# On the Hadamard Sequences

**Jeong-Heon Kim**

The Graduate School

Yonsei University

Department of Electrical and Electronic Engineering

# On the Hadamard Sequences

by

**Jeong-Heon Kim**

A Dissertation Submitted to the

Graduate School of Yonsei University

in partial fullfillment of the

requirements for the degree of

Doctor of Philosophy

Supervised by

Professor Hong-Yeop Song, Ph.D.

Department of Electrical and Electronic Engineering
The Graduate School

YONSEI University

December 2001

This certifies that the dissertation of
Jeong-Heon Kim is approved.

Thesis Supervisor: Hong-Yeop Song

Kyu Tae Park

Daesik Hong

DongKu Kim

Habong Chung

The Graduate School
Yonsei University
December 2001

# Contents

# List of Figures

# List of Tables

# ABSTRACT

## On the Hadamard Sequences

Jeong-Heon Kim
Department of Electrical and Electronic Eng.
The Graduate School
Yonsei University

In such systems as ranging systems, radar systems, and spread-spectrum communication systems, it needs to find sequences with good correlation property in order to improve the performance. The correlation property may be auto-correlation or cross-correlation according to the application. A binary sequence with ideal autocorrelation property are called a Hadamard sequence. In this thesis, Hadamard sequences and their properties(the linear complexity and the trace representation) are investigated. All known Hadamard sequences have periods of the following three types: (1)$N = 4k - 1$ is a prime number (2)$N = p(p + 2)$ is a product of twim primes (3)$N = 2^m - 1$, for $m = 2, 3, 4, \ldots$. It is conjectured that if a Hadamard sequence exists, the period $N$ of the Hadamard sequence must belong to one of the three types above. The conjecture is confirmed up to $N < 10000$, except for the the following 17 cases: 1295, 1599, 1935, 3135, 3439, 4355,

4623, 5775, 7395, 7743, 8227, 8463, 8591, 8835, 9135, 9215, 9423. We confirmed that there are no Hadamard sequences of periods $1295, 1599, 1935, 3135$.

Linear complexity of Hadamard sequences is investigated. we determined the linear complexity of Hall's sextic residue sequences and Jacobi sequences including twin prime sequences. As a result, the linear complexities of all Hadamard sequences which can be made by known construction methods were determined. A Hall's sextic residue sequence of period $p$ has the following linear comlexity.

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

Note that if $p \equiv 3 \pmod 8$, the Hall's sextic residue sequence of period $p$ has maximum linear complexity. The linear complexity of Jacobi sequences of period $pq$ can be classified as 10 cases according to $p \pmod 8$ and $q \pmod 8$, which are given in Table 3.2. Twin prime sequences of period $p(p+2)$ are given by

$$L = \begin{cases} \frac{p^2+4p-1}{2} & \text{if } p = 7 \pmod 8 \\ \frac{p^2-1}{2} & \text{if } p = 3 \pmod 8 \\ p(p+2) - 1 & \text{if } p = 1 \pmod 8 \text{ or } p = 5 \pmod 8 \end{cases}$$

which is the special case of Jacobi sequences.

In order to give some commonalities to the three types of Hadamard sequences, we investigate trace representation of Hadamard sequences. First, we give a general trace representation of Legendre sequences of all periods. There is close relation between the trace representation and linear complexity of a binary sequence. If the linear complexities of two binary sequences differ, the trace representations of those sequences differ too and vice versa. We determined the linear complexity of Hall's sextic residue sequences. As the linear complexity has different form with repect to the value of $p \pmod 8$, there

may be two forms in the trace representation of Hall's sextic residue sequences. we give one of them, the case of $p = 7 \pmod 8$.

**Key words :** ideal autocorrelation, Hadamard sequences, linear complexity, trace function representation

# Chapter 1

# Introduction

## 1.1 Motivation

In designing a communication system, one has to note that there is limited amount of resources. Such a restriction becomes more strict as the amount of information to transmit grows. Therefore, it needs to develop methods to use the available resources more efficiently. Signal design is one of solutions to this problem.

Communication systems in many cases require sets of signals which have the following properties [1] :

1. each signal in the set is easy to distinguish from the time shifted version of itself.
2. each signal in the set is easy to distinguish from (the possibly time-shifted version of) every other signal in the set.

As usual, the set of signals with the first property is said to have a good auto-correlation property and it is important for such applications as ranging systems, radar systems, and spread-spectrum communications systems. The set of signals with the second property is said to have a good cross-correlation property and it is important for simultane-

ous ranging to several targets, multiple-terminal system identification, and code-division multiple-access (CDMA) communication system.

In general, the simplification of system implementation requires the use of periodic signals. So, we restrict our attention to periodic signals in this thesis. In order to simplify the presentation, we consider the sets of signals of common period $T$. The following several paragraphs are some analysis of signals having good distinguishability by Sarwarte and Pursley [1].

One may use the mean-squared difference to measure the distinguishability of signals. For our purposes, two signals are easy to distinguish if and only if the mean-squared difference(MSD) between them is large. If modulation processes are involved, not only $x(t)$ but also $-x(t)$ must be considered. That is, we will require that

$$\begin{aligned} MSD &= \frac{1}{T}\int_0^T [y(t) \pm x(t)]^2\, dt \\ &= \frac{1}{T}\left\{\int_0^T [y^2(t) + x^2(t)]\, dt \pm 2\int_0^T x(t)y(t)dt\right\} \end{aligned} \tag{1.1}$$

is large.

Since the first integral on the right hand side of eq.(1.1) is the sum of the energy in $x(t)$ and $y(t)$ for $0 \le t \le T$, $y(t)$ is easy to distinguish from $x(t)$ if the magnitude of the quantity

$$r = \int_0^T x(t)y(t)dt \tag{1.2}$$

is small. For such communication, navigation, and radar systems as those with correlation receivers or matched filters, $r$ represents the output of the filter matched to the signal $y(t)$ when the input is $x(t)$. In a multiple-access communication system, for example,

$x(t)$ and $y(t)$ may represent the signals assigned to two different transmitters, in which case the parameter $r$ is a measure of the crosstalk interference between the two signals.

Properties 1 and 2 require the distinguishability of $x(t)$ and $y(t+\tau)$ for $0 \leq \tau \leq T$ if $x(t)$ and $y(t)$ are different signals, and for $0 < \tau < T$ if two signals are the same. Consequently, what we need to consider is the magnitude of the following cross-correlation function

$$r_{x,y}(\tau) = \int_0^T x(t)y(t+\tau)\,dt. \tag{1.3}$$

Due to the relative simplicity of their generation, the signals of interest for most applications are periodic signals which consist of sequences of elemental time-limited pulses. These pulses are all of the same shape, so that the signal can be written as

$$x(t) = \sum_{n=-\infty}^{\infty} x_n \psi(t - nT_c) \tag{1.4}$$

where $\psi(t)$ is the basic pulse waveform and $T_c$ is the time duration of this pulse. If $x(t) = x(t+T)$ for all $t$, then $T$ will be a multiple of $T_c$, and the sequence $(x_n)$ must be periodic with a period which is a divisor of $N = T/T_c$.

Suppose $x(t)$ and $y(t)$ are periodic as described above. $x(t)$ are given by eq.(1.4) and $y(t)$ is given by

$$y(t) = \sum_{n=-\infty}^{\infty} y_n \psi(t - nT_c). \tag{1.5}$$

Then it is easy to show that the parameter $r$ of eq.(1.2) is given by

$$r = \lambda \sum_{n=0}^{N-1} x_n y_n \tag{1.6}$$

where the constant $\lambda$ is

$$\lambda = \int_0^{T_c} \psi^2(t)\,dt \tag{1.7}$$

Thus, the inner product of continuous time signal $x(t)$ and $y(t)$ is proportional to the inner product of the corresponding vectors $(x_0, x_1, \cdots, x_{N-1})$ and $(y_0, y_1, \cdots, y_{N-1})$. Furthermore, if $\tau = lT_c$ it can be generalized to

$$r_{x,y}(\tau) = \lambda \sum_{n=0}^{N-1} x_n y_{n+l}. \tag{1.8}$$

Since $(y_n)$ is periodic with a period dividing $N$,

$$(y_l, y_{l+1}, \cdots, y_{l+N-1}) = (y_l, y_{l+1}, \cdots, y_{l-2}, y_{l-1}), \tag{1.9}$$

where the right-hand side of eq.(1.9) is the $l$th cyclic shift of $(y_0, y_1, \cdots, y_{N-1})$.

Above observation gives the motivation to consider the periodic cross-correlation function of the sequences $(x_n)$ and $(y_n)$ which is defined by

$$\theta_{x,y}(\tau) = \sum_{n=0}^{N-1} x_n y_{n+\tau}. \tag{1.10}$$

Since the periodic cross-correlation parameters for the continuous-time signals $x(t)$ and $y(t)$ of eq.(1.4) and eq.(1.5) are completely determined by the cross-correlation function, the signal design problem described at the beginning of this thesis can be reduced to the problem of finding the sets of periodic sequences with the following properties:

1. for each sequence $x = (x_n)$ in the set, $|\theta_{x,x}(\tau)|$ is small for $1 \leq \tau \leq N-1$.

2. for each pair of sequences $x = (x_n)$ and $y = (y_n)$, $|\theta_{x,y}(\tau)|$ is small for all $\tau$.

In recent years, the increasing interest in spread-spectrum communications and CDMA communications has led to a corresponding interest in aperiodic correlation parameters

and cross-correlation properties of periodic sequences. But the study of cross-correlation properties of periodic sequences requires the extensive study of auto-correlation properties as a preliminary. Generally, the set of sequences with low cross-correlation values are generated from the sequences with good auto-correlation property by some trade off between auto-correlation values and cross-correlation values. For instance, Gold and Kasami made sets of sequences with low cross-correlation values from the $m$-sequences [2] [3] [4] [5]. In addition, the sequences with ideal auto-correlation played one of the most important parts in several communication systems as previously mentioned. For example, those sequences are used as chip sequences in spread-spectrum communication systems and specifically an $m$-sequence of the period $2^{42} - 1$ with ideal auto-correlation is used in CDMA reverse channel for identification of each channel.

In this thesis, the main object is binary sequences with ideal auto-correlation called Hadamard sequences, which are formally defined as follows:

**Definition 1.1** A binary sequence $a = (a_i)$ of period $N$ where $N$ is odd is said to have an *ideal auto-correlation if the auto-correlation function* has $-1$ for all $\tau \neq 0$ and $N$ for $\tau = 0$ where auto-correlation function is defined as

$$R(\tau) = \sum_{i=0}^{N-1} (-1)^{a_i + a_{i+\tau}} \tag{1.11}$$

where subscript $i + \tau$ is taken modulo $N$. If the numbers of ones and zeros in a period differ by 1, then it is also said to be balanced and such a sequence is called *Hadamard sequence*.

We will investigate some existence problem of Hadarmard sequences and analyze some properties of those sequences, especially linear complexity and trace representation.

## 1.2 An Overview

In Chapter 2, we discuss the conjecture on the existence of Hadamard sequences. Some previous results concerning the conjecture are exhibited. Basic theory of Hadamard sequences is introduced. In Chapter 3, the linear complexity and the characteristic polynomial of Hall's sextic residue sequences and twin prime sequences are determined. In Chapter 4, the properties of Legendre sequences which are also Hadamard sequences are discussed. The trace representation of Legendre sequences of all period is determined. Partial result about the trace representation of Hall's sextic residue sequences is given. Finally, in Chapter 5, all those results of this thesis are summarized and some discussions follow.

# Chapter 2

# Binary Hadamard Sequences

Let $\{a_i\}, i = 0, 1, \ldots, N-1$ be a binary sequence of period $N$ where $N$ is odd. Reconsidering the auto-correlation function of binary sequences,

$$\begin{aligned} R(\tau) &= \sum_{i=0}^{N-1} (-1)^{a_i + a_{i+\tau}} \\ &= |\{i : a_i = a_{i+\tau}\}| - |\{i : a_i \neq a_{i+\tau}\}| \\ &= |\{i : a_i = a_{i+\tau} = 0\}| + |\{i : a_i = a_{i+\tau} = 1\}| \\ &\quad - \left(|\{i : a_i = 0, a_{i+\tau} = 1\}| + |\{i : a_i = 1, a_{i+\tau} = 0\}|\right). \end{aligned}$$

Let's define

$$\begin{aligned} x &= |\{i : a_i = a_{i+\tau} = 0\}|, \\ y &= |\{i : a_i = a_{i+\tau} = 1\}|, \\ z &= |\{i : a_i = 0, a_{i+\tau} = 1\}|, \\ w &= |\{i : a_i = 1, a_{i+\tau} = 0\}|. \end{aligned}$$

If $\{a_i\}$ is a Hadamard sequence, $R(\tau) = -1$ for all $\tau \equiv 0 \pmod{N}$ and the number of 1's in a period is $(N+1)/2$ and the number of 0's is $(N-1)/2$. Thus we have the

following equations:

$$x + y - (z + w) = R(\tau) = -1$$

$$x + y + z + w = N$$

$$x + z = (N - 1)/2$$

$$x + w = (N - 1)/2.$$

From the above four equations, one can conclude that $N \equiv -1 \pmod 4$. Therefore if a binary sequence is a Hadamard sequence, then the period must be $-1 \pmod 4$. All the known Hadamard sequences have periods of the following three types [6] [7]:

1. $N = 4n - 1$ is a prime number.
2. $N = p(p + 2)$ is a product of twin primes.
3. $N = 2^t - 1$, for $t = 2, 3, 4, \cdots$.

There is a conjecture that if a Hadamard sequence exists, the period $N$ must be one of the above three types [8]. In [6], it is reported that there are no other values of $N < 1000$ with Hadamard sequences of period other than those listed above, except for the six cases $N = 399, 495, 627, 651, 783,$ and 975, not fully investigated. In [7], Song and Golomb reconfirmed the conjecture for all $N < 1000$ including those six cases. Furthermore, it is verified up to $N < 10000$, except for the following 17 cases: 1295, 1599, 1935, 3135, 3439, 4355, 4623, 5775, 7395, 7743, 8227, 8463, 8591, 8835, 9135, 9215, 9423. The conjecture becomes more and more interesting since there seems to be no immediate common property among the three types of $v$ listed above and no counterexample has been discovered yet.

In this chapter, the four smallest previously unknown cases $v = 1295$,1599, 1935, 3135 are examined and confirmed the conjecture for all $v \leq 3435$. It will be discussed in the next section.

Out of three types of the period $N$, the case of $N = 2^n - 1$ gains its popularity because of its ease of implementation. There has been a lot of efforts to determine how many inequivalent Hadamard sequences of period $N = 2^n - 1$ there exist, and to figure out how to construct them systematically. So far, full search for these sequences has been completed up to $n = 10$.

## 2.1 Existence and non-existence of binary Hadamard sequences

A Hadamard sequence of period $N = 4n - 1$ is known to be equivalent to a $(v, k, \lambda)$-cyclic difference set with $v = 4n - 1, k = 2n - 1, \lambda = n - 1$.

**Definition 2.1** [6] Given a positive integer $v$, let $U$ denote the set of residues $\mod v$. Let $D$ be a $k$-subset of $U$. One calls $D$ a $(v, k, \lambda)$-cyclic difference set if for any non-zero $d \in U$, there are exactly $\lambda$ pairs of $(x, y), x, y \in D$ such that $d \equiv x - y \mod v$.

A $(v, k, \lambda)$-cyclic difference set with $v = 4n - 1, k = 2n - 1, \lambda = n - 1$ is called a cyclic Hadamard difference set, and it induces a binary sequence of period $v = 4n - 1$ with the ideal autocorrelation, a Hadamard sequence.

**Example 2.1** Let $D = \{0, 5, 7, 10, 11, 13, 14\}$. Then $D$ is a $(15, 7, 3)$-Hadamard difference set. Each nonzero $d < v$ can be written as differences modulo 15 of the following

three pairs.

$$1 = 0 - 14 = 11 - 10 = 14 - 13, \qquad 2 = 0 - 13 = 7 - 5 = 13 - 11,$$

$$3 = 10 - 7 = 13 - 10 = 14 - 11, \qquad 4 = 0 - 11 = 11 - 7 = 14 - 10,$$

$$5 = 0 - 10 = 5 - 0 = 10 - 5, \qquad 6 = 5 - 14 = 11 - 5 = 13 - 7,$$

$$7 = 5 - 13 = 7 - 0 = 14 - 7, \qquad 8 = 0 - 7 = 7 - 14 = 13 - 5,$$

$$9 = 5 - 11 = 7 - 13 = 14 - 5, \qquad 10 = 0 - 5 = 5 - 10 = 10 - 0,$$

$$11 = 7 - 11 = 10 - 14 = 11 - 0, \qquad 12 = 7 - 10 = 10 - 13 = 11 - 14,$$

$$13 = 5 - 7 = 11 - 13 = 13 - 0, \qquad 14 = 10 - 11 = 13 - 14 = 14 - 0.$$

Let $(a_i)$ be the binary sequence of period 15 in which $a_i = 0$ if $i \in D$ and $a_i = 1$ otherwise. Then it can be easily shown that $(a_i)$ is balanced and has ideal autocorrelation.

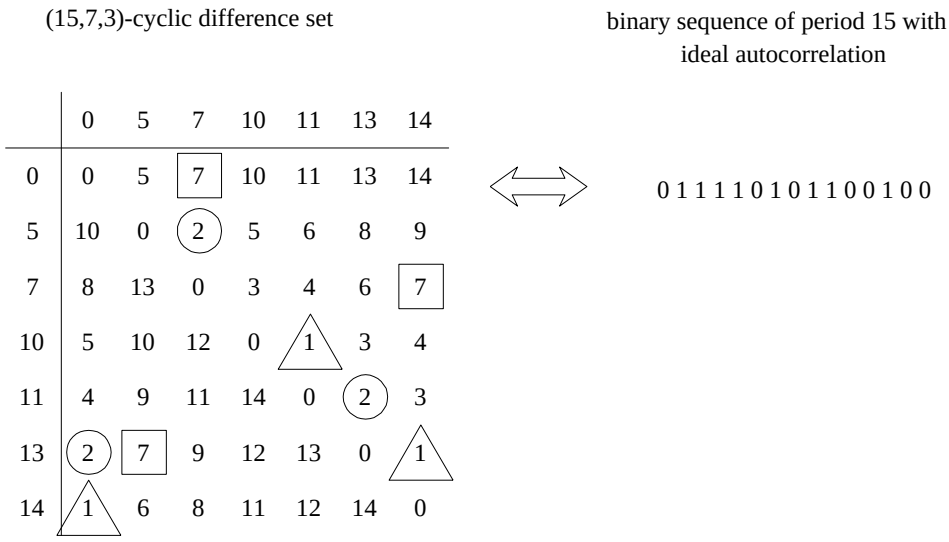


Figure 2.1: The difference set and Hadamard sequence of Example 2.1.

One of the most important properties of Hadamard difference sets is that it can have a multiplier. A multiplier of the Hadamard difference set can be defined as follows.

**Definition 2.2** Let $U$ be the $v$-set of the integers $0, 1, 2, \cdots, v-1$. An integer $t$ is called a *multiplier* of a $(v, k, \lambda)$-difference set $D = \{d_1, d_2, \cdots, d_k\}$ provided there exists a integer $s$ such that $E = \{td_1, td_2, \cdots, td_k\}$ and $E = \{d_1 + s, d_2 + s, \cdots, d_k + s\}$ are the same $k$-subset of $U$, where every operation is taken modulo $v$.

If a difference set $D = \{d_1, d_2, \cdots, d_k\}$ and $tD = \{td_1, td_2, \cdots, td_k\}$ are the same, then $D$ is said to be fixed by multiplier $t$. In [6], it is shown that if a difference set $D$ has a non-trivial multiplier $t$ [1], there is always a difference set $D'$ fixed by multiplier $t$. In fact, given a difference set $D$ and a multiplier $t$, there exist exactly $\gcd(t-1, v) = d$ shifts fixed by the multiplier $t$ [6]. Such a multiplier turns out to be very useful when one wants to exhaustively search for all the cyclic difference sets with given set of parameters.

Every known difference set has a non-trivial multiplier. But the question as to whether it is always true is open. Hall and Ryser proved the exitence of a non-trivial multiplier under certain circumstance in so-called the "mulitplier" theorem [6].

**Theorem 2.1** [6] Let $D$ be a $(v, k, \lambda)$-cyclic difference set. Let $d$ be a divisor of $k - \lambda$ and suppose that $(d, v) = 1$ and $d > \lambda$. If $t$ is an integer with the property that for each prime divisor $p$ of $d$ there is an integer $j$ such that $p^j \equiv t \pmod{v}$, then $t$ is a multiplier of $D$.

Baumert proved the following theorem which can be used to prove the non-existence of some cyclic Hadamard difference sets and can also be used to reduce the computa-

[1] "non-trivial" means $t \not\equiv 1 \pmod{v}$.

tional complexity of an exhaustive search.

**Theorem 2.2** [6] If a $(v, k, \lambda)$-cyclic difference set exists, then for every divisor $w$ of $v$, there exist integers $b_i$ $(i = 0, 1, 2, \cdots, w-1)$ satisfying the diophantine equations

$$\begin{aligned} \sum_{i=0}^{w-1} b_i &= k \\ \sum_{i=0}^{w-1} b_i^2 &= k - \lambda + v\lambda/w \\ \sum_{i=0}^{w-1} b_i b_{i-j} &= v\lambda/w, \quad \text{for } 1 \le j \le w-1 \end{aligned} \tag{2.1}$$

Here, the subscript $i - j$ is taken modulo $w$.

Basic steps to reach the nonexistence is the following. We assume first that a cyclic Hadamard difference set $D$ exists. By Theorem 2.1, its multiplier $m$ can be determined. For every divisor $w$ of $v$, its cyclotomic cosets can be determined by the multiplier $m$. We set some dummy indicators $b_i$ for each cyclotomic coset. There must be some sets of $b_i$'s satisfying the three diophantine equations in Theorem 2.2 if there exists a cyclic Hadamard difference set $D$. Thus, if these equations do not possess any solution for some divisor $w$, the non-existence is guaranteed.

### 2.1.1 Some computation

If there exists a $(1295, 647, 323)$-cyclic Hadamard difference set $D$, it must have the multiplier 16 by Theorem 2.1. There are 155 cyclotomic cosets modulo 1295. One needs to consider the cyclotomic cosets modulo each divisor of 1295.

Since $1295 = 5 \times 7 \times 37$, if there exists a $(1295, 647, 323)$-cyclic Hadamard difference set $D$, there must be integers satisfying the three diophantine equations in The-

orem 2.2 for each divisor $5, 7, 37, 35, 185,$ and $259$. Otherwise, one can conclude that there is no $(1295, 647, 323)$-cyclic Hadamard difference set.

For the divisor $w = 5$, we have the following equations :

$$\begin{aligned} \sum_{i=0}^{4} b_i &= 647 \\ \sum_{i=0}^{4} b_i^2 &= 83981 \\ \sum_{i=0}^{4} b_i b_{i+j} &= 83657, \text{ where } 1 \le j \le 4 \end{aligned} \tag{2.2}$$

and $0 \le b_i \le 255$. There are two solutions for $b_i$'s satisfying (2.2), which are

$$(b_0, b_1, b_2, b_3, b_4) = \begin{cases} (115, 133, 133, 133, 133) \\ (133, 115, 133, 133, 133) \end{cases}$$

For the divisor $w = 7$, we have the following equations :

$$\begin{aligned} \sum_{i=0}^{6} c_i &= 647 \\ \sum_{i=0}^{6} c_i^2 &= 60079 \\ \sum_{i=0}^{6} c_i c_{i+j} &= 59755, \text{ where } 1 \le j \le 6 \end{aligned} \tag{2.3}$$

and $0 \le c_0, c_1, c_2, c_3, \cdots, c_6 \le 175$. There are two solutions for $c_i$'s satisfying (2.3), which are

$$(c_0 = 77,\ c_1 = c_2 = c_4 = 95,\ c_3 = c_5 = c_6 = 95), \qquad \text{and}$$

$$(c_0 = 104,\ c_1 = c_2 = c_4 = 86,\ c_3 = c_5 = c_6 = 95)$$

For the divisor $w = 37$, we have the following equations :

$$\begin{aligned} \sum_{i=0}^{36} d_i &= 647 \\ \sum_{i=0}^{36} d_i^2 &= 11629 \\ \sum_{i=0}^{36} d_i d_{i+j} &= 11305, \text{ where } 1 \leq j \leq 36 \end{aligned} \tag{2.4}$$

and $0 \leq d_0, d_1, d_2, d_3, \cdots, d_{36} \leq 35$. There is only one solution.

$$\begin{aligned} d_0 &= 35, \\ d_1 = d_7 &= \cdots = d_{34} = 17, \\ d_2 = d_{14} &= \cdots = d_{32} = 17, \\ d_3 = d_4 &= \cdots = d_{36} = 17, \\ d_5 = d_6 &= \cdots = d_{35} = 17. \end{aligned}$$

For the divisor $w = 185$, we have the following equations :

$$\begin{aligned} \sum_{i=0}^{184} h_i &= 647 \\ \sum_{i=0}^{184} h_i^2 &= 2585 \\ \sum_{i=0}^{184} h_i h_{i+j} &= 2261, \text{ where } 1 \leq j \leq 184 \end{aligned} \tag{2.5}$$

Here, we use another dummy indicator $g_i$ which is related to $h_i$ by the following :

$$
\begin{aligned}
&g_0 = h_0 \\
&g_1 = h_{10} = h_{70} = \cdots = h_{160} \\
&g_2 = h_{15} = h_{20} = \cdots = h_{180} \\
&g_3 = h_{25} = h_{20} = \cdots = h_{175} \\
&g_4 = h_5 = h_{35} = \cdots = h_{170} \\
&g_5 = h_{111} \\
&g_6 = h_1 = h_{16} = \cdots = h_{181} \\
&g_7 = h_{31} = h_{51} = \cdots = h_{166} \\
&g_8 = h_{11} = h_{21} = \cdots = h_{176} \\
&g_9 = h_6 = h_{56} = \cdots = h_{171} \\
&g_{10} = h_{37} \\
&g_{11} = h_7 = h_{12} = \cdots = h_{182} \\
&g_{12} = h_2 = h_{32} = \cdots = h_{177} \\
&g_{13} = h_{27} = h_{62} = \cdots = h_{152} \\
&g_{14} = h_{17} = h_{22} = \cdots = h_{167} \\
&g_{15} = h_{148} \\
&g_{16} = h_{33} = h_{38} = \cdots = h_{158} \\
&g_{17} = h_{18} = h_{68} = \cdots = h_{168} \\
&g_{18} = h_3 = h_{28} = \cdots = h_{178} \\
&g_{19} = h_8 = h_{13} = \cdots = h_{183} \\
&g_{20} = h_{74} \\
&g_{21} = h_9 = h_{34} = \cdots = h_{174} \\
&g_{22} = h_{14} = h_{24} = \cdots = h_{179} \\
&g_{23} = h_4 = h_{64} = \cdots = h_{184} \\
&g_{24} = h_{19} = h_{54} = \cdots = h_{154}
\end{aligned}
\tag{2.6}
$$

and $0 \leq g_i \leq 7$ for $0 \leq i \leq 24$. In addition, since $185 = 5 \times 37$, there are relations

between $g_i$'s and the previous variables as follows :

$$\begin{aligned}
b_0 &= g_0 + 9(g_1 + g_2 + g_3 + g_4) & d_0 &= g_0 + g_5 + g_{10} + g_{15} + g_{20} \\
b_1 &= g_5 + 9(g_6 + g_7 + g_8 + g_9) & d_1 &= g_1 + g_6 + g_{11} + g_{16} + g_{21} \\
b_2 &= g_{10} + 9(g_{11} + g_{12} + g_{13} + g_{14}) & d_2 &= g_2 + g_7 + g_{12} + g_{17} + g_{22} \\
b_3 &= g_{15} + 9(g_{16} + g_{17} + g_{18} + g_{19}) & d_3 &= g_3 + g_8 + g_{13} + g_{18} + g_{23} \\
b_4 &= g_{20} + 9(g_{21} + g_{22} + g_{23} + g_{24}) & d_5 &= g_4 + g_9 + g_{14} + g_{19} + g_{24}
\end{aligned} \tag{2.7}$$

Recall that $(b_0, b_1, b_2, b_3, b_4)$ were already determined as (115, 133, 133, 133, 133) or (133, 115, 133, 133, 133), and $(d_0, d_1, d_2, d_3, d_5)$ were also determined as $(35, 17, 17, 17, 17)$. By executing a C program for a few hours of cpu time(Intel Pentium PC), we could confirm that there is no solution for $g_i$'s satisfying both the diophantine equations (2.5) and the above relations (2.7). Thus, one can conclude that there does not exist a $(1295, 647, 323)$-cyclic Hadamard difference set.

Similarly, the three cases $v = 1599, 1935,$ and $3135$ can also be examined and it turns out that no cyclic Hadamard difference set with $v = 1599, 1935$ or $3135$ exists. They can be summarized as follows.

- For $v = 1599$

  1. Multiplier is 25
  2. Number of cosets is 176
  3. Number of solutions for $w = 3$ is 2
  4. Number of solutions for $w = 41$ is 1
  5. Number of solutions for $w = 3 \times 41 = 123$ is 0

- For $v = 1935$

    1. Multiplier is 16
    2. Number of cosets is 175
    3. Number of solutions for $w = 3$ is 1
    4. Number of solutions for $w = 43$ is 10
    5. Number of solutions for $w = 3 \times 43 = 129$ is 0

- For $v = 3135$

    1. Multiplier is 49
    2. Number of cosets is 189
    3. Number of solutions for $w = 3$ is 5
    4. Number of solutions for $w = 5$ is 1
    5. Number of solutions for $w = 3 \times 5 = 15$ is 0

All of the above result in the smallest open case $v = 3439$ which is very special. The above analysis on the four cases basically depends on the existence of a multiplier. For the case $v = 3439$, we don't have any method to determine a multiplier. So far, we are not even sure of the existence of a multiplier in this case. The remaing 12 cases up to $v < 10000$ have relatively many cosets and the ranges of the possible solutions to the diophantine equations are much wider than the previous four cases. These result in the huge increase of complexity. It seems impossible to finish the exhaustive search in a reasonable amount of time.

## 2.2 Classification of cyclic Hadamard difference sets with $v = 2^n - 1$

In applications, Hadamard sequences of period $2^n - 1$ are most frequently used. Maximal length sequences, $m$-sequences in short, also belong to this family [9]. To describe Hadamard sequences of period $2^n - 1$, one can use the well-known trace function which is defined as follows [10]:

**Definition 2.1** The trace function $Tr_m^n(\cdot)$ is a linear mapping from $GF(2^n)$ to $GF(2^m)$, defined as

$$Tr_m^n(\alpha) = \alpha + \alpha^{2^m} + \alpha^{2^{2m}} + \cdots + \alpha^{2^{m(n/m-1)}}$$

where $m \mid n,\ \alpha \in GF(2^n)$.

Any two Hadamard sequences $a(i)$ and $b(i)$ of the same period $N$ are said to be equivalent if one can find integers $d$ and $s$ such that $a(i) = b(di + s)$ where $(d, N) = 1$ and $0 \leq s \leq N - 1$. Otherwise, we say that they are inequivalent. There have been some efforts to determine the number of inequivalent Hadamard sequences of period $2^n - 1$ for each $n$, which implies the classification of cyclic Hadamard difference sets(CHDS) with $v = 2^n - 1$, since every CHDS with $v = 2^n - 1$ is equivalant to a Hadamard sequence of period $2^n - 1$ by the well-known correspondence that, for each $i = 0, 1, \cdots, 2^n - 2$, $a(i) = 0$ if and only if $i \in D$. In this section, all the Hadamard sequences of period $2^n - 1$ for $n = 3, 4, \cdots, 10$ are classified and listed according to the known construction methods.

### 2.2.1 $(7, 3, 1)$-CHDS

There is only one $(7, 3, 1)$-CHDS. It is equivalent to an $m$-sequence which can be expressed as

$$s(t) = Tr_1^3(\alpha^t)$$

where $\alpha$ is a primitive element of $GF(2^3)$.

### 2.2.2 $(15, 7, 3)$-CHDS

There is only one $(15, 7, 3)$-CHDS. It is an $m$-sequence and its trace representation is

$$s(t) = Tr_1^4(\alpha^t)$$

where $\alpha$ is a primitive element of $GF(2^4)$.

### 2.2.3 $(31, 15, 7)$-CHDS

There are two inequivalent $(31, 15, 7)$-CHDS. Since 31 is a prime congruent to $3 \mod 4$, there must be a Legendre sequence of period 31. Let $\alpha$ be a primitive element of $GF(2^5)$.

- m31 ($m$-sequence) : $s(t) = Tr_1^5(\alpha^t)$.
- L31 (Legendre sequence) [11] : $s(t) = Tr_1^5(\alpha^t + \alpha^{5t} + \alpha^{7t})$.

### 2.2.4 $(63, 31, 15)$-CHDS

There are two $(63, 31, 15)$-CHDS. Let $\alpha$ be a primitive element of $GF(2^6)$.

- m63 ($m$-sequence) : $s(t) = Tr_1^6(\alpha^t)$.
- G63 (GMW-sequence) [12] :

$$s(t) = Tr_1^6(\alpha^t + \alpha^{15t})$$

### 2.2.5 $(127, 63, 31)$-CHDS

There are six $(127, 63, 31)$-CHDS [13]. Their trace representations are as follows where $\alpha$ is a primitive element of $GF(2^7)$.

- m127 ($m$-sequence) : $s_1(t) = Tr_1^7(\alpha^t)$.
- L127 (Legendre sequence) [11] :

$$s(t) = Tr_1^7(\alpha^t + \alpha^{9t} + \alpha^{11t} + \alpha^{13t} + \alpha^{15t} + \alpha^{19t} + \alpha^{21t} + \alpha^{31t} + \alpha^{47t})$$

- H127 (Hall's sextic residue sequence) [14] :

$$s(t) = Tr_1^7(\alpha^t + \alpha^{19t} + \alpha^{47t}).$$

- Miscellaneous sequences [15] [16] [17] :
  - M127-1 : $s(t) = Tr_1^7(\alpha^t + \alpha^{11t} + \alpha^{15t})$.
  - M127-2 : $s(t) = Tr_1^7(\alpha^t + \alpha^{3t} + \alpha^{7t} + \alpha^{19t} + \alpha^{29t})$.
  - M127-3 : $s(t) = Tr_1^7(\alpha^t + \alpha^{5t} + \alpha^{13t} + \alpha^{21t} + \alpha^{29t})$.

### 2.2.6 $(255, 127, 63)$-CHDS

There are four $(255, 127, 63)$-CHDS [18]. Their trace representations are as follows where $\alpha$ is a primitive element of $GF(2^8)$.

- m255 ($m$-sequence) : $s(t) = Tr_1^8(\alpha^t)$.
- G255 (GMW-sequence) [12] : $s(t) = Tr_1^8(\alpha^t + \alpha^{19t} + \alpha^{53t} + \alpha^{91t})$.
- Miscellaneous sequences [15] [16] [17] :

- M255-1 : $s(t) = Tr_1^8(\alpha^t + \alpha^{11t} + \alpha^{19t} + \alpha^{27t} + \alpha^{87t})$.
- M255-2 : $s(t) = Tr_1^8(\alpha^t + \alpha^{3t} + \alpha^{43t} + \alpha^{91t} + \alpha^{111t})$.

### 2.2.7 $(511, 255, 127)$-CHDS

There are five $(511, 255, 127)$-CHDS [19] [20]. Let $\alpha$ be a primitive element of $GF(2^9)$. Then the corresponding 5 binary sequences can be written as follows.

- m511 ($m$-sequence) : $s(t) = Tr_1^9(\alpha)$
- G511 (GMW-sequence) [12] : $s(t) = Tr_1^9(\alpha^t + \alpha^{11t} + \alpha^{43t})$.
- Miscellaneous sequences [15] [16] [17] [20] :
  - M511-1 : $s(t) = Tr_1^9(\alpha^t + \alpha^{23t} + \alpha^{31t})$.
  - M511-2 : $s(t) = Tr_1^9(\alpha^t + \alpha^{51t} + \alpha^{57t} + \alpha^{83t} + \alpha^{111t} + \alpha^{125t} + \alpha^{183t})$.
  - M511-3 : $s(t) = Tr_1^9(\alpha^t + \alpha^{7t} + \alpha^{57t} + \alpha^{77t} + \alpha^{83t} + \alpha^{103t} + \alpha^{111t} + \alpha^{127t} + \alpha^{183t})$.

### 2.2.8 $(1023, 511, 255)$-CHDS

There are ten $(1023, 511, 255)$-CHDS [21] [22]. Let $\alpha$ be a primitive element of $GF(2^{10})$.

- $m$-sequence (m1023) : $s(t) = Tr_1^{10}(\alpha^t)$.
- GMW-sequences [12] :
  - G1023-1 : $s(t) = Tr_1^{10}(\alpha^t + \alpha^{63t})$.
  - G1023-2 : $s(t) = Tr_1^{10}(\alpha^t + \alpha^{219t})$.
  - G1023-3 : $s(t) = Tr_1^{10}(\alpha^t + \alpha^{101t} + \alpha^{159t} + \alpha^{221t})$.

- G1023-4 : $s(t) = Tr_1^{10}(\alpha^t + \alpha^{39t} + \alpha^{157t} + \alpha^{221t})$.
- G1023-5 : $s(t) = Tr_1^{10}(\alpha^t + \alpha^{39t} + \alpha^{47t} + \alpha^{63t} + \alpha^{109t} + \alpha^{125t} + \alpha^{159t} + \alpha^{187t})$.

- Miscellaneous sequences [15] [16] [17] :
  - M1023-1 : $s(t) = Tr_1^{10}(\alpha^t + \alpha^{11t} + \alpha^{15t} + \alpha^{39t} + \alpha^{127t})$.
  - M1023-2 : $s(t) = Tr_1^{10}(\alpha^t + \alpha^{39t} + \alpha^{47t} + \alpha^{63t} + \alpha^{109t} + \alpha^{125t} + \alpha^{159t} + \alpha^{187t})$.
  - M1023-3 : $s(t) = Tr_1^{10}(\alpha^t + \alpha^{41t} + \alpha^{47t} + \alpha^{63t} + \alpha^{87t} + \alpha^{125t} + \alpha^{205t})$.
  - M1023-4 : $s(t) = Tr_1^{10}(\alpha^t + \alpha^{5t} + \alpha^{9t} + \alpha^{49t} + \alpha^{63t} + \alpha^{71t} + \alpha^{111t} + \alpha^{121t} + \alpha^{253t} + \alpha^{237t} + \alpha^{191t} + \alpha^{183t} + \alpha^{205t} + \alpha^{245t})$.

# Chapter 3

# Linear Complexity of Binary Sequences of Special Type

In real systems, binary sequences are usually generated by feedback shift registers. In cryptographic applications, they sometimes require sequences that cannot be easily generated by non-authorized party without some knowledge about the sequences. In such a situation, it would be desirable that the length of feedback shift registers that can generate the sequences are as long as possible. The linear complexity of a periodic binary sequence is defined as 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 [9]. It is equal to the degree $L$ of the feedback connection polynomial (or, the characteristic polynomial) of such a shift register. For applications of binary sequences to cryptographic systems, e.g. stream ciphers, or to spread spectrum communications, one usually prefers binary sequences with larger $L$ [23].

In this chapter, we determine the linear complexity of Hall's sextic residue sequences and twin prime sequences which have the ideal autocorrelation. Furthermore, we detemine the linear complexity of Jacobi sequences, a generalization of twin prime sequences.

## 3.1 The linear complexity of binary sequences

If a binary sequence $\{s_i\}$ of period $P$ has linear complexity $L$, 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.

It is known that the reciprocal characteristic polynomial $c^*(x)$ of the sequence $\{s(t)\}$ is given by [10]

$$c^*(x) = c_0 x^L + c_1 x^{L-1} + \cdots + c_{L-1}x + 1 = \frac{x^P - 1}{\gcd(x^P - 1, S(x))}$$

where

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

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

$$L = P - \deg[\gcd(x^P - 1, S(x))].$$

**Example 3.1** The characteristic polynomial of a binary $m$-sequence of period $2^n - 1$ is a primitive polynomial of degree $n$ over $GF(2)$. For example, if one wants to generate an $m$-sequence of period $2^4 - 1 = 15$, he only needs a linear feedback shift register with 5 stages. Let $c(x) = x^4 + x + 1$. Figure 3.1 shows the linear feedbak shift register with the connection polynomial $c(x) = x^4 + x + 1$ and Table 3.1 shows the values of each register with respect to the time index. A value sequence of a register is a shifted version of other registers and they are all $m$-sequences.

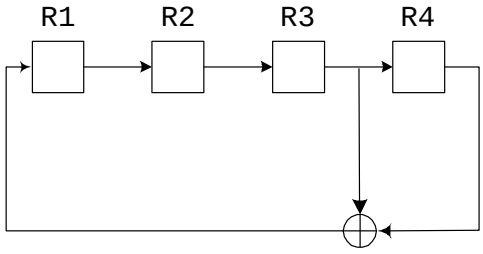


Figure 3.1: LFSR generating an $m$-sequence of period $15$

Table 3.1: The values of registers in Fig.3.1

| Time index | R1 | R2 | R3 | R4 |
|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 0 |
| 2 | 0 | 1 | 0 | 0 |
| 3 | 0 | 0 | 1 | 0 |
| 4 | 1 | 0 | 0 | 1 |
| 5 | 1 | 1 | 0 | 0 |
| 6 | 0 | 1 | 1 | 0 |
| 7 | 1 | 0 | 1 | 1 |
| 8 | 0 | 1 | 0 | 1 |
| 9 | 1 | 0 | 1 | 0 |
| 10 | 1 | 1 | 0 | 1 |
| 11 | 1 | 1 | 1 | 0 |
| 12 | 1 | 1 | 1 | 1 |
| 13 | 0 | 1 | 1 | 1 |
| 14 | 0 | 0 | 1 | 1 |
| 15 | 0 | 0 | 0 | 1 |

## 3.2 Linear complexity of Hall's sextic residue sequences

Let $p = 4u^2 + 27 = 6f + 1$ be a prime and $g$ be a primitive root modulo $p$ such that $3 \in C_1$ where

$$C_l = \{g^{6i+l} \mid i = 0, 1, \ldots, f-1\} \tag{3.1}$$

Hall's sextic residue sequence of period $p$ is defined as [24]

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

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

For Hall's sextic residue sequence of period $p$, the corresponding $S(x)$ is given by

$$\begin{aligned} S(x) &= s(0) + s(1)x + s(2)x^2 + \cdots + s(p-1)x^{p-1} \\ &= C_0(x) + C_1(x) + C_3(x) \end{aligned}$$

where, since $3 \in C_1$,

$$C_l(x) = \sum_{i \in C_l} x^i = \sum_{i=0}^{f-1} x^{3^l g^{6i}}. \tag{3.2}$$

Then the linear complexity of Hall's sextic residue sequence of period $p$ is given by

$$L = p - |\{j : S(\beta^j) = 0,\ 0 \le j \le p-1\}| \tag{3.3}$$

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

To determine the linear complexity of Hall's sextic residue sequences, we need the following lemma.

**Lemma 3.1** Let $p = 4u^2 + 27 = 6f + 1$ be a prime and $\beta$ be a primitive $p$th root of unity. Then the following are true.

P1. $|C_l| = (p-1)/6$, $aC_l = C_l$ for any $a \in C_0$ and $C_l(\beta) = C_0(\beta^{3^l})$.

P2. $C_l(\beta^a) = C_l(\beta)$ for any $a \in C_0$.

P3. $C_l(\beta^i) = C_l(\beta^j)$ if $i$ and $j$ are in the same class.

P4. If $2 \in C_0$, then $C_l(\beta) = 0$ or 1.

P5. $\sum_{l=0}^{5} C_l(\beta) = 1$.

P6. $-1 \in C_3$.

P7. If $p = 7 \pmod 8$ then $S(\beta)S(\beta^{-1}) = 0$. If $p = 3 \pmod 8$ then $S(\beta)S(\beta^{-1}) = 1$.

P8. If $p = 7 \pmod 8$ then $2 \in C_0$. If $p = 3 \pmod 8$ then $2 \in C_3$.

**Proof:** P1 is obvious from the definitions (1) and (2). If $a \in C_0$, then $a = g^{6i}$ for some integer $i$. Then $C_l(\beta^a) = \sum_{j=0}^{f-1} (\beta^{g^{6i}})^{3^l g^{6j}} = \sum_{j=0}^{f-1} \beta^{3^l g^{6(i+j)}} = C_l(\beta)$, which is P2. P3 is easily obtained by P2. If $2 \in C_0$, then $C_l(\beta)^2 = C_l(\beta^2) = C_l(\beta)$ by P2. Thus if $2 \in C_0$, $C_l(\beta) = 0$ or 1. P5 is proven by $\sum_{l=0}^{5} C_l(\beta) = \sum_{l=0}^{5} \sum_{i=0}^{f-1} \beta^{3^l g^{6i}} = \sum_{j=1}^{p-1} \beta^j = 1$. Since $3f = (p-1)/2 = 2u^2 + 13$, $f$ must be odd. Then P6 follows from the fact that $-1 = g^{(p-1)/2} = g^{(6f)/2} = g^{6(f-1)/2+3}$. For P7, we note that Hall's sextic residue sequence of period $p$ induces a cyclic Hadamard difference set with parameters $v = p, k = (p-1)/2$ and $\lambda = (p-3)/4$ [6]. Therefore, we have

$$S(x)S(x^{-1}) = u^2 + 7 + (u^2 + 6) \sum_{i=0}^{p-1} x^i \pmod{x^p - 1}.$$

P7 is obtained by substituting $\beta$ into $x$. P8 can be easily proved by observing that 2 is a cubic residue mod $p$ for any rational prime $p$ [25]. ■

**Lemma 3.2** Let $p = 4u^2 + 27 = 7 \pmod 8$ and $\beta$ be a primitive $p$th root of unity. Then one of $C_0(\beta) + C_3(\beta), C_1(\beta) + C_4(\beta)$ and $C_2(\beta) + C_5(\beta)$ is 1 and the others must be 0.

**Proof:** If $p = 7 \pmod 8$ then $2 \in C_0$. Then from P4 and P5 in Lemma 3.1, either one of $C_0(\beta) + C_3(\beta), C_1(\beta) + C_4(\beta)$ and $C_2(\beta) + C_5(\beta)$ is 1 or all three of them are 1. From P1 in Lemma 3.1, we have

$$C_1(\beta) + C_4(\beta) = C_0(\beta^3) + C_3(\beta^3) \tag{3.4}$$

$$C_2(\beta) + C_5(\beta) = C_0(\beta^{3^2}) + C_3(\beta^{3^2}). \tag{3.5}$$

Suppose that all of them are 1. Then from (4) and (5), $C_0(\beta^i) + C_3(\beta^i) = 1$ for all $i = 1, \ldots, p-1$. It also means that $C_1(\beta^i) + C_4(\beta^i) = 1$ for all $i = 1, \ldots, p-1$, which is impossible since the degree of $C_1(x) + C_4(x) + 1$ is less than $p - 1$. ■

**Theorem 3.1** Let $p = 6f + 1 = 7 \pmod 8$. Then there exists a primitive $p$th root $\beta$ of unity such that $S(\beta) = 1$, and for such $\beta$, we have $S(\beta^j) = 0$ for all $j \in C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5$.

**Proof:** Let $\gamma$ be a primitive $p$th root of unity. Then,

$$\begin{aligned}
\sum_{i=1}^{p-1} S(\gamma^i) &= \sum_{i=1}^{p-1} C_0(\gamma^i) + \sum_{i=1}^{p-1} C_1(\gamma^i) + \sum_{i=1}^{p-1} C_3(\gamma^i) \\
&= \sum_{j=0}^{5} C_0(\gamma^{3^j}) + \sum_{j=0}^{5} C_1(\gamma^{3^j}) + \sum_{j=0}^{5} C_3(\gamma^{3^j}) \\
&= \sum_{j=0}^{5} C_0(\gamma^{3^j}) \\
&= \sum_{k=0}^{p-2} \gamma^{g^k} \\
&= 1
\end{aligned}$$

Thus there exists at least one $i$ such that $S(\gamma^i) = 1$. Then $\beta = \gamma^i$ is what we want.

Now we will show that $S(\beta^j) = 0$ for all $j \in C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5$. From P3 in Lemma 3.1, it suffices to show that $S(\beta^{3^i}) = 0$ for $i = 1, \ldots, 5$. Recall that

$$S(\beta) = C_0(\beta) + C_1(\beta) + C_3(\beta) = 1. \tag{3.6}$$

P7 in Lemma 1 says $S(\beta)S(\beta^{-1}) = 0$, which concludes

$$S(\beta^{-1}) = S(\beta^{3^3}) = C_3(\beta) + C_4(\beta) + C_0(\beta) = 0. \tag{3.7}$$

Then we have $C_1(\beta) + C_4(\beta) = 1$ by adding two equations above and hence from Lemma 3.2,

$$C_0(\beta) + C_3(\beta) = C_2(\beta) + C_5(\beta) = 0.$$

From the above equation, (3.6) and (3.7), we also have $C_1(\beta) = 1$ and $C_4(\beta) = 0$. Furthermore

$$S(\beta^3) = C_1(\beta) + C_2(\beta) + C_4(\beta) = C_2(\beta) + 1$$

$$S(\beta^{-3}) = S(\beta^{3^4}) = C_4(\beta) + C_5(\beta) + C_1(\beta) = C_5(\beta) + 1$$

Since $C_2(\beta) = C_5(\beta)$, $S(\beta^3) = S(\beta^{3^4})$. But from P7 in Lemma 3.1, we have $S(\beta^3)S(\beta^{-3}) = 0$, which gives $S(\beta^3) = S(\beta^{3^4}) = 0$. Similarly, $S(\beta^{3^2}) = S(\beta^{3^5}) = 0$. ■

**Theorem 3.2** 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 $\beta$ is a primitive $p$th root of unity such that $S(\beta) = 1$. The linear complexity $L$ is given by

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

**Proof:** If $p \equiv 7 \pmod 8$, by Theorem 3.1 $S(\beta^a) = 1$ for $a \in C_0$ and $S(\beta^b) = 0$ for $b \in C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5$. Also $S(1) = [(p-1)/2 \pmod 2] = 1$. Thus $c^*(x)$ is given by

$$c^*(x) = \frac{(x^p - 1)}{\gcd(x^p - 1, S(x))} = (x-1)\prod_{i \in C_0}(x - \beta^i)$$

which is over $GF(2)$ since $2C_0 = C_0$. The linear complexity $L$ is $1 + (p-1)/6$.

If $p \equiv 3 \pmod 8$, by P7 in Lemma 3.1 we have $S(\beta^j)S((\beta^j)^{-1}) = 1$ for $j = 1, \ldots, p-1$. That is, $S(\beta^j) \neq 0$ for $j = 1, \ldots, p-1$. Also $S(1) = [(p-1)/2 \pmod 2] = 1$ because $p = 3 \pmod 8$. Thus $\gcd(x^p - 1, S(x)) = 1$ and hence $c^*(x) = x^p - 1$ and $L = p$. ■

**Example 3.2** Let $p = 4 \cdot 5^2 + 27 = 127$ and $\alpha$ be a primitive element in $GF(2^7)$ such that $\alpha^7 + \alpha + 1 = 0$. Then $\alpha$ is a primitive 127-th root of unity such that $S(\alpha) = 0$.

Thus the reciprocal of characteristic polynomial $c^*(x)$ is given by

$$\begin{aligned} c^*(x) &= (x-1)\prod_{i\in C_0}(x-\alpha^i) \\ &= (x-1)(x^7+x+1) \\ &\quad \cdot (x^7+x^6+x^5+x^4+1)(x^7+x^5+x^5+x^3+x^2+x+1) \end{aligned}$$

where $C_0 = \{3^{6i} \mid i = 0, 1, \cdots, 20\}$. ■

## 3.3 On the Linear Complexity of Binary Jacobi sequences of period $pq$

Define a Jacobi sequence $\{s(t)\}$ of period $pq$ for $t = 0, 1, 2, \ldots, pq-1$, where $p < q$ are distinct odd primes, as

$$s(t) = \begin{cases} 0 & \text{if } t \equiv 0 \pmod{pq} \\ 0 & \text{if } \left(\frac{t}{p}\right)\left(\frac{t}{q}\right) = 1 \\ 1 & \text{if } \left(\frac{t}{p}\right)\left(\frac{t}{q}\right) = -1 \\ 0 & \text{if } t \not\equiv 0 \pmod{p} \text{ and } t \equiv 0 \pmod{q} \\ 1 & \text{if } t \equiv 0 \pmod{p} \text{ and } t \not\equiv 0 \pmod{q} \end{cases} \tag{3.8}$$

where $\left(\frac{t}{p}\right)$ is the Legendre symbol defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p \\ -1 & \text{if } a \text{ is a quadratic non-residue of } p. \end{cases}$$

The above definition is a direct generalization of binary Legendre sequences in such a way that $s(t)$ takes on 1 or 0 according to whether the Jacobi symbol $\left(\frac{t}{pq}\right) = \left(\frac{t}{p}\right)\left(\frac{t}{q}\right)$ takes on $-1$ or 1, and $s(t)$ for other values of $t$ is assigned a value in the same way as the twin-prime sequence is assigned a value for an index which are multiples of $p$ or $q = p + 2$.

In this section, we determine the characteristic polynomial and the linear complexity of Jacobi sequences. Since twin prime sequences are special case of Jacobi sequences, we also determine those of twin prime sequences.

Let $\{s(t)\}$ be a Jacobi sequence of period $pq$ defined in (3.8), and let $R = \{0 \le i \le pq-1 \mid \left(\frac{i}{p}\right) \cdot \left(\frac{i}{q}\right) = 1\}$ and $N = \{0 \le i \le pq-1 \mid \left(\frac{i}{p}\right) \cdot \left(\frac{i}{q}\right) = -1\}$. Let

$$G(x) = s(0) + s(1)x + s(2)x^2 + \cdots + s(pq-1)x^{pq-1}.$$

Then from the definition of the Jacobi sequences, $G(x)$ can be rewritten by

$$G(x) = \sum_{i \in N} x^i + \sum_{i=1}^{q-1} x^{pi}.$$

As we already observed in section 5.1, the reciprocal characteristic poynomial of $\{s(t)\}$ is given by

$$(x^{pq}-1)/\gcd(x^{pq}-1, G(x))$$

and the linear complexity is

$$pq - \deg(\gcd(x^{pq}-1, G(x))).$$

**Lemma 3.3** Let $\beta$ be a primitive $pq$-th root over $GF(2^m)$ that is the splitting field of $x^{pq}-1$. Then $G(\beta^r) = G(\beta)$ for $r \in R$ and $G(\beta^n) = G(\beta)+1$ for $n \in N$. Furthermore, $G(\beta) \in \{0, 1\}$ if and only if $2 \in R$.

**Proof:** One can easily check that $(R, \cdot)$ is a group and $rR = R, nR = N, rN = N$ and $nN = R$ for any $r \in R$ and $n \in N$. Thus for $r \in R$,

$$G(\beta^r) = \sum_{i \in N} \beta^{ri} + \sum_{i=1}^{q-1} \beta^{rpi} = \sum_{i \in N} \beta^i + \sum_{i=1}^{q-1} \beta^{pi} = G(\beta). \tag{3.9}$$

For $n \in N$,

$$G(\beta^n) = \sum_{i \in N} \beta^{ni} + \sum_{i=1}^{q-1} \beta^{npi} = \sum_{i \in R} \beta^i + \sum_{i=1}^{q-1} \beta^{pi}. \tag{3.10}$$

Since $\beta$ is a primitive $pq$-th root of unity in $GF(2^m)$, $\beta^p$ and $\beta^q$ are primitive $q$-th and $p$-th root of unity respectively. Hence we have

$$\sum_{i=1}^{q-1} (\beta^p)^i = 1 \tag{3.11}$$

$$\sum_{i=1}^{p-1} (\beta^q)^i = 1. \tag{3.12}$$

Observing that

$$\sum_{i=0}^{pq-1} \beta^i = G(\beta) + G(\beta^n) + \sum_{i=1}^{q-1} (\beta^p)^i + \sum_{i=1}^{p-1} (\beta^q)^i + 1 = 0$$

from (3.9) and (3.10), we now know $G(\beta^n) = G(\beta) + 1$. The second statement is a consequence of the fact that $G(\beta)^2 = G(\beta^2) = G(\beta)$ if and only if $2 \in R$. ∎

Since $r \in R$ and $n \in N$ are relatively prime to $pq$, the above lemma gives us information about $G(\beta^i)$ where $(i, pq) = 1$. We now turn to the other case where $(i, pq) \neq 1$.

**Lemma 3.4** Let $\beta$ be a primitive $pq$-th root in $GF(2^m)$. Then we have

$$G(\beta^d) = \begin{cases} 0 & \text{if } (d, pq) = pq \\ 0 & \text{if } (d, pq) = p \text{ and } p \equiv 3, 7 \pmod 8 \\ 1 & \text{if } (d, pq) = p \text{ and } p \equiv 1, 5 \pmod 8 \\ 0 & \text{if } (d, pq) = q \text{ and } q \equiv 1, 5 \pmod 8 \\ 1 & \text{if } (d, pq) = q \text{ and } q \equiv 3, 7 \pmod 8 \end{cases}$$

**Proof:**

1. If $(d, pq) = pq$, then

$$G(\beta^d) = G(1) = \sum_{i \in N} 1 + \sum_{i=1}^{q-1} 1 = \frac{(p-1)(q-1)}{2} + q - 1 = 0.$$

2. If $(d, pq) = p$, then we can let $d = pk$ where $(k, q) = 1$. Using the fact that both $\beta^p$ and $\beta^{pk}$ are primitive $q$-th roots of unity and Remark 3.1, we obtain

$$\begin{aligned} G(\beta^d) = G(\beta^{pk}) &= \sum_{i \in N} \beta^{pki} + \sum_{i=1}^{q-1} (\beta^{pk})^{pi} \\ &= \sum_{i \in N} \beta^{pi} + \sum_{i=1}^{q-1} \beta^{pi} \\ &= \frac{p-1}{2} \cdot \left( \sum_{i=1}^{q-1} (\beta^p)^i \right) + 1 \\ &= \frac{p-1}{2} \cdot 1 + 1 \\ &= \begin{cases} 0 & \text{if } p \equiv 3, 7 \pmod 8 \\ 1 & \text{if } p \equiv 1, 5 \pmod 8. \end{cases} \end{aligned}$$

3. If $(d, pq) = q$, then we can let $d = ql$ where $(l, p) = 1$. Then similarly,

$$\begin{aligned} G(\beta^d) = G(\beta^{ql}) &= \sum_{i \in N} \beta^{qli} + \sum_{i=1}^{q-1} (\beta^{ql})^{pi} \\ &= \sum_{i \in N} \beta^{qi} + \sum_{i=1}^{q-1} 1 \\ &= \frac{q-1}{2} \cdot \left( \sum_{i=1}^{p-1} (\beta^q)^i \right) \\ &= \frac{q-1}{2} \cdot 1 \\ &= \begin{cases} 0 & \text{if } q \equiv 1, 5 \pmod 8 \\ 1 & \text{if } q \equiv 3, 7 \pmod 8. \end{cases} \end{aligned}$$

■

**Remark 3.1** Let $RN = \{0 \leq i \leq pq - 1 \mid \left(\frac{i}{p}\right) = 1 \text{ and } \left(\frac{i}{q}\right) = -1\}$ and $NR = \{0 \leq i \leq pq - 1 \mid \left(\frac{i}{p}\right) = -1 \text{ and } \left(\frac{i}{q}\right) = 1\}$. Then $N = RN \cup NR$. For any $i \in RN$, there are exactly $(q-1)/2$ elements in $RN$ such that they are all congruent

to $i$ mod $p$ and all distinct mod $q$. Similarly for any $i \in NR$. Therefore, we have $\sum_{i\in N}\beta^{pki} = \sum_{i\in N}\beta^{pi} = \frac{p-1}{2}\sum_{i=1}^{q-1}(\beta^p)^i$ in the proof of the second case of the lemma above. ■

**Remark 3.2** From Lemma 3.3, we know that $G(\beta^d) = 0$ if $pq|d$, which means that $x-1$ is always a factor of $G(x)$.

Now we are ready to determine the characteristic polynomial of Jacobi sequence $\{s(t)\}$ in (3.8). Consider first the case where $2 \in R$. From Lemma 3.3, we have $G(\beta) = 0$ or 1. Therefore, without loss of generality, we may let $G(\beta) = 0$ by renaming $\beta^n$ as $\beta$ if it is necessary. For this case where $2 \in R$, we assume that $\beta$ is a primitive $pq$-th root of unity such that $G(\beta) = 0$. We define the following polynomials for convenience:

$$
\begin{aligned}
r(x) &= \prod_{r\in R}(x-\beta^r) \\
n(x) &= \prod_{n\in N}(x-\beta^n) \\
p(x) &= \prod_{i=1}^{q-1}(x-\beta^{pi}) \\
q(x) &= \prod_{j=1}^{p-1}(x-\beta^{qj}).
\end{aligned}
$$

Clearly $(2,q) = 1$ and hence $\{\beta^{pi} \mid i = 1,2,\ldots,q-1\}$ and $\{\beta^{2pi} \mid i = 1,2,\ldots,q-1\}$ are the same set. Therefore $p(x)$ is the product of minimal polynomials of $\beta^{pi}, i = 1,2,\ldots,q-1$. Similarly $q(x)$ is the product of minimal polynomials of $\beta^{qi}, i = 1,2,\ldots,p-1$. Hence $p(x)$ and $q(x)$ are over $GF(2)$ (All coefficients of $p(x)$ and $q(x)$ are in $GF(2)$). If $2 \in R$, we know that $rR = R$ and $rN = N$ from Lemma 3.3. Then $r(x)$ and $n(x)$ are also products of some minimal polynomials and hence over

Table 3.2: Linear complexity of Jacobi sequences

| | $p \pmod 8$ | $q \pmod 8$ | $f(x)$ | $L$ |
|---|---|---|---|---|
| Case.1 | 1 | 1 | $p(x)n(x)$ | $(p+1)(q-1)/2$ |
| Case.2 | 1 | 7 | $p(x)q(x)n(x)$ | $(p+1)(q+1)/2-2$ |
| Case.3 | 3 | 3 | $q(x)n(x)$ | $(p-1)(q+1)/2$ |
| Case.4 | 3 | 5 | $n(x)$ | $(p-1)(q-1)/2$ |
| Case.5 | 5 | 5 | $p(x)n(x)$ | $(p+1)(q-1)/2$ |
| Case.6 | 7 | 7 | $q(x)n(x)$ | $(p-1)(q+1)/2$ |
| Case.7 | 1 | 3 | $r(x)n(x)p(x)q(x)$ | $pq-1$ |
| Case.8 | 1 | 5 | $r(x)n(x)p(x)$ | $p(q-1)$ |
| Case.9 | 3 | 7 | $r(x)n(x)q(x)$ | $q(p-1)$ |
| Case.10 | 5 | 7 | $r(x)n(x)p(x)q(x)$ | $pq-1$ |

$GF(2)$. The four polynomials $r(x), n(x), p(x), q(x)$ are factors of $x^{pq}-1$ and they do not have any common factor. Actually,

$$x^{pq}-1 = r(x)n(x)p(x)q(x)(x-1).$$

In the following theorem, we give the exact form of the characteristic polynomial and the linear complexity of Jacobi sequences using the lemmas described previously.

**Theorem 3.3** Let $\{s(t)\}$ be the sequence of period $pq$ as defined in (3.8). Then its reciprocal characteristic polynomial $f(x)$ and the linear complexity $L$ are given in Table 3.2. Here we distinguish 10 cases according to $p, q \equiv 1, 3, 5, 7 \pmod 8$.

**Proof:** As written in the beginning of this section, the reciprocal characteristic polyno-

mial $f(x)$ of Jacibi sequence of period $pq$ is given by

$$f(x) = \frac{x^{pq} - 1}{\gcd(x^{pq} - 1, G(x))}.$$

Therefore, what is to be done is just to find common factor of $x^{pq} - 1$ and $G(x)$. As we already noted, $x^{pq} - 1 = r(x)n(x)p(x)q(x)(x - 1)$ and $x - 1$ is always a factor of $G(x)$. Thus $x - 1 | \gcd(x^{pq} - 1, G(x))$.

For the first 6 cases, $2 \in R$. Therefore, Lemma 3.3 implies that $G(\beta^r) = G(\beta) = 0$ and $G(\beta^n) = 1$ for all $r \in R$ and $n \in N$. This gives $\gcd(r(x)n(x), G(x)) = r(x)$. For the remaining 4 cases, since $2 \notin R$, we have $\gcd(r(x)n(x), G(x)) = 1$.

In order to determine common factor of $p(x)q(x)$ and $G(x)$, one can use the result of Lemma 3.4. Consider Case 1 for example. In this case, we have $\gcd(r(x)n(x), G(x)) = r(x)$ because $2 \in R$. We also have $\gcd(p(x)q(x)(x - 1), G(x)) = q(x)(x - 1)$ from Lemma 3.4, since $G(\beta^{pi}) = 1$ for $1 \leq i \leq q - 1$, $G(\beta^{qi}) = 0$ for $1 \leq i \leq p - 1$, and $G(1) = 0$. Therefore, we have $\gcd(x^{pq} - 1, G(x)) = (x - 1)q(x)r(x)$ and hence $f(x) = p(x)n(x)$. All the other cases can be proved in the similar manner.

The linear complexity of a sequence is the degree of its characteristic polynomial. Thus we have to calculate the degrees of $r(x), n(x), p(x), q(x)$ to determine the linear complexity of Jacobi sequences. The degrees of $p(x)$ and $q(x)$ are obviously $q - 1$ and $p - 1$ respectively by definition. The degrees of $r(x)$ and $n(x)$ are the same as the cardinality of the set $R$ and $N$ respectively. Recall that $R$ is a subgroup of $\{i \mid 1 \leq i \leq pq - 1, (i, pq) = 1\}$ under multiplication and $N$ is the only coset of $R$. Thus $|R| = |N| = (p - 1)(q - 1)/2$, which is the degree of $r(x)$ and $n(x)$. Finally, the linear complexity is obtained by simple addition. ∎

**Corollary 3.1** The cases 2,4,7 and 10 of Theorem 3.3 covers the linear complexity and characteristic polynomial of twin prime sequences of period $p(p+2)$ where both $p$ and $p+2$ are prime.

**Remark 3.3** In this chapter, we determined the characteristic polynomial and the linear complexity of Jacobi sequences including twin prime sequences. In fact, Ding determined the linear complexity of twin prime sequences and its generalization in [26]. After we finished our work, we eventually found out that Ding had done the same thing. The methodologies of two indepedent works are almost same. Readers can refer [26] on behalf of their information. One can further extend the definition (3.8) to period $pqr$ where $p$, $q$ and $r$ are three distinct primes. It seems to be challenging but we believe after some calculations one can determine the characteristic polynomial and hence the linear complexity of these sequences of period $pqr$, which we omit here for the future research.

# Chapter 4

# Trace Representation of Hadamard Sequences

## 4.1 Introduction

As described in Chapter 2, the periods of all the known Hadamard sequences belong to one of the following three types.

I. $N = 4n - 1$ is a prime number.

II. $N = p(p + 2)$ is a product of twin primes.

III. $N = 2^t - 1$, for $t = 2, 3, 4, \cdots$.

In the case of type III, all the sequences from known construction methods can be represented as sums of trace function. For example, an $m$-sequence of period $2^n - 1$ can be represented as tr $\left(\alpha^t\right)$ where $\alpha$ is a primitive element of $GF(2^m)$. In the case of the other two types, there is no knowledge about the trace function representation of the sequences. The trace function representation of a sequence enables us to generate the sequence in more systematic way. Each term(trace function) in the representation corre-

sponds to a linear feedback shift register(LFSR) and consequently the sequence can be generated by a set of short LFSRs instead of comparatively long LFSR. We can use the set of LFSRs not only to obtain the sequence but also to generate other sequences which can be used in other parts of system.

There are three known construction methods in type I and II sequences. Legendre sequences and Hall's sextic residue sequences belong to type I and twin prime sequences belong to type II. In this chapter, we give full description on the trace function representation of Legendre sequences. Additionally, partial result about the trace function representation of Hall's sextic residue sequences is presented. Actually, Mersenne prime period case for Legendre sequences and Hall's sequences are already done by J.-S. No, et. al. in [11] and [14]. Some of our theorems in this chapter are generalized versions of No's results.

## 4.2 Legendre sequences

Legendre sequence $\{b(t)\}$ of period $p$ where $p$ is a prime is defined as [6, 9, 27]

$$b(t) = \begin{cases} 1 & \text{if } t \equiv 0 \mod p \\ 0 & \text{if } t \text{ is a quadratic residue mod } p \\ 1 & \text{if } t \text{ is a quadratic non-residue mod } p \end{cases} \tag{4.1}$$

If $p \equiv -1 \pmod 4$, the corresponding Legendre sequence is not only balanced but also has optimal autocorrelation property. Legendre sequences of period $p \equiv 1 \pmod 4$ do not have the ideal autocorrelation property. But their autocorrelation property is still good. The maximum amplitude of out-of-phase autocorrelation values is just 3. Here, we give an example which depicts the construction and autocorrelation property of Legendre sequences.

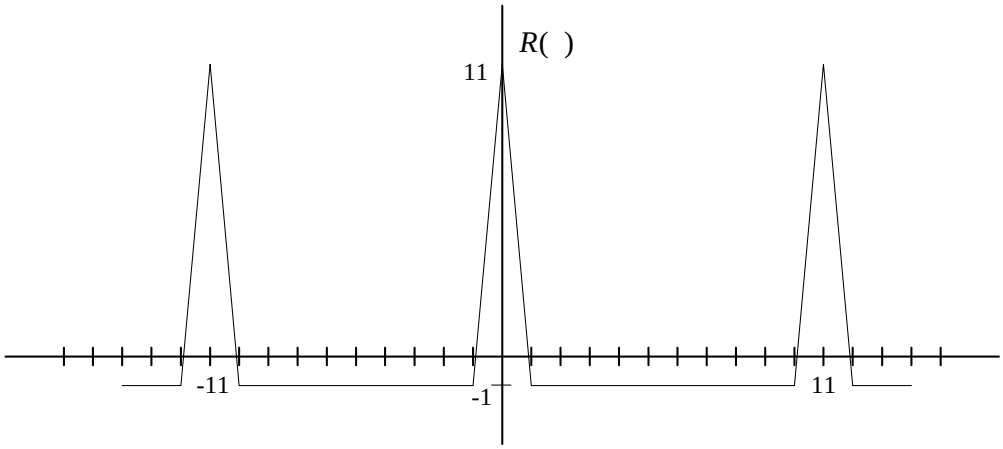


Figure 4.1: Autocorrelation function of Legendre sequence of period 11

**Example 4.1 Legendre sequence of period** $11 = 3 \pmod 4$ **:** 2 is a primitive root mod 11 and the powers of 2 mod 11 are given by

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| $2^i \pmod{11}$ | 1 | 2 | 4 | 8 | 5 | 10 | 9 | 7 | 3 | 6 |

From the definition of Legendre sequences,

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $s(i)$ | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 |

**Legendre sequence of period** $13 = 1 \pmod 4$ **:** 2 is a primitive root mod 13 and the powers of 2 mod 13 are given by

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $2^i \pmod{13}$ | 1 | 2 | 4 | 8 | 3 | 6 | 12 | 11 | 9 | 5 | 10 | 7 |

From the definition of Legendre sequences,

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $s(i)$ | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |

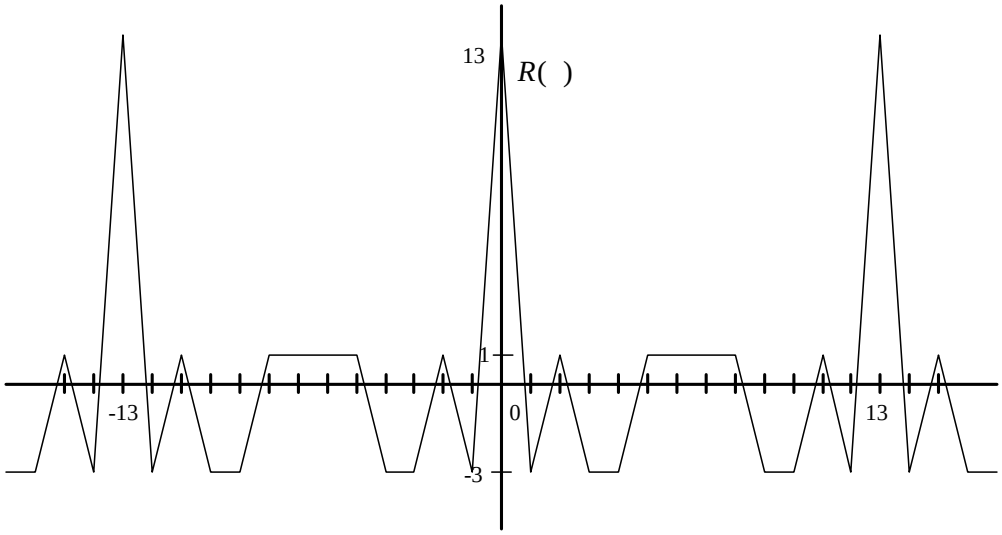


Figure 4.2: Autocorrelation function of Legendre sequence of period 13

In [27], the linear complexity of a Legendre sequence is determined, which was in fact already found in [28]. In [11], J.-S. No, *et. al.* have found the trace representation of Legendre sequences of Mersenne prime period. In this section, we give 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 section is a straightforward generalization of the result in [11].

## 4.3 Trace representation of Legendre sequences

In this section, we give the general trace representation of Legendre sequences of all prime periods. Legendre sequences have ideal auto-correlation if its period $p \equiv -1 \pmod 4$. So, they can be classfied as two families whether their periods are $-1 \pmod 4$

or $1 \pmod 4$. In the sense of linear complexity, it is a little bit different. Actually, they are classified according that their periods are $\pm 3 \pmod 8$ or $\pm 1 \pmod 8$. The following two subsections give the trace representations for the two families of Legendre sequences.

For convenience, we need the following lemma.

**Lemma 4.1** Let $p$ be an odd prime and $n$ be the order 2 mod $p$. Then there exists a primitive root $u$ mod $p$ such that $u^{(p-1)/n} \equiv 2 \pmod p$.

**Proof:** Let $g$ be a primitive root mod $p$. For every divisor $d$ of $p-1$, define

$$A_d = \{(g^i)^{\frac{(p-1)}{d}} | 1 \leq i \leq p-2, (i, p-1) = 1\}.$$

Every $x \in A_d$ has order $d$ and $A_d \cap A_{d'} = \varnothing$ for $d \neq d'$. Furthermore,

$$\bigcup_{d|p-1} A_d = \{1, 2, \cdots, p-2\}.$$

Thus one can say that $2 \in A_n$, which proves the lemma. ∎

In the remaining of this section, we use $u$ as a primitive root mod $p$ such that $u^{(p-1)/n} \equiv 2 \pmod p$.

### 4.3.1 When $p \equiv \pm 1 \pmod 8$

In this subsection, 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, $n$, the order of 2 mod $p$ divides $(p-1)/2$. Furthermore, if $i \equiv j \pmod{\frac{p-1}{n}}$, then we have $\mathrm{tr}\left(\beta^{u^i}\right) = \mathrm{tr}\left(\beta^{u^{\frac{p-1}{n}k+j}}\right) = \mathrm{tr}\left(\beta^{2^k u^j}\right) = \mathrm{tr}\left(\beta^{u^j}\right)$ for any $p$-th root of unity $\beta \in GF(2^n)$. All of these are summarized in the following:

**Lemma 4.2** 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 $\text{tr}\left(\beta^{u^i}\right) = \text{tr}\left(\beta^{u^j}\right)$ for any $p$-th root of unity $\beta \in GF(2^n)$.

**Theorem 4.1** 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

$$\sum_{i=0}^{\frac{p-1}{2n}-1} \text{tr}\left(\beta^{u^{2i}}\right) = 0 \tag{4.2}$$

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

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

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

$$\begin{aligned} \sum_{i=0}^{\frac{p-1}{2n}-1} \text{tr}\left(\gamma^{u^{2i}}\right) + \sum_{i=0}^{\frac{p-1}{2n}-1} \text{tr}\left((\gamma^u)^{u^{2i}}\right) &= \sum_{j=0}^{n-1} \left( \sum_{i=0}^{\frac{p-1}{2n}-1} (\gamma^{u^{2i}} + \gamma^{u^{2i+1}}) \right)^{2^j} \\ &= \sum_{j=0}^{n-1} \left( \sum_{i=0}^{\frac{p-1}{n}-1} (\gamma^{u^i}) \right)^{2^j} \end{aligned} \tag{4.3}$$

$$\text{Since } 2 = u^{(p-1)/n} \pmod p,$$

$$\begin{aligned} &= \sum_{j=0}^{n-1} \sum_{i=0}^{\frac{p-1}{n}-1} (\gamma^{u^{i+\frac{p-1}{n}j}}) \\ &= \sum_{k=0}^{p-2} \gamma^{u^k} = 1. \end{aligned} \tag{4.4}$$

Since one of the two summands in the left-hand side of (4.3) is 0 and the other is 1, either $\beta = \gamma$ or $\beta = \gamma^u$ is the primitive $p$-th root of unity satisfying (4.2).

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

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

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 4.2 and (4.2), therefore, we have

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

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

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

Since $\beta$ also satisfies the relation given from (4.3) up to (4.4), we have $s(1) + s(u) = 1$ and consequently $s(u) = 1$, which proves that $\{s(t)\}$ is the Legendre sequence of period $p$.

Let's care the other case $p \equiv 1 \pmod 8$. In this case $(p-1)/2$ is even. That is, $s(0) = 1 + \frac{p-1}{2} \cdot 1 = 1$. If $t$ is a quadratic residue mod $p$, then

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

Similarly to the first case, we have

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

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

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

Therefore we proved the theorem. ∎

**Example 4.2** The order of 2 mod 17 is 8 and a primitive root mod 17 is 6 such that $2 = 6^{(p-1)/8} = 6^2 \pmod{17}$. Let $\alpha$ be a primitive element of $GF(2^8)$ satisfying $\alpha^8 + \alpha^4 + \alpha^3 + \alpha^2 + 1 = 0$. Let $\beta = \alpha^{\frac{p-1}{n}6}$. Then we have

$$\sum_{i=0}^{\frac{p-1}{2n}-1} tr_1^n(\beta^{6^{2i}}) = tr_1^8(\beta^t) = 0.$$

The Legendre sequence $\{s(t)\}$ of period 17 is given by

$$s(t) = 1 + tr_1^8(\beta^{6t}).$$

**Example 4.3** The order 2 mod 127 is 7 and a primitive root mod 127 is 39 such that $2 = (39)^{\frac{p-1}{n}} = (39)^{14} \pmod{127}$. Let $\alpha$ be a primitive element of $GF(2^7)$ satisfying $\alpha^7 + \alpha^4 + 1 = 0$. Then we have

$$\sum_{i=0}^{\frac{p-1}{2n}-1} tr_1^n(\alpha^{u^{2i}}) = \sum_{i=0}^{8} tr_1^7(\alpha^{39^{2i}}) = 0.$$

The Legendre sequence $\{s(t)\}$ of period 127 is given by

$$s(t) = \sum_{i=0}^{8} tr_1^7(\alpha^{39^{2i}t} = \sum_{i=0}^{8} tr_1^7(\alpha^{124^i t}).$$

### 4.3.2 When $p \equiv \pm 3 \pmod 8$

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 $u^{(p-1)/n} = 2$ from Lemma 4.1. 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. That is,

$$\alpha^{2pm} + \alpha^{pm} + 1 = 0.$$

From the above equation, we have

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

For $p \equiv \pm 3 \pmod 8$, we already know that $(p-1)/n$ is odd and $n$ is even. Furthermore if $p \equiv 3 \pmod 8$, $n/2$ must be odd because $p - 1 = 2 \pmod 8$. If $p \equiv -3 \pmod 8$, $n/2$ is even because $p - 1 = 4 \pmod 8$. Therefore, we conclude that

$$\mathrm{tr}\,(\alpha^{pm}) = \begin{cases} 1 & \text{for } p \equiv 3 \pmod 8 \\ 0 & \text{for } p \equiv -3 \pmod 8 \end{cases} \tag{4.5}$$

All of these are summarized in the following:

**Lemma 4.3** Let $p > 3$ be a prime with $p \equiv \pm 3 \pmod 8$, let $n$ be the order of 2 mod $p$, $\alpha$ be a primitive element of $GF(2^n)$, and $2^n - 1 = 3pm$. Then, $\mathrm{tr}\,(\alpha^{pm})$ is given as (4.5).

**Theorem 4.2** 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

$$\sum_{i=0}^{\frac{p-1}{n}-1} \mathrm{tr}\left((\alpha^{pm})^{2^i}\beta^{u^i}\right) = 0, \tag{4.6}$$

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

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

**Proof:** Let $\gamma$ be a primitive element in $GF(2^n)$. Then

$$\sum_{i=0}^{\frac{p-1}{n}-1} \mathrm{tr}\left((\gamma^{pm})^{2^i}\beta^{u^i}\right) + \sum_{i=0}^{\frac{p-1}{n}-1} \mathrm{tr}\left((\gamma^{2pm})^{2^i}\beta^{u^i}\right) = \sum_{i=0}^{\frac{p-1}{n}-1} \mathrm{tr}\left((\gamma^{pm}+\gamma^{2pm})^{2^i}\beta^{u^i}\right) \tag{4.7}$$

$$\begin{aligned} &= \sum_{i=0}^{\frac{p-1}{n}-1} \mathrm{tr}\left(\beta^{u^i}\right) \\ &= \sum_{i=0}^{\frac{p-1}{n}-1} \sum_{j=0}^{n-1} (\beta^{u^i})^{2^j} \\ &= \sum_{i=0}^{\frac{p-1}{n}-1} \sum_{j=0}^{n-1} (\beta^{u^{i+\frac{p-1}{n}j}}) \\ &= \sum_{k=0}^{p-2} \beta^{u^k} \\ &= \sum_{k=1}^{p-1} \beta^k = 1. \end{aligned} \tag{4.8}$$

Therefore, either $\alpha = \gamma$ or $\alpha = \gamma^2$ is the primitive element satisfying (4.6). We would like to note that for such $\alpha$ we have

$$\sum_{i=0}^{\frac{p-1}{n}-1} \mathrm{tr}\left((\alpha^{2pm})^{2^i}\beta^{u^i}\right) = 1. \tag{4.9}$$

Consider the case $p \equiv 3 \pmod 8$. Since $(p-1)/n$ is odd, by Lemma 4.3, we have

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

From (4.6), (4.7), and (4.9), we also have $s(1) = 0$ and

$$\begin{aligned} s(2) &= \sum_{i=0}^{\frac{p-1}{n}-1} \text{tr}\left((\alpha^{pm})^{2^i}(\beta^{u^i})^2\right) \\ &\quad \text{Since } \alpha^{pm} = \alpha^{4pm}, \\ &= \sum_{i=0}^{\frac{p-1}{n}-1} \text{tr}\left((\alpha^{2pm})^{2^i}(\beta^{u^i})\right) \\ &= 1. \end{aligned}$$

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

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

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 (4.1). The other case where $p \equiv -3 \pmod 8$ can be proved similarly. ∎

**Example 4.4** The order of 2 mod 43 is 14 and a primitive root mod 43 is 20 such that $2 = 20^{(p-1)/n} = 20^3 \pmod{43}$. Let $\alpha$ be a primitive element of $GF(2^{14})$ satisfying $\alpha^{14} + \alpha^5 + \alpha^3 + \alpha + 1 = 0$. Then we have

$$\sum_{i=0}^{\frac{p-1}{n}-1} \text{tr}\left((\alpha^{pm})^{2^i}\beta^{u^i}\right) = \sum_{i=0}^{2} tr_1^{14}((\alpha^{5461})^{2^i}\beta^{20^i}) = 0.$$

The Legendre sequence of period 43 is given by

$$s(t) = \sum_{i=0}^{\frac{p-1}{n}-1} \text{tr}\left((\alpha^{pm})^{2^i}\beta^{u^i t}\right) = \sum_{i=0}^{2} tr_1^{14}((\alpha^{5461})^{2^i}\beta^{20^i t})$$

**Example 4.5** The order of 2 mod 13 is 12 and a primitive root mod 13 is 2 such that $2 = 2^{(p-1)/n} = 2$. Let $\alpha$ be a primitive element of $GF(2^{12})$ satisfying $\alpha^{12} + \alpha^6 + \alpha^4 + \alpha + 1 = 0$. Then we have

$$\sum_{i=0}^{\frac{p-1}{n}-1} \text{tr}\left((\alpha^{pm})^{2^i}\beta^{u^i}\right) = tr_1^{12}(\alpha^{1365}\beta) = 0.$$

The Legendre sequence of period 13 is given by

$$s(t) = \sum_{i=0}^{\frac{p-1}{n}-1} \text{tr}\left((\alpha^{pm})^{2^i}\beta^{u^i t}\right) = tr_1^{12}(\alpha^{1365}\beta^t).$$

### 4.3.3 Some Remarks

The linear complexity and the characteristic polynomial of Legendre sequences were already determined in [27] and [28]. 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 |
|---|---|---|
| $p \equiv -1 \pmod 8$ | $Q(x)$ | $(p-1)/2$ |
| $p \equiv 1 \pmod 8$ | $(x+1)N(x)$ | $(p+1)/2$ |
| $p \equiv 3 \pmod 8$ | $(x^p+1)/(x+1)$ | $p-1$ |
| $p \equiv -3 \pmod 8$ | $x^p+1$ | $p$ |

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 (4.2). Assume that 2 is a quadratic residue mod $p$. Then, both $\beta^i$ and $\beta^{2i}$ are quadratic residue or otherwise both of them are quadratic nonresidue. Therefore $Q(x)$ and $N(x)$ are products of minimal polynomials of $\beta^i$'s. Since 2 is a quadratic residue mod $p$ for $p \equiv \pm 1 \pmod 8$, one can assure that the characteristic polynomials $Q(x)$ and $(x+1)N(x)$ are binary polynomials.

## 4.4 Trace function representation of Hall's sextic residue sequences

A Hall's sextic residue sequence exists only if the period $p$ is a prime with $p = 4v^2 + 27$ from some positive integer $v$. Such a prime is $7 \pmod 8$ or $3 \pmod 8$ according that $v$ is even or odd. As already shown in Chapter 3, the linear complexity of Hall's sextic residue sequence of period $p$ is $1 + (p-1)/6$ or $p$, which is determined by whether $p$ is $7 \pmod 8$ or $3 \pmod 8$. Consequently, the trace function representations are also different according to the value $p \pmod 8$. In this section, the case $p \equiv 7 \pmod 8$ is investigated. the case $p \equiv 1 \pmod 8$ remains unsolved.

Let $n$ be the order of 2 mod $p$ and $g$ be a primitive root mod $p$. If $p \equiv 7 \pmod 8$,

then $2 \in C_0$ from P8 in Lemma 3.1. Thus $2 = g^{6i}$ for some $i$. Then

$$2^{(p-1)/6} = (g^{6i})^{(p-1)/6} = g^{(p-1)i} \equiv 1 \pmod{p}.$$

Since $n$ is the order of 2 mod $p$, $n \mid \frac{p-1}{6}$. Let $u$ be a primitive root mod $p$ such that $3 = u^{6i+1} \pmod{p}$ for some $i$, that is, $3 \in C_1$.

**Lemma 4.4** Let $p$ be a prime with $p \equiv 7 \pmod{8}$. Let $n$ be the order of 2 mod $p$ and $H$ be the cyclic subgroup of $C_0$ generated by 2. Then, for any primitive root $u$ mod $p$

$$C_0 = \bigcup_{i=0}^{\frac{p-1}{6n}-1} u^{6i} H$$

where $u^{6i}H$ is a coset of $H$ in $C_0$.

**Proof:** Since $p \equiv 7 \pmod{8}$, $2 \in C_0$. Then $H$ is clearly a subgroup of $C_0$ and there are exactly $\frac{p-1}{6n}$ cosets of $H$ in $C_0$. Thus, it suffices to show that

$$u^{6i}H \neq u^{6j}H \quad \text{for all } i, j, \quad 0 \leq j < i < \frac{p-1}{6n}. \tag{4.10}$$

Assume $u^{6i}H = u^{6j}H$. Then $u^{6(i-j)}H = H$, which implies $u^{6(i-j)} \equiv 2^k \pmod{p}$. Since $2 = u^{\frac{p-1}{n}l}$ for some integer $l$,

$$u^{6(i-j)} \equiv u^{\frac{p-1}{n}lk} \pmod{p}. \tag{4.11}$$

Let's consider the range of the exponents of two sides in the above equation. First, $0 \leq i - j < \frac{p-1}{6n}$ and hence $0 < 6(i-j) < \frac{p-1}{n}$. On the right hand side, we can let $0 < lk < n$ since $u^{\frac{p-1}{n}}$ has order $n$ mod $p$. Thus $\frac{p-1}{n} \leq \frac{p-1}{n}lk < p-1$. Consequently, the two sides in (4.11) cannot be the same mod $p$, which proves (4.10).

**Lemma 4.5** Let $p$ be a prime with $p \equiv 7 \pmod 8$, $n$ be the order of 2 mod $p$ and $u$ be a primitive root mod $p$ such that $3 \in C_1$. Then, for any primitive $p$-th root of unity $\beta \in GF(2^n)$, $\beta$ satisfies

$$\sum_{i=0}^{\frac{p-1}{6n}-1} \text{tr}\left(\beta^{u^{6i}}\right) = C_0(\beta)$$

where $tr(\cdot)$ is a trace function from $GF(2^n)$ to $GF(2)$.

**Proof:**

$$\begin{aligned}\sum_{i=0}^{\frac{p-1}{6n}-1} \text{tr}\left(\beta^{u^{6i}}\right) &= \sum_{i=0}^{\frac{p-1}{6n}-1} \sum_{j=0}^{n-1} (\beta^{u^{6i}})^{2^j} \\ &= \sum_{i=0}^{\frac{p-1}{6}-1} \beta^{u^{6i}} \quad \text{(from Lemma 4.4)} \\ &= C_0(\beta)\end{aligned}$$

■

**Theorem 4.3** Let $\{s(t)\}$ be the Hall's sextic residue sequence of period $p$ with $p \equiv 7 \pmod 8$ and

$$S(x) = s(0) + s(1)x + \cdots + s(p-1)x^{p-1}.$$

Let $n$ be the order of 2 mod $p$, $u$ be a primitive root mod $p$ such that $3 \in C_1$ and $\beta$ be a primitive $p$-th root of unity in $GF(2^n)$ such that $S(\beta^{-1}) = 1$. Then

$$s(t) = 1 + \sum_{i=0}^{\frac{p-1}{6n}-1} \text{tr}\left(\beta^{u^{6i}}\right).$$

**Proof:** Let $s'(t) = 1 + \sum_{i=0}^{\frac{p-1}{6n}-1} \text{tr}\left(\beta^{u^{6i}}\right)$. Then from Lemma 4.5, we have $s'(t) = 1 + C_0(\beta^t)$. In order to prove that $s(t) = s'(t)$, we have to prove

$$s'(t) = \begin{cases} 1 & \text{if } t \in C_0 \cup C_1 \cup C_3 \\ 0 & \text{otherwise} \end{cases}$$

where $t = 0, 1, \ldots, p-1$. Clearly $s'(0) = 1 + C_0(1) = 0$ since $\frac{p-1}{6n}$ is odd. Recall that $C_0(\beta^i) = C_l(\beta)$ where $i \in C_l$. Since $s'(t) = 1 + C_0(\beta^t)$, it suffices to show that

$$C_0(\beta) = C_1(\beta) = C_3(\beta) = 0 \text{ and}$$
$$C_2(\beta) = C_4(\beta) = C_5(\beta) = 1.$$

It can be proved by reconsidering the proof of Theorem 3.1. What have to be noted is that $\beta$ in this theorem is the inverse of that in Theorem 3.1. In the proof of Theorem 3.1, we showed that $C_1(\beta^{-1}) = C_4(\beta) = 1$ and $C_4(\beta^{-1}) = C_1(\beta) = 0$. Since $S((\beta^{-1})^3) = 0 = C_2(\beta^{-1}) + 1$, $C_2(\beta^{-1}) = C_5(\beta) = 1$ and similarly $C_2(\beta) = 1$. The other two values $C_0(\beta)$ and $C_3(\beta)$ can be determined as 0 by the fact that $S((\beta^{-1})^{3^2}) = S((\beta^{-1})^{3^5}) = 0$. ■

**Example 4.6** 3 is a primitive root mod 127 such that $3 \in C_1$ and the order of 2 mod 127 is 7. Let $\beta$ be a primitive element in $GF(2^n)$ satisfying $\beta^7 + \beta^6 + 1 = 0$. Then it is easy to check that

$$S(\beta^{-1}) = C_0(\beta^{-1}) + C_1(\beta^{-1}) + C_3(\beta^{-1}) = 1.$$

Then by Theorem 4.3, the Hall's sextic residue sequence of period 127 is given by

$$\begin{aligned} s(t) &= 1 + \text{tr}\left(\beta^t\right) + \text{tr}\left(\beta^{3^6 t}\right) + \text{tr}\left(\beta^{3^{12} t}\right) \\ &= 1 + \text{tr}\left(\beta^t\right) + \text{tr}\left(\beta^{94t}\right) + \text{tr}\left(\beta^{73t}\right). \end{aligned}$$

# Chapter 5

# Conclusion

## 5.1 Summary

In this thesis, Hadamard sequences and their properties (the linear complexity and the trace representation) are investigated. All known Hadamard sequences have periods of the following three types: (1)$N = 4k - 1$ is a prime number (2)$N = p(p + 2)$ is a product of twim primes (3)$N = 2^m - 1$, for $m = 2, 3, 4, \ldots$. It is conjectured that if a Hadamard sequence exists, the period $N$ of the Hadamard sequence must belong to one of the three types above. In [6, 7], the conjecture is confirmed up to $N < 10000$, except for the the following 17 cases: 1295, 1599, 1935, 3135, 3439, 4355, 4623, 5775, 7395, 7743, 8227, 8463, 8591, 8835, 9135, 9215, 9423. In chapter 2, we confirmed that there are no Hadamard sequences of periods $1295, 1599, 1935, 3135$.

In chapter 3, linear complexity of Hadamard sequences is investigated. we determined the linear complexity of Hall's sextic residue sequences and Jacobi sequences including twin prime sequences. As a result, the linear complexities of all Hadamard sequences which can be made by known construction methods were determined. A Hall's

sextic residue sequence of period $p$ has the following linear comlexity.

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

The linear complexity of Jacobi sequences of period $pq$ can be classified as 10 cases according to $p \pmod 8$ and $q \pmod 8$, which are given in Table 3.2. Twin prime sequences of period $p(p+2)$ are given by

$$L = \begin{cases} \frac{p^2+4p-1}{2} & \text{if } p = 7 \pmod 8 \\ \frac{p^2-1}{2} & \text{if } p = 3 \pmod 8 \\ p(p+2) - 1 & \text{if } p = 1 \pmod 8 \text{ or } p = 5 \pmod 8 \end{cases}$$

which is the special case of Jacobi sequences.

In chapter 4, trace representation of Hadamard sequences was investigated. First, we gaved a general trace representation of Legendre sequences of all periods. There is close relation between the trace representation and linear complexity of a binary sequence. If the linear complexities of two binary sequences differ, the trace representations of those sequences differ too and vice versa. We determined the linear complexity of Hall's sextic residue sequences in chapter 3. As the linear complexity has different form with repect to the value of $p \pmod 8$, there may be two forms in the trace representation of Hall's sextic residue sequences. we gave one of them, the case of $p = 7 \pmod 8$.

## 5.2 Future Directions and Open Problems

Throughout this paper, we investigated the existence and the properties of Hadamard sequences. In the future research, we will study the following unsolved problems.

1. As already mentioned, all known Hadamard sequences have periods of the three

types. Then, is it true that a Hadamard sequence exists only if the period of the sequence belong to one of the three types?

2. The conjecture have been confirmed up to 10000 except the 13 cases. Is it also true for the remaining 13 cases? For the smallest case 3439, how can we find a multiplier?

3. One of the most popular Hadamard sequences is $m$-sequences. $m$-sequences have periods of $2^m-1$ where $m = 2, 3, 4, \ldots$. Hadamard sequences of period $2^m-1$ are frequently used in many applications. So far, All Hadamard sequences of period $2^m - 1$ are found by exhausitve search up to $m = 10$. The next case $2^{11} - 1$ should be done.

4. In chapter 4, we determined the trace representation of Legendre sequences and Hall's sextic residue sequences. But, we could not find the trace reprentation of Hall's sextic residue sequences of period $p \equiv 3 \pmod 8$. Furthermore, we are also interested in the trace representation of twin prime sequences.

5. There seems to be no clear similarities in the three forms of periods of Hadamard sequences. Can we explain why they exist only for the three types of periods? Or can we find a common expression for all Hadamard sequences?

# Bibliography

[1] Dilip V. Sarwarte and Michael B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, no. 5, pp. 593–619, May 1980.

[2] R. Gold, "Optimal binary sequences for spread spectrum multiplexing," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 619–621, 1967.

[3] R. Gold, "Maximal recursive sequences with 3-valued recursive crosscorrelation functions," *IEEE Trans. Infrom. Theory*, vol. IT-14, pp. 154–156, 1968.

[4] T. Kasami, "Weight distribution formula for some class of cyclic codes," Tech. Rep. R-108,(AD 632574), Cordinated Science Lab., Univ. Illinois, Urbana, 1966.

[5] T. Kasami, "Weight distribution of bose-chaudhuri-hocquenghem codes," Tech. Rep. R-317, Cordinated Science Lab., Univ. Illinois, Urbana, 1966.

[6] L. D. Baumert, *Cylic Difference Sets*, Springer-Verlag, New York, 1971.

[7] H.-Y. Song and S. W. Golomb, "On the existence of cyclic hadamard difference sets," *IEEE Trans. Inform. Theory*, vol. 40, no. 4, pp. 1266–1268, July 1994.

[8] S. W. Golomb and H.-Y. Song, "A conjecture on the existence of cyclic hadamard difference sets," *Journal of statistical planning and inference*, vol. 62, pp. 39–41, 1997.

[9] S. W. Golomb, *Shift register sequences*, Holden-Day, San Francisco, CA (Revised Edition, Aegean Park Press, Laguna Hills, CA, 1982), 1967.

[10] R. Lidl and H. Neiderreiter, *Finite fields*, vol. 20 of *Encyclopedia of Mathematics and Its Applications*, Addison-Wesley, Reading, MA, 1983.

[11] Jong-Seon No, Hwan-Keun Lee, Habong Chung, Hong-Yeop Song, and Kyeongcheol Yang, "Trace representation of legendre sequences of mersenne prime period.," *IEEE Transactions on Information Theory*, vol. 42, no. 6, pp. 2254–2255, Nov. 1996.

[12] B. Gordon, W. H. Mills, and L. R. Welch, "Some new difference sets," *Canadian J. Math.*, vol. 14, pp. 614–625, 1962.

[13] L. D. Baumert and H. Fredricksen, "The cyclotomic numbers of order eighteen with applications to difference sets," *Math. Computation*, vol. 21, no. 98, pp. 204–219, 1967.

[14] H.-K. Lee, J.-S. No, H. Chung, K. Yang, J.-H. Kim, and H.-Y. Song, "Trace function representation of Hall's sextic residue sequences and some new sequences with ideal autocorrelation," in *Proceedings of APCC'97*. APCC, Dec. 1997, pp. 536–540.

[15] J.-S. No, H. Chung, K. Yang, and H.-Y. Song, "On the construction of binary sequences with ideal autocorrelation property," in *Proceedings of IEEE International Symposium on Information Theory and Its Application*, 1996, pp. 837–840.

[16] J.-S. No, H.-K. Lee, H. Chung, K. Yang, and H.-Y. Song, "On the classification of binary sequences of period $2^n - 1$ with ideal autocorrelation," in *Proceedings of ISIT*, 1997, p. 42.

[17] J.-S. No, S. W. Golomb, Guang Gong, H.-K. Lee, and Peter Gaal, "Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation," *IEEE Transactions on Information Theory*, vol. 44, no. 2, pp. 814–817, Mar. 1998.

[18] U. Cheng, "Exhaustive construction of $(255, 127, 63)$-cyclic difference sets," *J. Combinatorial Theory*, vol. 35, no. 2, pp. 115–125, September 1983.

[19] R. Dreier, "(511,255,127) cyclic difference sets," in *IDA Talk*, 1992.

[20] J.-H. Kim, "On the binary sequences of period 511 with ideal autocorrelation," M.S. thesis, Yonsei University, Korea, 1998.

[21] Peter Gaal and S. W. Golomb, "Exhaustive determination of (1023,511,255)-cyclic difference sets," preprint, 1997.

[22] J.-H. Kim and H.-Y. Song, "Existence of cyclic hadamard difference sets and its relation to binary sequences with ideal autocorrelation," Padova, Italy, July 1998, Mathematical Theory of Networks and Systems, invited for presentation.

[23] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*, Computer Science Press, Rockville, 1985.

[24] M. Hall Jr., "A survey of difference sets," *Proc. Amer. Math. Soc*., vol. 7, pp. 975–986, 1956.

[25] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 2 edition, 1990.

[26] Cunsheng Ding, "Linear complexity of generalized cyclotomic binary sequences of order 2," *Finite Fields and Their Applications*, vol. 3, pp. 159–174, 1997.

[27] Cunsheng Ding, Tor Helleseth, and Weijuan Shan, "On the linear complexity of legendre sequences," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 1276–1278, May 1998.

[28] R. Turyn, "The linear generation of the legendre sequences," *Journal of Soc. Ind. Appl. Math.*, vol. 12, no. 1, pp. 115–117, March 1964.

[29] M. Hall Jr. and J. H. van Lint, *Combinatorial Theory*, Ginn (Blaisdell), Boston, 1967.

[30] B. Gordon, W. H. Mills, and L. R. Welch, "Some new difference sets," *Canadian J. Math.*, vol. 14, pp. 614–625, 1962.

[31] Y. Niho, *Multi-valued cross-correlation functions between two maximal linear recursive sequences*, Ph.D. thesis, Dept. Elec. Eng., Univ. Southern California, 1972.

[32] R. G. Stanton and D. A. Sprott, "A family of difference sets," *Canadian J. Math.*, vol. 10, pp. 73–77, 1958.

[33] J.-S. No, H.-K. Lee, H. Chung, K. Yang, and H.-Y. Song, "On the classification of binary sequences of period $2^n - 1$ with ideal autocorrelation," in *Proceedings of ISIT*, 1997, p. 42.

[34] Jeong-Heon Kim and Hong-Yeop Song, "On the linear complexity of Hall's sextic residue sequences," preprint, April 2000.

[35] Jeong-Heon Kim and Hong-Yeop Song, "Trace representation of legendre sequences," *Designs,Codes and Cryptography*, vol. 24, no. 3, pp. 343–348, July 2001.

[36] Jeong-Heon Kim and Hong-Yeop Song, "On the linear complexity of hall's sextic residue sequences," *IEEE Transaction on Information Theory*, vol. 47, no. 5, pp. 2094–2096, June 2001.

[37] Jeong-Heon Kim and Hong-Yeop Song, "Existence of cyclic hadamard difference sets and its relation to binary sequences with ideal autocorrelation," *Journal of Communications and Networks*, vol. 1, no. 1, pp. 14–18, March 1999.

# 국 문 요 약

## 하다마드 수열에 관한 연구

상관 특성이 좋은 수열을 찾는 문제는 종종 레이다 시스템이나 주파수 확산 통신 시스템에서 그 성능을 향상시키기 위한 중요한 문제로 대두된다. 수열의 상관 특성은 크게 자기 상관 특성과 상호 상관 특성으로 나뉘는데, 각 응용들의 성격에 따라 이 두가지 특성이 모두 요구되기도 하고 한가지만을 요구하기도 한다. 이중에서 특히 최적 자기 상관 특성을 갖는 이진 수열을 하다마드 수열이라고 부르며, 본 논문에서는 이러한 하다마드 수열의 존재성 및 선형 복잡도, 트레이스 함수 표현등의 성질에 대해서 논의한다. 현재까지 알려진 모든 하다마드 수열들은 그 주기가 다음의 세가지 형태 중의 하나이다: (1) $N = 2^m - 1$의 형태로서 소수이다. (2) $N = p(p+2)$의 형태로서 두 연속된 소수의 곱이다. (3) $N = 2^m - 1$, for $m = 2, 3, 4, ldots$. 현재까지 알려진 모든 하다마드 수열이 위의 세가지 중 하나의 형태의 주기를 갖기 때문에 모든 하다마드 수열은 반드시 위의 세가지 중 한가지 형태의 주기를 갖는다는 가설이 세워졌다. 그리고 이러한 가설은 현재 $N < 10000$까지 다음 17가지 경우를 제외하고 참이라는 사실이 알려져있다: 1295, 1599, 1935, 3135, 3439, 4355, 4623, 5775, 7395, 7743, 8227, 8463, 8591, 8835, 9135, 9215, 9423. 본 논문에서는 이중에서 1295, 1599, 1935, 3135에 대해서도 가설이 참임을 전영역 탐색을 통해서 증명하였다.

랜덤 수열의 선형 복잡도는 수열의 생성 및 암호학에서의 안전도 측면에서 매우 중요시되어왔다. 본 논문에서는 하다마드 수열중 Hall의 sextic residue 수열과 twin prime 수열의 일반화된 형태인 Jacobi 수열의 선형복잡도와 특성다항식을 결정하였다. 결과적으로 그 생성 방법이 알려진 모든 하다마드 수열의 선형

복잡도가 이로써 결정된 셈이다. 주기 $p$를 갖는 Hall의 sextic residue 수열의 선형 복잡도는 다음과 같이 주어진다.

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

만약 $p \equiv 3 \pmod 8$이면, Hall 수열은 가질 수 있는 가장 큰 선형 복잡도를 갖게 됨을 수식으로부터 확인할 수 있다. Jacobi 수열의 선형복잡도는 표3.2 에 정리되어있다. Jacobi 수열의 특별한 경우라고 할 수 있는 twin prime 수열의 선형복잡도는 다음과 같이 주어진다.

$$L = \begin{cases} \frac{p^2+4p-1}{2} & \text{if } p = 7 \pmod 8 \\ \frac{p^2-1}{2} & \text{if } p = 3 \pmod 8 \\ p(p+2)-1 & \text{if } p = 1 \pmod 8 \text{ or } p = 5 \pmod 8 \end{cases}$$

위에 제시한 하다마드 수열이 가질 수 있는 세가지 형태의 주기는 그 사이에 연관성이 쉽게 눈에 띄지 않는다. 이들 세가지 형태의 주기를 갖는 하다마드 수열들의 공통점을 찾는 하나의 노력으로서 수열들을 트레이스 함수 형태로 표현하려는 몇몇 연구가 있었다. 본 논문에서는 그 연장선 상에서 Legendre 수열의 일반적인 트레이스 함수 표현을 찾아내었다. 그리고 Hall 수열에 대해서는 Hall 수열이 가질 수 있는 두가지 형태의 주기, 즉 $p = 3 \pmod 8$ 과 $p = 7 \pmod 8$ 중에서 $p = 7 \pmod 8$인 Hall 수열의 트레이스 함수 표현을 결정하였다.

---

핵심되는 말: 최적 자기상관 특성, 하다마드 수열, 선형 복잡도, 트레이스 함수 표현