On the Characteristic Polynomial and Linear Complexity of Hall's Sextic Residue Sequences

May 2001

Jeongheon Kim and Hong-Yeop Song

Yonsei University
Seoul 120-749, Korea
(heon@eve.yonsei.ac.kr hysong@yonsei.ac.kr)

Contents

- Introduction
  - Hall's sextic residue sequences
  - Linear complexity and Characteristic polynomial
- Main Theorem and proof
- Historical Remarks
  - Binary sequences with ideal autocorrelation
  - Their linear complexities

Historical Remarks

ALL EVERY KNOWN

◇ Periods of balanced binary sequences with ideal autocorrelation

(I) $N \equiv 3 \pmod 4$ is a prime; < Legendre sequences for all such prime; Hall's sextic residue sequences for $p = 4u^2 + 27$ ⇐

(II) $N = p(p+2)$ is a product of twin primes; or twin-prime sequences

(III) $N = 2^n - 1$, for $t = 2, 3, 4, \ldots$. m-sequences and more ...

◇ Conjecture

No other period N would be possible for the existence of balanced binary sequences with ideal autocorrelation.

- $N = 3439$ is the smallest unsettled case.
- Only 13 unsettled cases for $N < 10000$.

Introduction

◇ Linear Complexity of binary sequences

- the least positive integer L such that there exists an L-stage linear feedback shift register (LFSR, in short) that generates the sequence with a suitable initial loading

◇ Characteristic polynomial

- Let L be the linear complexity of $\{s_i\}$ of period p. Then there exist constants $c_0 = 1, c_1, \ldots, c_L \in GF(2)$ such that

$$s_i = c_{L-1}s_{i-1} + c_{L-2}s_{i-2} + \cdots + c_0 s_{i-L}, \quad \text{for all } L \leq i < p.$$

The polynomial $c(x) = x^L + c_{L-1}x^{L-1} + \cdots + c_0$ is called the characteristic polynomial of the sequence.

Introduction (cont.)

- $c(x)$ can be obtained from $c^*(x)$ given by

$$\begin{aligned} c^*(x) &= c_0 x^L + c_1 x^{L-1} + \cdots + c_{L-1} x + 1 \\ &= (x^p - 1)/\gcd(x^p - 1, S(x)) \end{aligned}$$

where

$$S(x) = s_0 + s_1 x + \cdots + s_{p-1} x^{p-1}.$$

- The linear complexity of $\{s(t)\}$ is given by

$$\begin{aligned} L &= p - \deg[\gcd(x^p - 1, S(x))] \\ &= p - |\{j : S(\beta^j) = 0,\ 0 \le j \le p-1\}| \end{aligned}$$

where $\beta \in GF(2^n)$ is a primitive pth root of unity and $GF(2^n)$ is the splitting field of $x^p - 1$.

Introduction

◇ Hall's sextic residue sequences

Let $p = 4u^2 + 27 = 6f + 1$ be a prime and g be a primitive root mod p such that $3 \in C_1$ where six ~~cyclotomic~~ residue classes $C_l, l = 0, 1, \cdots, 5$ are given by

$$C_l = \{g^{6i+l} \mid i = 0, 1, \ldots, f-1\} \tag{1}$$

Hall's sextic residue sequence of period p is defined as

$$s(t) = \begin{cases} 1 & \text{if } t \in C_0 \cup C_1 \cup C_3 \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

where $t = 0, 1, \ldots, p-1$.

◇ Example : $p = 4 + 27 = 6(5) + 1 = 31$, $(g = 3)$

$$C_0 = \{1, 2, 4, 8, 16\} \qquad C_1 = \{3, 6, 12, 17, 24\}$$
$$C_2 = \{5, 9, 10, 18, 20\} \qquad C_3 = \{15, 23, 27, 29, 30\}$$
$$C_4 = \{7, 14, 19, 25, 28, 14\} \quad C_5 = \{11, 13, 21, 22, 26\}$$

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$s(t)$	0	1	1	1	1	0	1	0	1	0	0	0	1	0	0	1	1	1	0	0	0	0	0	1	1	0	0	1	0	1	1

Main Results

Hall's sextic residue sequence of period $p = 4u^2 + 27$ has the following reciprocal characteristic polynomial $c^*(x)$:

$$c^*(x) = \begin{cases} (x-1)\prod_{i \in C_0}(x - \beta^i) & \text{if } p = 7 \pmod 8 \\ x^p - 1 & \text{if } p = 3 \pmod 8 \end{cases}$$

where β is a primitive pth root of unity such that $S(\beta) = 1$. The linear complexity L is given by

$$L = \begin{cases} 1 + \frac{p-1}{6} & \text{if } p \equiv 7 \pmod 8 \\ p & \text{if } p \equiv 3 \pmod 8 \end{cases}$$

For Hall's Sextic Residue Sequence of period p,

$$S(x) = C_0(x) + C_1(x) + C_3(x),$$

where

$$C_\ell(x) \triangleq \sum_{k \in C_\ell} x^k = \sum_{k=0}^{f-1} x^{g^{6k+\ell}}.$$

Now, we need a series of **Lemmas**.

[1] $|C_\ell| = \frac{p-1}{6} = f = \text{odd}$, $(\ell = 0,1,2,\cdots,5)$ since $3f = \frac{p-1}{2} = 2u^2+13$.

[2] if $a \in C_0$ then $a \cdot C_\ell = C_\ell$, $\forall \ell$.

[3] $C_\ell(x) \triangleq \sum_{k=0}^{f-1} x^{g^{6k+\ell}} = \sum_{k=0}^{f-1} x^{3^\ell \cdot g^{6k}}$

Pf: $3 \in C_1 \rightarrow 3 = g^{6s+1}$ some s

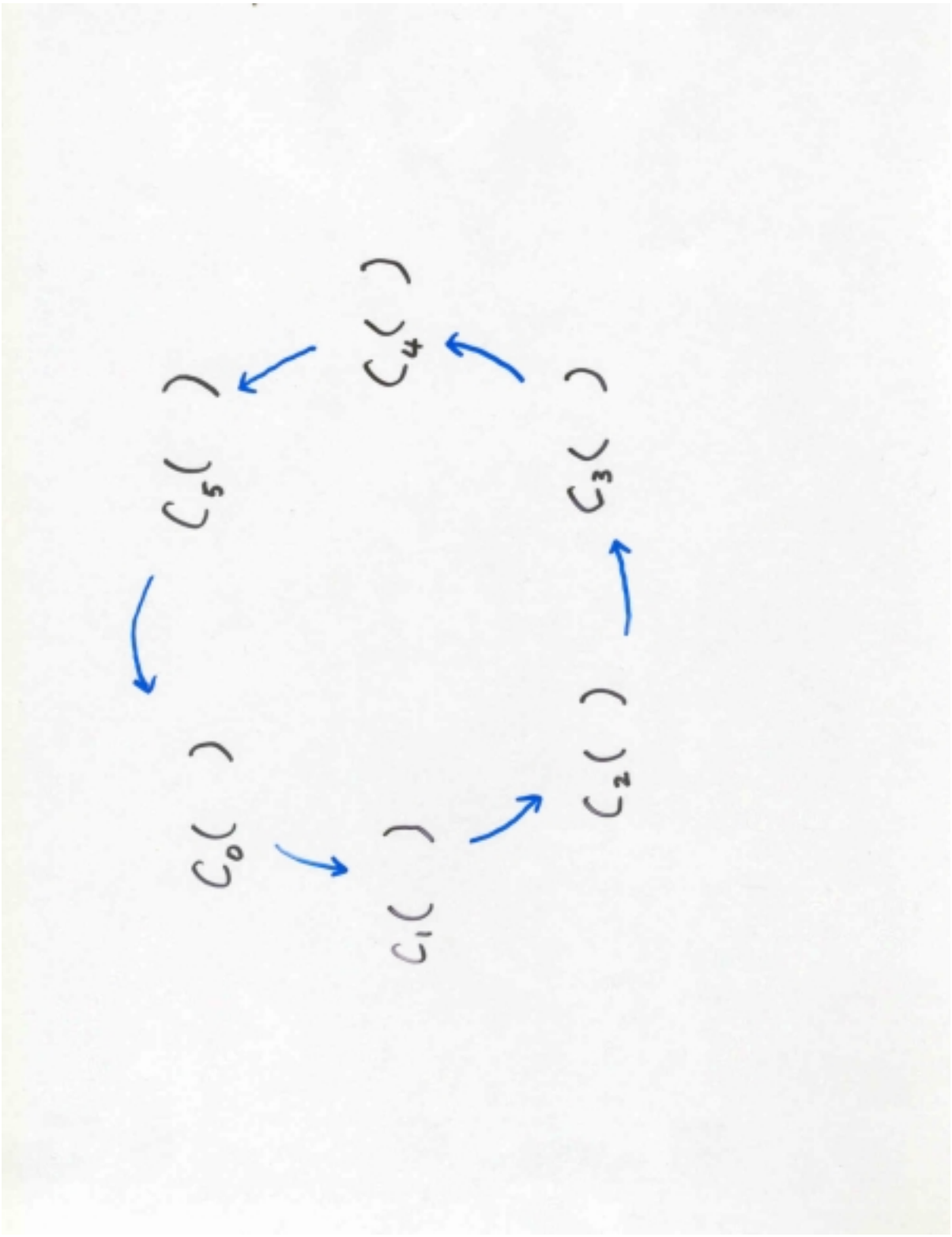
$\therefore 3^\ell \cdot g^{6k} = g^{6\ell s+\ell} \cdot g^{6k} = g^{6(\ell s+k)+\ell}$.

[4] Let β be a primitive p^{th} root of 1. Then

$$C_\ell(\beta^3) = \sum_{k=0}^{f-1} \beta^{3 \cdot 3^\ell \cdot g^{6k}} = C_{\ell+1}(\beta)$$

↖ mod 6.

seta09_2.jpg (1528x1920x16M jpeg)



in particular, we have

$$C_0(\beta^{3^l}) = C_1(\beta^{3^{l-1}}) = \cdots = C_l(\beta).$$

[5] $C_l(\beta^i) = C_l(\beta^j)$ if i & j belong to the same residue class.

Pf: $i = g^{6a+m}$, $j = g^{6b+m}$. Then

$$C_l(\beta^i) = \sum_{k=0}^{f-1} \beta^{g^{6k+l+6a+m}} = \sum_{k=0}^{f-1} \beta^{g^{6k+l+6b+m}} = C_l(\beta^j).$$

CASE: $p = 4u^2+27 = 6f+1 \equiv 3 \pmod 8 \Rightarrow S(\beta)\cdot S(\beta^{-1}) = 1$. ... [6]

CASE: $p = \cdots \equiv 7 \pmod 8 \Rightarrow S(\beta)\cdot S(\beta^{-1}) = 0$.

Pf. $S(x) = C_0(x) + C_1(x) + C_3(x)$

$= \sum_{i\in D} x^i$ where $D = C_0 \cup C_1 \cup C_3$ is a

cyclic $(p, \frac{p-1}{2}, \frac{p-3}{4})$-difference set.

$\therefore S(x)\cdot S(x^{-1}) \equiv (k-\lambda) + \lambda\cdot\sum_{i=0}^{v-1} x^i \equiv (u^2+7) + (u^2+6)\cdot\sum_{i=0}^{p-1} x^i \pmod{x^p-1}$

Note $p = 4u^2+27 \equiv \begin{cases} 3 \pmod 8 \leftrightarrow u = \text{even} \leftrightarrow u^2+7 = \text{odd} \\ 7 \pmod 8 \leftrightarrow u = \text{odd} \leftrightarrow u^2+7 = \text{even}. \end{cases}$

What we have done for the case of $p \equiv 3 \pmod 8$:

[6] says: $S(\beta) \cdot S(\beta^{-1}) = 1$ for any primitive p^{th} root of 1

$\Rightarrow S(\beta) \neq 0$ for any such β.

$\Rightarrow S(\beta^j) \neq 0$ for $j = 1, 2, \cdots, p-1$.

For $j=0$,

$$S(1) = C_0(1) + C_1(1) + C_3(1) = \frac{p-1}{2} = 2u^2 + 13 = 1$$

Therefore $$L = p - \left| \{ j \mid S(\beta^j) = 0,\ 0 \le j \le p-1 \} \right| = p.$$

[7] It is well-known that 2 is a cubic residue mod p.

$$\Rightarrow 2 \in C_0 \cup C_3 .$$

Therefore

$p \equiv 3 \pmod 8 \Leftrightarrow 2$ is a QNR mod $p \Leftrightarrow 2 \in C_3$

$p \equiv 7 \pmod 8 \Leftrightarrow 2$ is a QR mod $p \Leftrightarrow 2 \in C_0$

[8] $-1 \in C_3$ $\because$ -1 is a cubic residue & quadratic non-residue mod p.

[9] $C_\ell(\beta^a) = C_\ell(\beta)$ for $a \in C_0$

"
$$\sum_{k=0}^{f-1} \beta^{a \cdot g^{6k+\ell}} = \sum_{k=0}^{f-1} \beta^{g^{6(i+k)+\ell}} = C_\ell(\beta), \quad (a = g^{6i} \text{ some } i)$$

Assume $p \equiv 7 \pmod 8$ in the remaining.

[6] says $S(\beta) \cdot S(\beta^{-1}) = 0$ in this case.

$3 \in C_1, 2 \in C_0, -1 \in C_3$

Now,

[7] $\Rightarrow$ $2 \in C_0$

[9] $\Rightarrow$ $C_\ell(\beta^2) = C_\ell(\beta)$

Since $C_\ell(\beta^2) = C_\ell(\beta)^2$

$\Rightarrow$ $C_\ell(\beta) \in \{0, 1\}$ ... [10]

Observe that

$$C_0(\beta) + C_1(\beta) + \cdots + C_5(\beta) = \sum_{i \in C_0 \cup \cdots \cup C_5} \beta^i = \sum_{i=1}^{p-1} \beta^i = 1 \quad \cdots [11]$$

[12]

$$\begin{aligned} C_0(\beta)+C_3(\beta) &= 1 \\ C_1(\beta)+C_4(\beta) &= 1 \\ C_2(\beta)+C_5(\beta) &= 1 \end{aligned} \quad \left\{\begin{matrix}1\\1\\0\end{matrix}\right\} \text{or} \left\{\begin{matrix}1\\0\\1\end{matrix}\right\} \text{or} \left\{\begin{matrix}0\\1\\1\end{matrix}\right\} \text{or} \left\{\begin{matrix}0\\0\\0\end{matrix}\right\}$$

claim that ⇑ is impossible.

pf: [4] $\Rightarrow C_k(\beta^3) = C_{k+1}(\beta)$. since $3 \in C_1$.

$\therefore$ $C_1(\beta)+C_4(\beta) = C_0(\beta^3)+C_3(\beta^3)$

$C_2(\beta)+C_5(\beta) = C_0(\beta^{3^2})+C_3(\beta^{3^2})$

$\therefore$ If $C_0(\beta)+C_3(\beta) = C_1(\beta)+C_4(\beta) = C_2(\beta)+C_5(\beta) = 1$,

$\Rightarrow C_0(\beta)+C_3(\beta) = C_0(\beta^3)+C_3(\beta^3) = C_0(\beta^{3^2})+C_3(\beta^{3^2}) = 1$.

Furthermore, $C_0(\beta^{3^3})+C_3(\beta^{3^3}) = C_3(\beta)+C_0(\beta) = 1$, etc.

$\cdots \Rightarrow C_0(x)+C_3(x)+1 = 0$ has roots $\beta, \beta^3, \beta^{3^2}, \cdots\cdots$

$\Rightarrow C_1(x) + C_4(x) + 1 = 0$ has roots $\beta, \beta^3, \beta^{3^2}, \ldots$.

Now, [5] $\Rightarrow C_\ell(\beta^i) = C_\ell(\beta^j)$ for $i, j \in C_k$

Therefore

$C_1(x) + C_4(x) + 1 = 0$ has $p-1$ roots β^i $(i \in C_0 \cup C_1 \cup \cdots \cup C_5)$

↑

But this has degree $< p-1$

since $x^{p-1} \equiv x^{-1} \pmod{x^p - 1}$, and $-1 \in C_3$ by [8].

(i.e. $-1 \notin C_1 \cup C_4$) ∎

Theorem Let $p = 6f+1 \equiv 7 \pmod 8$
$= 4u^2+27$

Then, there exists a primitive p^{th} root β of 1 such that $S(\beta) = 1$.

For such β, we have $S(\beta^j) = 0$ for $j \in C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5$

Remark: Then the main result comes as a corollary.

Since $\left| \{ j \mid S(\beta^j) = 0,\ 0 \le j \le p-1 \} \right| = \frac{5}{6}(p-1)$

Note: $S(1) = C_0(1) + C_1(1) + C_3(1) = \frac{p-1}{2} = 3 \cdot f = 1$.
$(\because f = \text{odd})$

Existence: Let η be a primitive p^{th} root of 1.

Consider $$\sum_{i=1}^{p-1} S(\eta^i) = \sum_{i=1}^{p-1} C_0(\eta^i) + \sum_{i=1}^{p-1} C_1(\eta^i) + \sum_{i=1}^{p-1} C_3(\eta^i)$$

$$= \sum_{j=0}^{5} \sum_{k=0}^{f-1} C_0\left(\eta^{g^{6k+j}}\right) + \cdots$$

↖ f summands are all the same by [5] ∵ f = odd.

$$= \sum_{j=0}^{5} C_0(\eta^{g^j}) + \cdots$$

by [5], and g^j and 3^j belong to the same class

$$= \sum_{j=0}^{5} C_0(\eta^{3^j}) + \sum_{j=0}^{5} C_1(\eta^{3^j}) + \sum_{j=0}^{5} C_3(\eta^{3^j})$$

↖ they are the same. ↗

$$= \sum_{j=0}^{5} C_j(\eta)$$

$$= 1. \qquad \therefore\ S(\eta^i) = 1 \text{ for at least one } i.$$

Now, we will show that, for such β,

$$S(\beta^j) = 0 \quad \text{for } j \in C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5.$$

$$\Leftrightarrow \quad S(\beta^{3^i}) = 0 \quad \text{for } i = 1, 2, 3, 4, 5.$$

$\because$

- $S(x) \triangleq C_0(x) + C_1(x) + C_3(x)$
- $C_\ell(\beta^{3^i}) = C_\ell(\beta^j)$ if 3^i & j belong to the same class
- $3^i \in C_i$ for $i = 0, 1, 2, 3, 4, 5$

⊙ We will eventually determine the value of

$$C_\ell(\beta) \quad \text{for } \ell = 0, 1, 2, \cdots, 5.$$

⊙ By the choice of β,

$$1 = S(\beta) = C_0(\beta) + C_1(\beta) + C_2(\beta) \rightarrow S(\beta^j) = 1 \text{ for } j \in C_0$$

20)

$$\begin{cases} 1 = S(\beta) = C_0(\beta) + C_1(\beta) + C_3(\beta) \\ 0 = S(\beta^{-1}) = S(\beta^3) = C_3(\beta) + C_4(\beta) + C_0(\beta) \end{cases} \rightarrow S(\beta^{-1}) = 0 = S(\beta^3)$$

$$\Rightarrow 1 = S(\beta) + S(\beta^{-1}) = C_1(\beta) + C_4(\beta)$$

$$\rightarrow \begin{cases} C_2(\beta) + C_5(\beta) = 0 \\ C_0(\beta) + C_3(\beta) = 0 \end{cases} \rightarrow \begin{cases} C_1(\beta) = 1 \\ C_4(\beta) = 0 \end{cases}$$

$$\begin{cases} S(\beta^3) = C_1(\beta) + C_2(\beta) + C_4(\beta) = C_2(\beta) + 1 \\ S(\beta^{-3}) = S(\beta^4) = C_4(\beta) + C_5(\beta) + C_0(\beta) = C_5(\beta) + 1 \end{cases}$$

$$\Rightarrow 0 = S(\beta^3) \cdot S(\beta^{-3}) = (C_2(\beta) + 1) \cdot (C_5(\beta) + 1) \rightarrow C_2(\beta) = C_5(\beta) = 1$$

$$\rightarrow S(\beta^4) = S(\beta^{-3}) = 0 = S(\beta^3)$$

$$\begin{cases} S(\beta^{3^2}) = C_2(\beta) + C_3(\beta) + C_5(\beta) = C_3(\beta) \\ S(\beta^{-3^2}) = S(\beta^5) = C_5(\beta) + C_0(\beta) + C_2(\beta) = C_0(\beta) \end{cases}$$

$$\Rightarrow 0 = S(\beta^{3^2}) \cdot S(\beta^{-3^2}) = C_0(\beta) \cdot C_3(\beta) \rightarrow C_0(\beta) = C_3(\beta) = 0$$

$$\rightarrow S(\beta^{3^2}) = S(\beta^5) = 0$$

* Recently, we were able to prove that, for $p \equiv 7 \pmod 8$

$$S(t) = 1 + \sum_{i=0}^{\frac{p+1}{6n}-1} tr_1^n\left(\beta^{-g^{6i}\cdot t}\right), \qquad 0 \le t \le p-1$$

But, we are not YET able to express

$\{S(t)\}$ as a sum of traces for $p \equiv 3 \pmod 8$

Above "representation" includes the 3 instances of Mersenne primes p for which Hall's sextic residue sequence of period p exists. .... earlier done by NO, CHUNG, YANG, SONG. ('98)

Proof of the Above representation is very much similar to that for the trace representation of Legendre sequences.

..... by KIM & SONG (2000)

(for Mersenne prime cases .... NO CHUNG YANG SONG)