and K.Yang

Seoul, Korea

Introduction (Motivation)

- Let *s(t)* for *t*=0,1,2,...,*N*-1, be a balanced binary sequences of period N for some odd *N*.
  - "balanced" $\longleftrightarrow$ | *#0's - #1's*|=*1*, for odd *N*.

- There are wide application area of these balanced binary sequences of period *N* if it has two-level autocorrelation function.
  - Two-level autocorrelation function:

$$\phi(\tau) = \sum_{t=0}^{N-1} (-1)^{s(t) \oplus s(t+\tau)} = \begin{cases} N, & \tau = 0 \pmod N \\ -1, & \tau \neq 0 \pmod N \end{cases}$$

Motivation (cont.)

- Such a balanced binary sequences with two-level autocorrelation sequence is known to exist if the period *N* is one of following three types:
  - (A) *N* is a prime congruent to 3 mod 4,
  - (B) *N* is a product of twin primes,
  - (C) $N = 2^n - 1$ for $n=1,2,3,.....$

- However, its converse is still a conjecture:

  If a balanced binary sequence of period *N* has the two-level autocorrelation function, then its period *N* must be one of the above three types.

Motivation (cont.)

- Systematic constructions according to types of *N*
  - For Type (A),
    - » "Legendre sequences" using quadratic residues mod p,
    - » "Hall's sextic residue" sequences for $p=27+x^2$.
  - For Type (B),
    - » twin prime construction for $N=p(p+2)$: "Jacobi sequences"
  - For Type (C),
    - » "Linear shift register" construction: m-sequences
    - » GMW construction: GMW-sequences.
- For the period of 127, 511, and 1023, some examples are known to exist <u>which cannot be explained using any of the above methods.</u>

Motivation (final)

- The conjecture is recently confirmed to be true for N up to 10,000 except possibly for 17 cases the smallest of which is 12??.
- **Some thoughts**:
  - m-sequences are best described using traces from GF(2^n) onto GF(2);

$$s(t) = T_1^n(\alpha^t), \quad t = 0,1,2,\ldots,2^n - 2.$$

  - Legendre sequences are best described using quadratic residues mod p, where p=3 (mod 4);

$$s(t) = \begin{cases} 1, & t = 0 \pmod p \\ \left(\frac{t}{p}\right), & t \neq 0 \pmod p \end{cases}$$

Main Theorem

Legendre sequence *s(t)* of Mersenne prime period *p* of the form $p = 2^n - 1$, where $n \geq 3$, is expressed as

$$s(t) = \sum_{i=0}^{\frac{p-1}{2n}-1} T_1^n(a^{u^{2i}t}),\ t = 0,1,2,\ldots,2^n-2,$$

where $p = 2^n - 1$ is a prime, u is a primitive element in Z_p, α is a primitive element GF(2^n) satisfying

$$\sum_{i=0}^{\frac{p-1}{2n}-1} T_1^n(a^{u^{2i}}) = 0, \qquad T_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}.$$

Example: $n=5,\ p=2^5-1=31$

u=3 is a primitive root mod 31. α is a primitive element of GF(32) satisfying

$$\alpha^5 + a^2 + 1 = 0.$$

Therefore, for $t = 0,1,2,\ldots,30$,

$$s(t) = \sum_{i=0}^{2} T_1^5(a^{9^i t}) = T_1^5(a^t) + T_1^5(a^{9t}) + T_1^5(a^{19t})$$

is the Legendre sequence of period 31.

Why it works ?

Cyclotomic cosets mod 31

$\{0\}$

$\rightarrow \{1, 2, 4, 8, 16\}$

$\{3, 6, 12, 24, 17\}$

$\rightarrow \{9, 18, 5, 10, 20\}$

$\{27, 23, 15, 30, 29\}$

$\rightarrow \{19, 7, 14, 28, 25\}$

$\{26, 21, 11, 22, 13\}$

Essential steps

$$u^{\frac{p-1}{n}} = 2^i \pmod{p},$$

for some integer i.

There exists an α in GF(p +1) such that

$$\sum_{i=0}^{\frac{p-1}{2n}-1} T_1^n(a^{u^{2i}}) = 0.$$

Example: $n=7,\ p=2^7-1=127$

u=3 is a primitive root mod 127 and α is a primitive element of GF(128) satisfying

$$\alpha^7 + a^4 + 1 = 0.$$

Therefore,

$$s(t) = \sum_{i=0}^{8} T_1^7(a^{9^i t}),\ t = 0,1,2,\ldots,126,$$

is the Legendre sequence of period 127.

Proof of Main Theorem

Claim $\forall \alpha \in \mathrm{GF}(p+1) \quad \exists \sum_{i=0}^{\frac{p-1}{2n}-1} T_1^n(a^{u^{2i}}) = 0.$

Let $f(x) = \sum_{i=0}^{\frac{p-1}{2n}-1} T_1^n(x^{u^{2i}}) \Rightarrow f(x) = \sum_{j \in \mathrm{QR}} x^j$

$f(x^u) = \sum_{j \in \mathrm{QNR}} x^j$

$\Rightarrow f(x) + f(x^u) = 1, \quad \forall x \in \mathrm{GF}(p+1), x \neq 1, x \neq 0$

$\Rightarrow f(a) = 0$ or $f(a^u) = 0$ for any primitive $a \in \mathrm{GF}(p+1)$

➔ the existence of such α is gauranteed, since both α and α^u are primitive in GF(p +1), and by changing the name if necessary.

Proof of Main Theorem (Conti.)

Therefore, using such a primitive element α ,

$$s(1) = f(a) = 0. \quad \cdots\cdots\cdots\cdots\cdots \quad (*)$$

On the other hand, Since both n and $\frac{p-1}{2n}$ are odd,

$$s(0) = \frac{p-1}{2n} \cdot T_1^n(1) = 1. \quad \cdots\cdots\cdots \quad (**)$$

Proof of Main Theorem (Conti.)

For any quadratic residue t (mod p), $t = u^{2j}$, and hence,

$$s(t) = s(u^{2j}) = \sum_{i=0}^{\frac{p-1}{2n}-1} T_1^n(\alpha^{u^{2(i+j)}})$$

$$= \sum_{k=0}^{\frac{p-1}{2n}-1} T_1^n(\alpha^{u^{2k}}) = s(1) = 0.$$

Proof of Main Theorem (Conti.)

For any quadratic non-residue t (mod p),

since $t = u^{2j+1}$,

$$s(t) = s(u^{2j+1}) = \sum_{i=0}^{\frac{p-1}{2n}-1} T_1^n(\alpha^{u^{2(i+j)+1}})$$

$$= \sum_{k=0}^{\frac{p-1}{2n}-1} T_1^n(\alpha^{u^{2k+1}}) = \sum_{k=0}^{\frac{p-1}{2n}-1} T_1^n(\alpha^{u^{2k}u}) = s(u) = 1.$$

Concluding Remarks

- Characteristic polynomial of Legendre sequences of Mersenne prime period becomes

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

- Linear span: $L = \frac{p-1}{2} = 2^{n-1} - 1.$

- These sequences are invariant under the decimation by u^{2i} for any i. That is,

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