This is to certify that the
dissertation entitled

CONSTRUCTION OF EVEN LENGTH BINARY SEQUENCES
WITH ASYMPTOTIC MERIT FACTOR 6.0

presented by

Tingyao Xiong

has been accepted towards fulfillment
of the requirements for the

Ph.D. degree in Mathematics

Major Professor's Signature

August 6, 2010

Date

MSU is an Affirmative Action/Equal Opportunity Employer

CONSTRUCTION OF EVEN LENGTH BINARY SEQUENCES WITH ASYMPTOTIC MERIT FACTOR 6.0

By

Tingyao Xiong

A DISSERTATION

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

Mathematics

2010

ABSTRACT

CONSTRUCTION OF EVEN LENGTH BINARY SEQUENCES WITH ASYMPTOTIC MERIT FACTOR 6.0

By

Tingyao Xiong

The known families of binary sequences having asymptotic merit factor ≥ 6 are all modifications to real primitive character sequences. In this thesis, we show a general technique of constructing an even length binary sequence based on a symmetric or antisymmetric sequence. With this technique, we will give new modifications to the character sequences of length $N = p$, $N = pq$, and $N = p_1 p_2 \dots p_r$ respectively. This in turn gives the construction of binary sequences of length $2p$, $2pq$, and $2p_1 p_2 \dots p_r$ with asymptotic merit factor 6.0.

DEDICATION

This dissertation is dedicated to my dearly beloved husband Xuejian Liu and dearest son Cephas Liu. I give my deepest expressions of love and appreciation to them for the encouragement they gave and the sacrifices they made during this graduate program.

Special gratitude goes to my loving parents Guowei Xiong and Qingfu Wang, whose words of encouragement and push for tenacity ring in my ears. My sister Tingqi Xiong has always stood by me and is very special.

I also dedicate this dissertation to my parents-in-law Chengxun Liu and Quanqin Liu, who have supported me throughout the entire process.

ACKNOWLEDGMENT

I would like to express my deepest and sincerest gratitude to my advisor, Dr. Jonathan I. Hall, for his exceptional support and constant encouragement. Without his help, this thesis would not have been possible. I am very thankful to him for his understanding, unconditional trust, and unwavering faith in me, which have helped me persevere through the most challenging times of my doctoral program. It has been an enormously enjoyable experience to work under his supervision.

My gratitude goes to my defense committee members, Dr. Meierfrankenfeld Ulrich, Dr. Michael Shapiro, Dr. George Pappas and Dr. Rajesh Kulkarni, for their expertise and precious time. I am thankful to Dr. Meierfrankenfeld Ulrich for his countless hours of answering my dispersive questions. I would like to thank to Dr. Michael Shapiro for his generous help, including that of translating a Russian paper into English for me. Thank you to Dr. George Pappas for all the enlightening conversations. Special thanks to Dr. Rajesh Kulkarni for consenting to serve on my committee despite the late notification.

I acknowledge and thank Dr. Jonathan Jedwab for his generous help, even though we have never met each other.

Finally I would like to thank Dr. Zhengfang Zhou and Mrs. Barbara Miller. Their encouragement and support will forever be appreciated.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

Introduction

The problem of finding long binary sequences with the best value of the merit factor has resisted decades of attack by mathematicians and communications engineers. The best theoretical proven value for the asymptotic merit factor, 6.0, has remained unchanged since 1988. All the previously known binary sequence families attaining the highest asymptotic merit factor 6.0 are of odd length. This thesis is mainly focused on constructing new families of binary sequences of even length with asymptotic merit factor 6.0.

In Chapter 1, we introduce the historical background of the Merit Factor Problem, in both theoretical and applicable aspects. We will give a brief review of the known results about the asymptotic merit factor, both theoretical and numerical, in Chapter 2. In Chapter 3, we will collect the definitions and properties which will be referred to in the following chapters. In Chapter 4, we show a common technique of constructing an even length sequence based on a symmetric or antisymmetric sequence. With the technique introduced in Chapter 4, we will construct binary sequences of length $N = 2p$, $N = 2pq$, and $N = 2p_1p_2 \dots p_r$ with asymptotic merit factor 6.0 in Chapters 5, 6, 7 respectively.

Now we start with the history of *Merit Factor Problem* (M.F.P.), and the appli-

cation of M.F.P. for both theoretical and practical purposes.

1.1 History of Merit Factor Problem

In this thesis, we transfer the well-known binary digits 0 and 1 into the equivalent forms: $1 = (-1)^0$ and $-1 = (-1)^1$. Thus we call sequence $x = (x_0, x_1, \ldots, x_{N-1})$ a binary sequence of length N if all the x_j's are $+1$ or -1, where $j = 0, 1, \ldots, N-1$.

Correlation is a commonly used measure to describe the similarity, or relatedness, between two phenomena. When properly normalized, the correlation measure is a real number between $+1$ and -1. For instance, in statistics, the correlation between two sets of data is called their covariance. Specifically, let $\alpha = (\ \alpha_0, \alpha_1, \ldots, \alpha_n\ )$ and $\gamma = (\ \gamma_0, \gamma_1, \ldots, \gamma_n\ )$ be two n-dimensional vectors of real numbers, which could represent two sets of experimental data. The magnitudes of these vectors are

$$|\alpha| = (\ \sum_{i=1}^{n} \alpha_i^2\ )^{\frac{1}{2}}, \qquad |\gamma| = (\ \sum_{i=1}^{n} \gamma_i^2\ )^{\frac{1}{2}}$$

then the covariance of the two data sets

$$C(\alpha, \gamma) = \frac{(\alpha \cdot \gamma)}{|\alpha|\ |\gamma|} = \frac{\sum_{i=1}^{n} \alpha_i \gamma_i}{\left(\sum_{i=1}^{n} \alpha_i^2\right)^{\frac{1}{2}} \left(\sum_{i=1}^{n} \gamma_i^2\right)^{\frac{1}{2}}}$$

Similarly, suppose $x = (\ x_0, x_1, \ldots, x_n\ )$ and $y = (\ y_0, y_1, \ldots, y_n\ )$ are both binary vectors. Thus

$$|x| = (\ \sum_{i=1}^{n} x_i^2\ )^{\frac{1}{2}} = \sqrt{n} = (\ \sum_{i=1}^{n} y_i^2\ )^{\frac{1}{2}} = |y|$$

then the *binary correlation* between x and y is

$$C(x, y) = \frac{1}{n} \sum_{i=1}^{n} x_i y_i$$

Note that if $x = y$, we call $C(x, x) = 1$ the autocorrelation of sequence x.

To conduct research in simpler forms, mathematicians and engineers have studied the following correlations forms. The application of these definitions will become clear soon.

Let $x = (x_0, x_1, \ldots, x_{N-1})$ and $y = (y_0, y_1, \ldots, y_{N-1})$ be sequences of *length* N (not necessarily binary). The *aperiodic crosscorrelation* function between x and y at shift i is defined to be

$$A_{x,y}(i) = \sum_{j=0}^{N-i-1} x_j y_{j+i}, \quad i = 1, ..., N-1 \tag{1.1}$$

When $x = y$, we call $A_x(i) = A_{x,x}(i)$ the *aperiodic autocorrelation* function of x at shift i, where $A_x(i)$ is defined as following:

$$A_x(i) = \sum_{j=0}^{N-i-1} x_j x_{j+i}, \qquad i = 1, ..., N-1 \tag{1.2}$$

Binary sequences with low aperiodic autocorrelations have been widely applied in communication engineering. To see this statement more clearly, we look at a simplified communication system with only one signal sender and receiver.

In order to communicate information from a sender to a receiver, the sender needs to transmit messages through the so called *communication channel.* It is important to distinguish here between a signal and a message. In this thesis, a signal is a single digit 1 or -1. While a message means a binary sequence with entries 1 or -1.

As shown in Figure 1.1, in the real world, the sender and receiver have to communicate over a noisy communication channel. That is, the signals that are received do not look identical to the signals that are sent. As a result, the receiver must decide which signal was actually sent, given the actual signal that was received.

The basic problem that serves as a model of detection theory concerns the situation

Figure 1.1: A Simple Model of Communication Channel

in which there are two possible transmitted signals, represented by 1 and -1, and these are corrupted by Gaussian noise. For instance, if 1 (or -1) is sent, let r be the corresponding signal received. Then we assume that r has a Gaussian distribution (normal distribution) with mean value 1 (or -1) and standard deviation σ. The larger value of σ, the noisier the channel and the greater the probability that the receiver will make an incorrect decision as to what was sent.

If a message x is represented by a binary sequence $x = (x_0, x_1, \ldots, x_{N-1})$ of length N, we use notation $x^{[i]} = (0, \ldots, 0, x_0, x_1, \ldots, x_{N-1-i})$ to represent the sequence delayed by i time units. Then $A_x(i)$ represents the correlation between message x and the delayed message $x^{[i]}$ (not normalized). In 1953, in a foundational paper [1] of communication engineering, Barker proposed a group synchronization digital system, based on the use of binary sequences x with correlations $\mid A_x(i) \mid$'s collectively small. The purpose of this constraint was to ensure a large difference between $A_x(0)$, the correlation of message x to itself, and $A_x(i)$, the correlation of message x to its delay $x^{[i]}$.

In 1961, Fano [2] proved a considerably general result: Over a channel corrupted by Gaussian noise, the optimum decision process is to perform correlation detection,

that is, to calculate the correlation between the actual received message and ideal models of each of the possibly transmitted messages. And the message having the highest value of the correlation with the actual received message is the message that was actually sent. The optimum detector for a given channel is known as the matched filter for that channel, and the result we have just mentioned is frequently described as follows: the matched filter for the Gaussian channel is a *correlation detector.*

Since 1960's, binary sequences with low aperiodic autocorrelations have been widely applied in radar, sonar, and many other communication systems as well as synchronization.

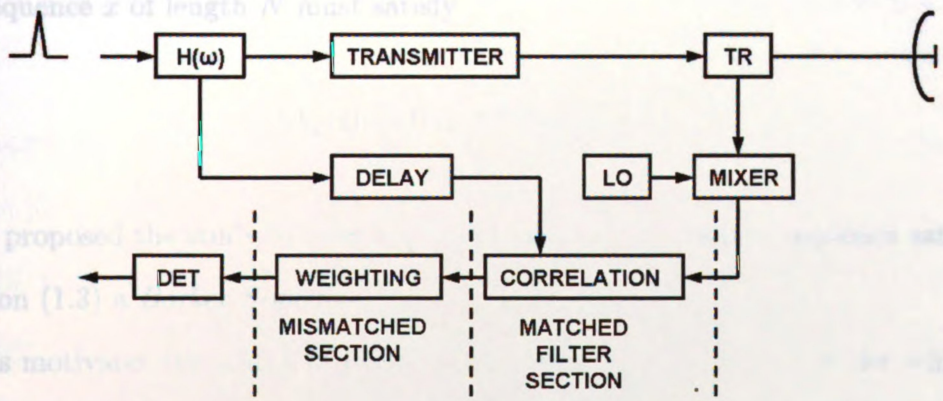

Figure 1.2: Pulse Compression Radar Using Correlation

Figure 1.2 is from Radar Handbook ([3], page 10.2, figure (c)). It gives a concrete example of the application in a radar system. In Figure 1.2, the detection process is called *pulse compression radar using correlation* , which has been widely used in radar technology. In this system, once a message x' is received, the correlation detector ("CORRELATOR" in the figure) not only calculates the correlations between x' and all the possibly transmitted messages x, but also the correlations between x' and all the delays of $x^{[i]}$ by i time units. The message x having the highest correlation values with x' will be detected as the message that was actually sent. Therefore we

want the correlations between x' and all the delays of $x^{[i]}$ ($\sim A_x(i)$) to be small, for $i > 0$, since $x^{[i]}$ is not the correct message. In this model, we can see clearly that using binary sequences with low aperiodic autocorrelations will increase the accuracy of correlation detector significantly. More discussion about the application of binary sequences for which $|A_x(i)|$ is small for each $i \neq 0$, can be found in [4], [5], and [7].

The importance of finding binary sequences x with small $|A_x(i)|$ values led Barker to seek answers for large N to the following question:

Question 1.1.1. *minimise* $\max_{0<i<N} |A_x(i)|$ *over all length* N *binary sequences* x.

Barker therefore observed that, for this synchronization application, an ideal binary sequence x of length N must satisfy

$$|A_x(i)| = 0 \text{ or } 1 \text{ for all } i \neq 0. \tag{1.3}$$

and he proposed the study of such sequences. We call any binary sequence satisfying condition (1.3) a *Barker Sequence.*

This motivates the search of binary sequences x of large length N, for which the elements of the set $\{|A_x(1)|, |A_x(2)|, \ldots, |A_x(s-1)|\}$ are collectively as small as possible. Unfortunately, most mathematicians believe that the following conjecture is true:

Conjecture 1.1.2. *There is no Barker sequence of length* $N > 13$.

Another important definition for binary sequences, which is similar to the definition of aperiodic correlation, is called the periodic correlation. We will use both aperiodic and periodic correlations heavily in this thesis.

The *periodic crosscorrelation* function between x and y at shift i is defined to be

$$P_{x,y}(i) = \sum_{j=0}^{N-1} x_j\, y_{j+i}, \quad 0 \leq i < N \tag{1.4}$$

where all the subscripts are taken modulo N. Similarly, when $x = y$, put

$$P_x(i) = \sum_{j=0}^{N-1} x_j x_{j+i}, \quad 0 \le i < N \,, \tag{1.5}$$

the *periodic autocorrelation* function of x at shift i, where all the subscripts are taken modulo N.

Turyn and Storer proved the following theorem [6] in 1961.

Theorem 1.1.3. *(Turyn and Storer) Conjecture 1.1.2 is true for odd N. Furthermore, for a Barker sequence B of even length $N > 2$, $P_B(i)$ equal 0 for all $0 < i < N$.*

Readers can find more discussion about Barker sequences in many papers, for instance [8].

In 1972, to describe the "good" binary sequences with aperiodic autocorrelations collectively small, Golay ([9]) proposed another important measure called *Merit Factor*. Given a binary sequence x of length N, the *merit factor* of the sequence x, is defined as

$$F_x = \frac{N^2}{2\sum_{i=1}^{N-1} A_x^2(i)} \quad . \tag{1.6}$$

Using the concept Merit Factor, given N fixed, finding a binary sequence x of length N with $|A_x(i)|$'s collectively small is equivalent to finding a binary sequence x of length N with high merit factor value.

Moreover, for the family of sequences

$$S = \{x^1, x^2, \ldots, x^n, \ldots\}$$

where for each $i \ge 1$, x^i is a binary sequence of length N_i, if as i approaches infinity,

N_i also approaches infinity, and the limit of F_{x^i} exists, then we call

$$F = \lim_{i \to \infty} F_{x^i} \tag{1.7}$$

the asymptotic merit factor of the sequence family S.

Golay not only gave a simple measure describing the feature that a binary sequence has aperiodic autocorrelations collectively small but also revealed the close connection between the length of the sequence and the aperiodic autocorrelations in an elegant way. For nearly twenty years, Golay studied the following problem: Let X_n be the set of all binary sequences of length n,

Question 1.1.4. $F_n = \max_{x \in X_n} F_x = ?$

In his series of publications ([9], [10], [11],[12], [13], and [14]), Golay either used probability theory or computer searching to study Question 1.1.4. Indeed, Question 1.1.4 is still open. That is, at each length N, we do not know the maximum merit factor value of all the binary sequences with length N except by conducting exhaustive search for small N. We will discuss these numerical searching results in next chapter.

As discussed before, finding a binary sequence x with $|A_x(i)|$'s collectively small can be considered as finding a binary sequence x with high merit factor F_x. In real communication systems, because of the large amount of information needed to be transmitted, engineers have more interest in merit factor behavior when the length of binary sequence is large. Meanwhile, mathematicians have made important break through in finding the upper bound of the asymptotic merit factor of binary sequences. To express this question in a mathematical form, we have the following:

Question 1.1.5. $\limsup_{n \to \infty} F_n = ?$

where F_n is as defined in Question 1.1.4.

Traditionally, people call Question 1.1.5 the *Merit Factor Problem* (M.F.P.). Compared to Question 1.1.4, mathematicians have made remarkable progress on the M.F.P., which will be discussed in more details in next chapter. This thesis is mainly focused on constructing new families of sequences achieving the known highest value of asymptotic merit factor.

1.2 Merit Factor and Littlewood's Conjecture

Mathematicians (for instance, [18],[23], [15]) have tried to approach the merit factor problem through complex analysis and number theory. An optimal method is to study polynomials with ± 1 coefficients on the unit circle of the complex plane, which have been studied by some famous mathematicians like Littlewood [17]. This section will give some examples about this connection. Although the topic of this section will not play a role in the rest of this thesis, here we observe that merit factor is not only of engineering but also of mathematical interest.

Prior to Golay's definition of merit factor in 1972, Littlewood [16] and other number theorists studied questions concerning the norms of polynomials with ± 1 coefficients on the unit circle of the complex plane. Furthermore, some properties and conjectures from complex analysis can be written in terms of Merit Factors. Before we see some concrete examples, we need some definitions here.

Let $Q_\alpha(z) = \sum_{i=0}^{N-1} \alpha_i z^i$ be the complex-valued polynomial whose coefficients are the elements of the sequence $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{N-1})$ of length N. The L_β norm of the polynomial $Q_\alpha(z)$ on the unit circle of the complex plane is defined to be

$$||Q_\alpha||_\beta = \left(\frac{1}{2\pi} \int_0^{2\pi} |Q_\alpha(e^{i\theta})|^\beta d\theta \right)^{1/\beta} \tag{1.8}$$

If the coefficient sequence $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{N-1})$ is a binary sequence, then we can

write the merit factor of α as ([25], Theorem 1.2, page 35)

$$F_\alpha = \frac{||Q_\alpha||_2^4}{||Q_\alpha||_4^4 - ||Q_\alpha||_2^4} \tag{1.9}$$

where F_α is the merit factor of sequence α as defined in (1.6).

The following is one of many Littlewood's Conjectures ([17], §6, page370):

Conjecture 1.2.1. ***(Littlewood)*** *Let Q_N be the set of all the complex-valued polynomials whose coefficients are the elements of some binary sequence of length N. Then there exists a polynomial $f_N \in Q_N$, so that $||f_N||_4^4 = N^4 + o(N^4)$.*

If we write Conjecture 1.2.1 in terms of merit factor, we will have

Conjecture 1.2.2. ***(Littlewood)*** $\limsup_{n\to\infty} F_n = \infty$.

By studying the L_4 norms of polynomials with coefficients ± 1, Newman and Byrnes [18] obtained an important result on the asymptotic behaviour of the merit factor in 1990:

Property 1.2.3. *The mean value of $1/F$, taken over all sequences of length n, is $\frac{n-1}{n}$.*

□

We see that the merit factor as defined in (1.6) is of considerable practical and theoretical interest to both engineers and mathematicians. Starting in the next chapter, we will be mainly focused on the *Merit Factor Problem* as introduced in Question 1.1.5.

Chapter 2

Known Results

In this chapter, we will review all the known research results, both theoretical and numerical, about the *Merit Factor Problems* as mentioned in Question 1.1.5. From now on, we always use (i, N) to represent the greatest common divisor of integers i and N.

2.1 Theoretical Results

For p an odd prime, a *Legendre Sequence* of length p is defined by the *Legendre symbols*

$$\alpha_j = \left(\frac{j}{p}\right), \ j = 0, \ldots, p-1,$$

where

$$\left(\frac{j}{p}\right) = \begin{cases} 1, & \text{if } j \text{ is a square modulo } p; \\ -1, & \text{otherwise.} \end{cases} \tag{2.1}$$

More generally, for $N = p_1 \ldots p_r$, where $p_1 < p_2 < \cdots < p_r$ and each p_j is an odd prime, a *Jacobi Sequence* β of length N is defined by

$$\beta_j = \left(\frac{j}{p_1}\right)\left(\frac{j}{p_2}\right)\cdots\left(\frac{j}{p_r}\right) \tag{2.2}$$

Given a sequence $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{N-1})$ of length N. We call

$$\alpha^f = (\alpha_{\lfloor fN \rfloor}, \alpha_{\lfloor fN \rfloor + 1}, \cdots, \alpha_{N-1}, \alpha_0, \alpha_1, \ldots, \alpha_{\lfloor fN \rfloor - 1})$$

α of length N offset by the factor f.

In 1988, Høholdt and Jensen [23] made an important breakthrough by proving the following theorem:

Theorem 2.1.1. *The asymptotic merit factor F of Legendre sequences of length p offset by the factor f is*

$$1/F = 1/6 + 8(f - 1/4)^2, \qquad |f| \leq 1/2, \tag{2.3}$$

□

By Theorem 2.1.1, offset Legendre sequences have an asymptotic merit factor 6.0 at the fraction $|f| = \frac{1}{4}$. This Theorem is very important because even today, 6.0 is still the best theoretically proven value for asymptotic merit factors.

In 1991, J.M. Jensen, and H.E. Jensen and Høholdt [24] defined a new family of binary sequences called *Modified Jaclobi sequences* at length $N = pq$, with $p < q$ odd primes:

$$m_j = \begin{cases} +1, & \text{if } j = 0, q, 2q, \ldots, (p-1)q \\ -1, & \text{if } j = p, 2p, \ldots, (q-1)p \\ \left(\frac{j}{p}\right) \cdot \left(\frac{j}{q}\right), & \text{otherwise .} \end{cases} \tag{2.4}$$

In the same paper [24], J.M. Jensen, and H.E. Jensen and Høholdt proved that the formula (2.3) is also correct for Jacobi Sequences and Modified Jaclobi sequences of length pq provided p and q satisfy

$$\frac{(p+q)^5 \log^4 N}{N^3} \to 0, \quad \textit{for } N \to \infty . \tag{2.5}$$

On the other hand, given an odd prime p, the real primitive character modulo p takes the form

$$\chi_p(j) = \begin{cases} \left(\frac{j}{p}\right) & , \text{ if } (j,p) = 1\,; \\ 0 & , \text{ otherwise} \end{cases} \tag{2.6}$$

where $\left(\frac{j}{p}\right)$ is the Legendre symbol as defined in (2.1).

More generally, for an odd number N, where N is a product of distinct odd primes $p_1 p_2 \cdots p_r$ with $p_1 < p_2 < \cdots < p_r$, the real primitive character modulo N takes the form

$$\chi_N(j) = \chi_{P_1}(j)\chi_{P_2}(j)\cdots\chi_{P_r}(j) \tag{2.7}$$

The Legendre sequences, Jacobi and Modified Jacobi sequences just redefine the value at the i-th position where $(i, N) > 1$. In this sense, all of the Legendre sequences, Jacobi and Modified Jacobi sequences are modifications of character sequences. Table 2.1 shows the close connection between the two categories.

x_k	$(k,N) = 1$	$k \equiv 0 (\text{mod } p)$	$k \equiv 0 (\text{mod } q)$
Legendre sequence	$\chi_N(k)$	$+1$	$-$
Jacobi sequence at length $N = pq$	$\chi_N(k)$	$\chi_q(k/p)$	$\chi_p(k/q)$
Modified Jacobi sequence	$\chi_N(k)$	$+1$	-1

Table 2.1: Primitive characters and sequences of Legendre families

We can see clearly all the known families of sequences with high asymptotic merit factor are highly related to the primitive character sequences as defined in (2.7). By performing calculations on the character forms (which are actually triple-valued), Borwein and Choi [25] proved that (2.3) is correct for all the sequences defined as in

(2.7) under an improved restriction on p_i's

$$\frac{N^{\epsilon}}{p_1} \to \infty \text{ for any } \epsilon \text{ small enough} \tag{2.8}$$

We can combine all the theoretical results mentioned above into the following theorem.

Theorem 2.1.2. *(Høholdt , Jensens, Borwein and Choi, 1988, 1991, 2001) Let* α^N *be*

(1) a Legendre Sequence of length $N = p_1$,

(2) a Jacobi or Modified Jacobi Sequence of length $N = p_1 p_2$,

(3) a real primitive character Sequence of length $N = p_1 p_2 \dots p_r$

with $p_1 < p_2 < \cdots < p_r$ *and each* p_j *is an odd prime. Now construct any infinite sequence of such sequences*

$$\alpha = \{\alpha^{N_1}, \alpha^{N_2}, \dots \alpha^{N_i}, \dots\},$$

Then the asymptotic merit factor F *of* α *offset by the factor* f *is*

$$1/F = 2/3 - 4|f| + 8f^2, \qquad |f| \le 1/2$$

provided that

$$N^{\epsilon}/p_1 \to 0, \text{ for any } \epsilon > 0 \text{ small enough as } N \to \infty.$$

□

In Chapter 3, we will explore the properties of character sequences more deeply.

2.2 Numerical Approaches

2.2.1 Skew-symmetric Sequences

A common strategy for extending the reach of merit factor computations is to impose restrictions on the structure of the sequence. One of the most historically popular definition is the *skew-symmetric* binary sequences, defined by Golay [9]:

A binary sequence $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{2m})$ of odd length $2m+1$ is called a *skew-symmetric* binary sequence if

$$\alpha_{m+i} = (-1)^i \alpha_{m-i} \qquad \text{for } i = 1, 2, \ldots, m.$$

Skew-symmetric binary sequences are good possibilities to have large merit factor because of the following property [9]:

Property 2.2.1. *A skew-symmetric binary sequence x of odd length has $A_x(i) = 0$ for all odd i.* □

The computational advantage of only searching skew-symmetric binary sequences with large merit factor is that it roughly doubles the sequence length that can be searched with given computational resources. In [11], Golay showed that skew-symmetric sequences attain the optimal merit factor value F_n (as defined in Question 1.1.1) for the following odd values $n < 60$: 3, 5, 7, 9, 11, 13, 15, 17, 21, 27, 29, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, and 59. The optimal merit factor over all skew-symmetric sequences of odd length n was calculated independently by Golay and Harris [14] for $n \leq 69$ in 1990 and by de Groot, Würtz and Hoffmann [26] for $n \leq 71$ in 1992. And also in 1990, Golay and Harris [14] found good skew-symmetric sequences for odd length n with $71 \leq n \leq 117$ by interleaving one symmetric sequences and another anti-symmetric binary sequence.

Based on heuristic searches for long skew-symmetric sequences, Golay proposed the following conjectures:

Conjecture 2.2.2. *(Golay, [11]) The asymptotic optimal merit factor of the set of skew-symmetric sequences is equal to* $\limsup_{n\to\infty} F_n$.

Conjecture 2.2.3. *(Golay, [12])* $\limsup_{n\to\infty} F_n \leq 12.32$.

2.2.2 Exhaustive Computation

The other results of exhaustive searching for F_n values are listed as following:

(i) for "small n" in 1965 by Lunelli [19]

(ii) for $7 \leq n \leq 19$ by Swinnerton-Dyer, as presented by Littlewood [16] in 1966

(iii) for $n \leq 32$ by Turyn, as presented by Golay [12] in 1982

(iv) for $n \leq 48$ by Mertens [20] in 1996

(v) for $n \leq 60$ by Mertens and Bauke [21] in 2004

2.2.3 Periodic Appending

From Section 2.1 we know that 6.0 is the best theoretical proven value of the asymptotic merit factor. In other words, we can safely claim that

$$6.0 \leq \limsup_{n\to\infty} F_n \leq \infty$$

In [23], Høholdt and Jensen made the following conjecture:

Conjecture 2.2.4. *(Høholdt and Jensen)* $\limsup_{n\to\infty} F_n = 6.0$

On the other hand, some numerical observation ([27]) strongly suggest that

$$\limsup_{n\to\infty} F_n > 6.0\,.$$

Before we introduce that result, we need some definitions. Given sequences $X = \{x_0, x_1, \ldots, x_{N-1}\}$ of length N, $Y = \{y_0, \ldots, y_{M-1}\}$ of length M, a real number $0 \le r < 1$, we define

- Rotation $\quad X^r = \{x_{0+\lfloor rN \rfloor}, x_{1+\lfloor rN \rfloor}, \ldots, x_{N-1+\lfloor rN \rfloor}\}$,
- Truncation $\quad X_r = \{x_0, x_1, \ldots, x_{\lfloor rN \rfloor - 1}\}$,
- Appending $\quad X;Y = \{x_0, \ldots, x_{N-1}, y_0, \ldots, y_{M-1}\}$.

In 2004, Borwein, Choi, and Jedwab [27] used the rotation and appending method as just defined and obtained the following result:

Observation 2.2.5. *(Borwein, Choi, and Jedwab) Suppose X is a Legendre sequence of length $N = p$ with p prime, then*

- *For large N, the merit factor of the appended sequence $X^{\frac{1}{4}}; X_t^{\frac{1}{4}}$ is greater than 6.2 when $t \sim 0.03$.*
- *For large N, the merit factor of the appended sequence $X^r; X_t^r$ is greater than 6.34 for $r \sim 0.22$ and $r \sim 0.72$, when $t \sim 0.03$.*

Furthermore, Borwein, Choi, and Jedwab ([27], Theorem 6.4 and equation (20)) gave an estimate of the asymptotic merit factor of the appended sequence $X^r; X_t^r$:

Theorem 2.2.6. *(Borwein, Choi, and Jedwab) Let X be a Legendre sequence of*

prime length p and let r, t satisfy $0 \le r \le 1$ and $0 < t \le 1$. Then for large p

$$\frac{1}{F_{X^r;X_t^r}} \sim \begin{cases} 2\left(\frac{t}{1+t}\right)^2\left(\frac{1}{F_{X_t^r}}+1\right)+\left(\frac{1-t}{1+t}\right)^2\left(\frac{1}{F_{X_{1-t}^{r+t}}}\right) & , \textit{for } t<1; \\ \frac{1}{2}\left(\frac{1}{F_{X^r}}+1\right) & , \textit{for } t=1. \end{cases}$$

Now we summarize the known results about the asymptotic merit factor of binary sequences.

- 6.0 is the highest proven asymptotic merit factor value.
- All the known "good" sequences with high asymptotic merit factor are *modification of the character sequences* by putting new values at positions i, with $(i, N) > 1$.
- All the known "good" sequences with high asymptotic merit factor are of *odd length*: $p_1 p_2 \dots p_r$, and each p_i is an odd prime.
- All the known "good" sequences with high asymptotic merit factor are *rotations* of modified character sequences.
- It may be possible to obtain sequences with asymptotic merit factor > 6.34 by *rotating, truncating, and appending* a Legendre sequence.

In the summation above, we have put the key phrases in italic forms. In the following chapters, we will construct new families of binary sequences. In contrast with the features listed above, these new families of sequences satisfy the following:

- Obtain high asymptotic merit factor value 6.0.
- Give *new modification of the character sequences* at positions i, with $(i, N) > 1$.
- Are of *even length*: $2p_1 p_2 \dots p_r$, and each p_i is an odd prime.

- Are *free of rotations* of modified character sequences.

We will start with introducing new definitions and properties in next chapter .

Chapter 3

Preliminaries

This chapter provides the definitions, notation and properties that will be used in later chapters. Some well-known results are included in order to make the presentation self-contained.

3.1 Definitions

Given a sequence $x = (x_0, x_1, \ldots, x_{N-1})$ of length N, we have the *Discrete Fourier Transform* (DFT) of the sequence, that is,

$$x\,[\xi_N^j] = \sum_{k=0}^{N-1} x_k (\xi_N^j)^k, \quad j = 0, 1, \ldots, N-1 \tag{3.1}$$

where $\xi_N^j = e^{\frac{2\pi j}{N} i}$.

Definition 3.1.1. *Given two sequences* $x = (x_0, x_1, \ldots, x_{N-1})$ *and* $y = (y_0, y_1, \ldots, y_{N-1})$, *we define the product sequence* $b = x * y$ *by* $b_i = x_i y_i$, *for* $i = 0, 1, ..., N-1$.

Definition 3.1.2. *A binary sequence* $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{N-1})$ *of odd length is* symmetric *if* $\alpha_i = \alpha_{N-i}$, *for* $1 \leq i \leq N-1$, *and* antisymmetric *if* $\alpha_i = -\alpha_{N-i}$, *for*

$1 \le i \le N-1$.

Lemma 3.1.3. *Suppose N is an odd integer. We define a sequence*

$$s = (s_0, s_1, \ldots, s_{N-1})$$

of length N by

$$s_j = \begin{cases} (-1)^{\overline{jN}} & , \text{ if } (j,N) = 1; \\ 0 & , \text{ otherwise .} \end{cases} \tag{3.2}$$

Then the sequence s is antisymmetric.

Proof. For $1 \le j \le N-1$, via Lemma 3.1.7 and 3.1.3, $s_{N-j} = (-1)^{\overline{N-j}} = (-1)^{N-\overline{j}} = -(-1)^{\overline{j}} = -s_j$ since N is odd. Therefore, s is antisymmetric. □

Definition 3.1.4. *Given a binary sequence $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{N-1})$, we write $-\alpha$ for $(-\alpha_0, -\alpha_1, \ldots, -\alpha_{N-1})$.*

Definition 3.1.5. *For $\delta = 0, 1$, let the four sequences $\pm\beta^{(\delta)}$ be given by*

$$\beta_j^{(\delta)} = (-1)^{\binom{j+\delta}{2}} \tag{3.3}$$

For instance,

$$-\beta^{(0)} = -1, -1, +1, +1, \ldots, -1, -1, +1, +1, \ldots$$

and

$$\beta^{(1)} = +1, -1, -1, +1, \ldots, +1, -1, -1, +1, \ldots$$

Definition 3.1.6. *Suppose r is an integer. For any $1 \le i \le r$, if $(i,r) = 1$, then there exists a unique $\overline{ir}$, with $1 \le \overline{ir} \le r$, such that $i \cdot \overline{ir} \equiv 1 \pmod{r}$. Put $\widetilde{ir} = \overline{kr}$, where $k = min\{i, r-i\}$.*

For instance, when $r = 5$, $i = 3$, then $\overline{ir} = \overline{3_5} = 2$, because $3 \times 2 \equiv 1 \pmod 5$. While $\widetilde{ir} = \widetilde{3_5} = \overline{2_5} = 3$, because $2 = \min\{3, 5-3\}$.

As $(r-i)(r-\overline{ir}) \equiv 1 \pmod r$, we have

Lemma 3.1.7. *Suppose r is a positive integer. For any integer i, if $(i,r) = 1$, then $\overline{(r-i)_r} = r - \overline{ir}$.* □

For example, if $r = 5$, $i = 3$, then $\overline{(r-i)_r} = \overline{(5-3)_5} = \overline{2_5} = 5 - \overline{3_5} = 3$.

Definition 3.1.8. *Given two nonnegative numbers A and B, $A \ll B$ means that there exist a positive constant C, independent of A and B, so that $A < CB$.*

Definition 3.1.9. *For an integer n, the divisor function $d(n)$, is defined to be the number of positive divisors of n, or*

$$d(n) = \sum_{0<d|n} 1$$

Definition 3.1.10. *For n a positive integer, write $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, where p_i's are distinct primes. We define $\omega(n) = r$ to be the number of distinct prime divisors of n.*

We will end this section with a notation commonly used in number theory.

Definition 3.1.11. *Let n be a positive integer, and $f(x)$ be a function. Define*

$$\sum_{x=1}^{n}{}' f(x) = \sum_{\substack{x=1 \\ (x,n)=1}}^{n} f(x)$$

For example,

$$\sum_{x=1}^{4}{}' x^2 = 1^2 + 3^2 = 10, \qquad \text{and} \qquad \sum_{x=1}^{N}{}' 1 = \phi(N).$$

where $\phi(N)$ is the *Euler Function* of N.

3.2 Properties

Property 3.2.1. *Let* $x = (x_0, x_1, \ldots, x_{N-1})$ *and* $y = (y_0, y_1, \ldots, y_{N-1})$ *be sequences of equal length* N, *and* $A_{x,y}(i)$ *and* $P_{x,y}(i)$ *are as defined in expressions (1.1) and (1.4). Then*

$$P_{x,y}(i) = A_{x,y}(i) + A_{x,y}(N-i), \qquad \text{for } 0 < i < N.$$

In particular, if $x = y$, *then*

$$P_x(i) = A_x(i) + A_x(N-i) \qquad \text{for } 0 < i < N.$$

Proof. The proof of Property 3.2.1 could be found in many resources, for instance in ([36], (2), page 137). □

Property 3.2.2. *For any integer* i, $(-1)^{(im)} = (-1)^{-i}$, *for any odd* m.

Proof. $(-1)^{i(m+1)} = 1$ since $m+1$ is even. Thus $(-1)^{im} = (-1)^{-i}$. □

Let the character sequence χ_N be as defined in expression (2.7). Then we have the following property

Property 3.2.3. χ_N *is symmetric if* $N \equiv 1 \pmod 4$, *and antisymmetric if* $N \equiv 3 \pmod 4$. *In particular,* $\chi_N(-1) = (-1)^{\frac{N-1}{2}}$ *is* 1 *if* $N \equiv 1 \pmod 4$ *and* -1 *if* $N \equiv 3 \pmod 4$.

Proof. First of all, we assume $N = p$, so $r = 1$. But in $\mathbb{Z}_p^*$, -1 is a square if and only if $p \equiv 1 \pmod 4$, as desired. Now suppose $N = p_1 p_2 \ldots p_r$ with $r \geq 2$. Without loss of generality, suppose $p_1 \equiv p_2 \equiv \cdots \equiv p_k \equiv 3 \pmod 4$, and $p_{k+1} \equiv p_{k+2} \equiv \cdots \equiv$

$p_r \equiv 1 \pmod 4$. Then by the $r = 1$ case,

$$\begin{aligned}\chi_N(N-i) &= \chi_{p_1}(N-i)\cdots\cdot\chi_{p_k}(N-i)\cdot\chi_{p_{k+1}}(N-i)\cdots\cdot\chi_{p_r}(N-i)\\ &= (-1)^k\chi_{p_1}(i)\cdots\cdot\chi_{p_k}(i)\cdot\chi_{p_{k+1}}(i)\cdots\cdot\chi_{p_r}(i)\\ &= (-1)^k\chi_N(i)\,.\end{aligned}$$

Therefore, if k is even, then $N \equiv 1 \pmod 4$, $\chi_N(N-i) = \chi_N(i)$, and χ_N is symmetric; while if k is odd, then $N \equiv 3 \pmod 4$, $\chi_N(N-i) = -\chi_N(i)$, and χ_N is antisymmetric. □

Property 3.2.4. *Suppose N is odd. For the sequence $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{N-1})$ of length N, let the sequence $\beta = (\beta_0, \beta_1, \ldots, \beta_{N-1})$ with $\beta_j = (-1)^j\alpha_j$. If α is symmetric, then β is antisymmetric, while if α is antisymmetric, then β is symmetric.*

Proof. If α is symmetric, then $\alpha_j = \alpha_{N-j}$, for $1 \le j \le N-1$. Therefore, $\beta_j = (-1)^j\alpha_j = (-1)^j\alpha_{N-j} = -(-1)^{N-j}\alpha_{N-j} = -\beta_{N-j}$ since N is odd. So β is antisymmetric. Interchanging the roles of α and β gives the other case. □

Lemma 3.2.5. *Suppose χ_p is as defined in form (2.6). Then*

$$\sum_{n=0}^{p-1}\chi_p(n)\chi_p(n-k) = \begin{cases} p-1 & , \text{if } p|k;\\ -1 & , \text{otherwise}\end{cases}$$

Proof. Readers can find the proof to Lemma 3.2.5 in many references, for instance, Lemma 2 in [42]. □

An immediate application of Lemma 3.2.5 is the following property.

Property 3.2.6. *For an odd prime p, suppose α is a Legendre sequence of length p as defined in expression (2.1).*

(1) $P_\alpha(i) = -1$, *if* $p \equiv 3 \pmod 4$.

(2) $P_\alpha(i) = 1$ *or* -3, *if* $p \equiv 1 \pmod 4$.

Proof. For $0 < j < p$, from Property 3.2.3, $\alpha_j = \begin{cases} \alpha_{p-j}, & \text{if } p \equiv 1 \pmod 4; \\ -\alpha_{p-j}, & \text{if } p \equiv 3 \pmod 4. \end{cases}$

For $0 < i < p$

$$\begin{aligned} P_\alpha(i) &= \sum_{j=0}^{p-1} \alpha_j \alpha_{j+i} \\ &= \alpha_0\alpha_i + \alpha_{p-i}\alpha_0 + \sum_{j=0}^{p-1} \chi_p(j)\chi_p(j+i) \\ &= \alpha_0(\alpha_i + \alpha_{p-i}) - 1 \quad \text{by Lemma 3.2.5} \end{aligned}$$

When $p \equiv 3 \pmod 4$,

$$\alpha_i = -\alpha_{p-i} \quad \Rightarrow \quad P_\alpha(i) = 1 \times 0 - 1 = -1.$$

This finishes the proof of part (a). When $p \equiv 1 \pmod 4$,

$$\alpha_i = \alpha_{p-i} \quad \Rightarrow \quad P_\alpha(i) = 2\alpha_0\alpha_i - 1 = 1 \text{ or } -3.$$

□

Theorem 2.1.1 is based on a famous result for *Gauss Sums*:

Theorem 3.2.7. *(Gauss Sum) For any* $j \in \boldsymbol{Z}$, *let* $\xi_N^j = e^{\frac{2\pi j}{N} i}$. *The* ***Gauss sum*** *is the DFT* $\chi_N[\,\xi_N^j]$ *associated to the primitive character* χ *mod* N *of (2.7):*

$$\chi_N\,[\,\xi_N^j\,] = \sum_{m=0}^{N-1} \chi_N(m)\,\xi_N^{mj}$$

Then

$$\left| \chi_N[\, \xi_N^j \,] \right| = \begin{cases} \sqrt{N}, & \text{if } (j, N) = 1; \\ 0, & \text{otherwise} \end{cases} \tag{3.4}$$

Proof. This is a very well-known result. Readers can find the proof in many resources, for instance, [38] page233.

Lemma 3.2.8. *Let $N = p_1 p_2 \dots p_r$, where $p_1 < p_2 < \cdots < p_r$' are distinct odd primes. Then*

$$d(N) < r \times \frac{N}{p_1}$$

where $d(N)$ is the divisor function of N.

Proof.

$$d(N) < \sum_{i=1}^{r} (N/p_i - 1) < r \times \frac{N}{p_1}$$

□

Property 3.2.9. *Given a sequence $x = (x_0, x_1, \dots, x_{N-1})$ of length N, let $x\,[\,\xi_N^j]$ be defined as in expression (3.1) for $0 \le j \le N-1$. An interpolation formula is*

$$x\,[-\xi_N^j] = \frac{2}{N} \sum_{k=0}^{N-1} \frac{\xi_N^k}{\xi_N^k + \xi_N^j}\, x\,[\,\xi_N^k]$$

Proof. This is a well-known result from numerical analysis. Readers can find the proof in many references, for instance, [23], ((2.5), page162) and [24], (5.6), (page 624). □

For the rest of this section, to simplify the notation, without confusion, we use ξ_j instead of ξ_N^j, to represent $e^{\frac{2\pi j}{N} i}$.

Given a binary sequence $x = (x_0, x_1, \dots, x_{N-1})$ of length N, the following property gives the relation between the merit factor F_x and the DFT of the sequence x.

Property 3.2.10. *Given a binary sequence* $x = (x_0, x_1, \ldots, x_{N-1})$ *of length* N*, for* $\xi_j = e^{\frac{2\pi j}{N} i}$*, let* $x\,[\,\xi_j]$ *be as defined in expressions (3.1), and* $x\,[-\xi_j]$ *as defined as in Property 3.2.9. Then the merit factor* F_x *satisfies*

$$\frac{1}{F_x} = \frac{\sum_{j=0}^{N-1} \left[\left| x\,[\,\xi_j] \right|^4 + \left| x\,[-\xi_j] \right|^4 \right]}{2N^3} - 1$$

Proof. Again, the proof of this Property 3.2.10 could be found in many papers, for instance [23], ((2.2) and (2.3), page 161), and [24], (expression (1.9), page 618). □

If a sequence u could be written as a sum of two sequences U and v, then following property shows the difference of $1/F_u - 1/F_U$.

Property 3.2.11. *Suppose sequences* u*,* U*, and* v *are all of length* N*. And* $u = U + v$*, that is* $u_j = U_j + v_j$*, for* $j = 0, 1, \ldots, N-1$*. Let* $\xi_j = e^{\frac{2\pi j}{N} i}$*, write*

$$u[\,\xi_j] = U[\,\xi_j] + v[\,\xi_j] = U[\,\xi_j] + a_j, \quad \text{where } a_j = v[\,\xi_j].$$

$$u[-\xi_j] = U[-\xi_j] + v[-\xi_j] = U[-\xi_j] + b_j, \quad \text{where } b_j = v[-\xi_j].$$

Let

$$\frac{1}{F_u} - \frac{1}{F_U} = \frac{G}{2N^3}$$

Then

$$\begin{aligned} |G| \le & \sum_{j=0}^{N-1} \left[|a_j|^4 + 6 \left| U[\,\xi_j] \right|^2 |a_j|^2 + 4(\left| U[\,\xi_j] \right|^2 + |a_j|^2)|a_j| \left| U[\,\xi_j] \right| \right] \\ & + \sum_{j=0}^{N-1} \left[|b_j|^4 + 6 \left| U[-\xi_j] \right|^2 |b_j|^2 + 4(\left| U[-\xi_j] \right|^2 + |b_j|^2)|b_j| \left| U[-\xi_j] \right| \right] \end{aligned}$$

Proof. From Property 3.2.10,

$$\frac{1}{F_u} = \frac{\sum_{j=0}^{N-1} \left(\left| u\left[\xi_j\right] \right|^4 + \left| u\left[-\xi_j\right] \right|^4 \right)}{2N^3} - 1$$

$$= \frac{\sum_{j=0}^{N-1} \left(\left| U\left[\xi_j\right] + a_j \right|^4 + \left| U\left[-\xi_j\right] + b_j \right|^4 \right)}{2N^3} - 1\,;$$

$$\frac{1}{F_U} = \frac{\sum_{j=0}^{N-1} \left(\left| U\left[\xi_j\right] \right|^4 + \left| U\left[-\xi_j\right] \right|^4 \right)}{2N^3} - 1$$

Therefore $\frac{1}{F_u} - \frac{1}{F_U}$

$$= \frac{\sum_{j=0}^{N-1} \left(\left| U\left[\xi_j\right] + a_j \right|^4 - \left| U\left[\xi_j\right] \right|^4 + \left| U\left[-\xi_j\right] + b_j \right|^4 - \left| U\left[-\xi_j\right] \right|^4 \right)}{2N^3}$$

Then

$$G = \sum_{j=0}^{N-1} \left(\left| U\left[\xi_j\right] + a_j \right|^4 - \left| U\left[\xi_j\right] \right|^4 + \left| U\left[-\xi_j\right] + b_j \right|^4 - \left| U\left[-\xi_j\right] \right|^4 \right)$$

$$\leq \sum_{j=0}^{N-1} \left[\left(\left| U\left[\xi_j\right] \right| + |a_j| \right)^4 - \left| U\left[\xi_j\right] \right|^4 + \left(\left| U\left[-\xi_j\right] \right| + |b_j| \right)^4 - \left| U\left[-\xi_j\right] \right|^4 \right]$$

$$\leq \sum_{j=0}^{N-1} \left[|a_j|^4 + 6\left|U[\xi_j]\right|^2 |a_j|^2 + 4(\left|U[\xi_j]\right|^2 + |a_j|^2)|a_j| \left|U[\xi_j]\right| \right]$$

$$+ \sum_{j=0}^{N-1} \left[|b_j|^4 + 6\left|U[-\xi_j]\right|^2 |b_j|^2 + 4(\left|U[-\xi_j]\right|^2 + |b_j|^2)|b_j| \left|U[-\xi_j]\right| \right]$$

□

Given a family of binary sequences $\{A(n)\}$, if at each length n, we only change positions considerably small in number compared to the n value, the following property show that the asymptotic merit factor of the new family of sequences is equal to the asymptotic merit factor of $\{A(n)\}$.

Property 3.2.12. *Let $\{A(n)\}$ and $\{B(n)\}$ be sets of sequences, where each of $A(n)$ and $B(n)$ has length n. Suppose that for each n, all elements of $A(n)$ and $B(n)$ are bounded by a constant independent of n. Suppose further that, as $n \to \infty$, the number of nonzero elements of $B(n)$ is $o(\sqrt{n})$ and that $F_{A(n)} = O(1)$ and $P_{A(n)} = O(n)$. Then, as $n \to \infty$, the element-wise sequence sums $\{A(n) + B(n)\}$ satisfy*

$$\frac{1}{F(A(n) + B(n))} = \frac{1}{F(A(n))}(1 + o(1))$$

Proof. The reader can find the detailed proof at [36] (Proposition 1., page138). □

For a sequence u (not necessarily binary) is the sum of two sequences U and v (both U and v are not necessarily binary), the following property gives a concrete expression of the periodic autocorrelations of a sequence u , in terms of the periodic autocorrelations of U and v.

Property 3.2.13. *For sequences u, U and v, (not necessarily binary) of length N. If $u_j = U_j + v_j$, for $0 \leq j < N - 1$, then we have*

$$\begin{aligned}\sum_{i=1}^{N-1} P_u^2(i) = &\sum_{i=1}^{N-1} P_V^2(i) + \sum_{i=1}^{N-1} P_v^2(i) + 2\sum_{i=1}^{N-1} P_V(i)P_v(i) \\ &+ \sum_{i=1}^{N-1} \left[2P_V(i)P_{V,v}(i) + 2P_V(i)P_{v,V}(i) \right] \\ &+ \sum_{i=1}^{N-1} \left[2P_v(i)P_{V,v}(i) + 2P_v(i)P_{v,V}(i) \right]\end{aligned}$$

$$+ \sum_{i=1}^{N-1} \Big[\, 2P_{V,v}(i)P_{v,V}(i) + P^2_{V,v}(i) + P^2_{v,V}(i) \,\Big]$$

where P_V, P_v, $P_{v,V}$ and $P_{V,v}$ are as defined in expressions (1.5) and (1.4).

Proof.

$$\sum_{i=1}^{N-1} P_u^2(i) = \sum_{i=1}^{N-1} \left[\sum_{j=0}^{N-1} u_j u_{j+i} \right]^2$$

$$= \sum_{i=1}^{N-1} \left[\sum_{j=0}^{N-1} (V_j + v_j)(V_{j+i} + v_{j+i}) \right]^2$$

$$= \sum_{i=1}^{N-1} \left[\sum_{j=0}^{N-1} \Big(V_j V_{j+i} + V_j v_{j+i} + v_j V_{j+i} + v_j v_{j+i} \Big) \right]^2$$

$$= \sum_{i=1}^{N-1} \left[\sum_{j=0}^{N-1} \Big(V_j V_{j+i} + V_j v_{j+i} + v_j V_{j+i} + v_j v_{j+i} \Big) \right]^2$$

$$= \sum_{i=1}^{N-1} \Big[\, P_V(i) + P_{V,v}(i) + P_{v,V}(i) + P_v(i) \,\Big]^2$$

$$= \sum_{i=1}^{N-1} P_V^2(i) + \sum_{i=1}^{N-1} P_v^2(i) + 2 \sum_{i=1}^{N-1} P_V(i) P_v(i)$$

$$+ \sum_{i=1}^{N-1} \Big[\, +2P_V(i)P_{V,v}(i) + 2P_V(i)P_{v,V}(i) \,\Big]$$

$$+ \sum_{i=1}^{N-1} \left[2P_v(i)P_{V,v}(i) + 2P_v(i)P_{v,V}(i) \right]$$

$$+ \sum_{i=1}^{N-1} \left[2P_{V,v}(i)P_{v,V}(i) + P_{V,v}^2(i) + P_{v,V}^2(i) \right]$$

$$= A + B + C + D + E + F$$

In the proof above, we have separated the summands into six groups. For instance, in the summation above,

$$F = \sum_{i=1}^{N-1} \left[2P_{V,v}(i)P_{v,V}(i) + P_{V,v}^2(i) + P_{v,V}^2(i) \right].$$

□

Chapter 4

Construction of Even Length Binary Sequences

In this chapter, we will give a technique of constructing an even length binary sequence based on a symmetric or an antisymmetric sequence. In the following chapters this technique will be used heavily.

We will start with a property about the sequences β as defined in expression (3.3).

Lemma 4.0.14. *Let N be an odd number. If the binary sequence β of length $2N$ is one of the four sequences $\pm\beta^{(\delta)}$ of Definition 3.1.5, then for $0 \leq a, b < 2N$ we have*

$$\beta_a \, \beta_b = (-1)^{\frac{(\, b - a \,)(\, b + a + 2\,\delta - 1\,)}{2}}$$

Proof. When $0 \leq a, b < 2N$, by definition

$$\beta_a \, \beta_b = (-1)^{\binom{a+\delta}{2} + \binom{b+\delta}{2}}$$

$$= (-1)^{\frac{(\, a+\delta \,)(\, a+\delta-1\,) + (\, b+\delta\,)\,(\, b+\delta-1\,)}{2}}$$

$$= (-1)^{\frac{a^2 + 2\,a\,\delta + \delta^2 - a - \delta + b^2 + 2\,b\,\delta + \delta^2 - b - \delta}{2}}$$

$$= (-1)^{\frac{a^2 + 2\,a\,\delta - a + b^2 + 2\,b\,\delta - b}{2}} \qquad \text{since } \delta^2 - \delta = 0 \text{ when } \delta = 0 \text{ or } 1$$

$$= (-1)^{\frac{a^2 + 2\,a\,\delta - a + b^2 + 2\,b\,\delta - b}{2} - a^2 + a - 2\,a\,\delta}$$

since $-\ a^2\ +\ a$ is always even and $-\ 2\,a\,\delta$ is also an even

$$= (-1)^{\frac{b^2 - a^2 + a - b + 2\,b\,\delta - 2\,a\,\delta}{2}}$$

$$= (-1)^{\frac{(\,b - a\,)(\,b + a + 2\,\delta - 1\,)}{2}}.$$

□

Suppose the sequence β is one of the four sequences $\pm\beta^{(\delta)}$ from Definition 3.1.5. The notations ";" and "$*$" are as defined in Observation 2.2.5 and 3.1.1. Then we have the following two lemmas:

Lemma 4.0.15. *Let α be an arbitrary binary sequence of length N, and let β of length $2N$ be one of the four sequences $\pm\beta^{(\delta)}$ from Definition 3.1.5. Consider the new sequence $b = \{\alpha\ ;\ \alpha\} * \beta$. For even i, we have*

$$A_b(i) = \begin{cases} (-1)^{i/2}\,[A_\alpha(i) + P_\alpha(i)], & if\ 0 < i < N; \\ \\ (-1)^{i/2} A_\alpha(i - N), & i \geq N \end{cases}$$

Proof. Note that the sequence b is of length $2N$. When $0 < i < N$,

$$A_b(i) = \sum_{j=0}^{2N-i-1} b_j b_{j+i}$$

$$= \sum_{j=0}^{N-i-1} b_j b_{j+i} + \sum_{j=N-i}^{N-1} b_j b_{j+i} + \sum_{j=N}^{2N-i-1} b_j b_{j+i} \tag{4.1}$$

$$= I_l + I_m + I_r \,.$$

Here I_l only contains the items from the first half of the sequence, I_r only contains the items from the second half, and I_m consists of the products of the terms from the first half and the terms from the second half. As i is even, by Lemma 4.0.14 we have

$$I_l = \sum_{j=0}^{N-i-1} b_j b_{j+i} = \sum_{j=0}^{N-i-1} \beta_j \beta_{j+i} \alpha_j \alpha_{j+i} \tag{4.2}$$

$$= \sum_{j=0}^{N-i-1} (-1)^{\frac{i(i+2j+2\delta-1)}{2}} \alpha_j \alpha_{j+i} \qquad \text{by Lemma 4.0.14}$$

because $i + 2j + 2\delta - 1$ is odd when i is even

$$= (-1)^{i/2} \sum_{j=0}^{N-i-1} \alpha_j \alpha_{j+i} = (-1)^{i/2} A_\alpha(i) \qquad \text{by Property 3.2.2}$$

Similarly, by definition, we have

$$I_r = \sum_{j=N}^{2N-i-1} b_j b_{j+i} = \sum_{j=N}^{2N-i-1} \beta_j \beta_{j+i} \alpha_{j-N} \alpha_{j+i-N} \tag{4.3}$$

$$= \sum_{j=0}^{N-i-1} (-1)^{\frac{i\,(\,2\,j\,+\,i\,+\,2\,\delta\,-\,1\,)}{2}} \alpha_{j-N}\alpha_{j+i-N} \qquad \text{by Lemma 4.0.14}$$

$$= \sum_{j=0}^{N-i-1} (-1)^{i/2}\alpha_j\alpha_{j+i} = (-1)^{i/2}A_\alpha(i) \qquad \text{by Property 3.2.2}$$

$$I_m = \sum_{j=N-i}^{N-1} b_j b_{j+i} = \sum_{j=N-i}^{N-1} \beta_j\beta_{j+i}\alpha_j\alpha_{j+i-N} \tag{4.4}$$

$$= (-1)^{i/2} \sum_{j=0}^{N-1-(N-i)} \alpha_j\alpha_{j+N-i} = (-1)^{i/2}A_\alpha(N-i)\,.$$

Combining (4.2), (4.3), and (4.4), by Property 3.2.1, we have

$$I_l + I_m + I_r = (-1)^{i/2}\,[\,2A_\alpha(i) + A_\alpha(N-i)\,] = (-1)^{i/2}\,[\,A_\alpha(i) + P_\alpha(i)\,]\,.$$

For even $i \geq N$, Lemma 4.0.14 gives

$$A_b(i) = \sum_{j=0}^{2N-i-1} b_j b_{j+i} = \sum_{j=0}^{2N-i-1} \beta_j\beta_{j+i}\alpha_j\alpha_{j+i-N}$$

$$= \sum_{j=0}^{2N-i-1} (-1)^{\frac{i(i+2j+2\delta-1)}{2}} \alpha_j\alpha_{j+i-N}$$

$$= \sum_{j=0}^{N-(i-N)-1} (-1)^{\frac{i}{2}}\alpha_j\alpha_{j+(i-N)} = (-1)^{\frac{i}{2}}A_\alpha(i-N)\,.$$

This finishes the proof of Lemma 4.0.15. □

Lemma 4.0.16. *For an odd integer N, let $\alpha = (\alpha_0, \alpha_1, ...\alpha_{N-1})$ be a symmetric or antisymmetric binary sequence of length N as defined in Definition 3.1.2, and let $b = \{\alpha|\ \alpha\} * \beta$ be the corresponding sequence defined in Lemma 4.0.15. For odd i, we have*

$$A_b(i) = \begin{cases} (-1)^{\delta+\frac{i-1}{2}}\alpha_0\alpha_{N-i}, & if\ 0 < i < N; \\ \\ (-1)^{\delta+\frac{i-1}{2}}\alpha_0\alpha_{i-N}, & if\ i \geq N. \end{cases}$$

Proof. When $0 < i < N$, following (4.1) we write

$$A_b(i) = \sum_{j=0}^{2N-i-1} b_j b_{j+i}$$

$$= \sum_{j=0}^{N-i-1} b_j b_{j+i} + \sum_{j=N-i}^{N-1} b_j b_{j+i} + \sum_{j=N}^{2N-i-1} b_j b_{j+i} \tag{4.5}$$

$$= I_l + I_m + I_r\,.$$

First consider any term $b_j b_{j+i} = \beta_j\beta_{j+i}\alpha_j\alpha_{j+i}$ in I_l. By the definition of b and Lemma 4.0.14

$$b_{j+N}b_{j+i+N} = \beta_{j+N}\beta_{j+i+N}\alpha_j\alpha_{j+i} = (-1)^{\frac{i(2j+2N+i+2\delta-1)}{2}}\alpha_j\alpha_{j+i}$$

because Ni is odd. By Property 3.2.2, we have

$$b_{j+N}b_{j+i+N} = -(-1)^{\frac{i(2j+i+2\delta-1)}{2}}\alpha_j\alpha_{j+i} = -\beta_j\beta_{j+i}\alpha_j\alpha_{j+i} = -b_j b_{j+i}\,.$$

Thus $b_j b_{j+i}$ is canceled by $b_{j+N} b_{j+i+N}$ from I_r. That is, $I_l + I_r = 0$. For any

item $b_j b_{j+i} = \beta_j \beta_{j+i} \alpha_j \alpha_{j+i-N}$ in I_m with $i + j \neq N$, we have $0 < j < N$ and

$i + j > N$. From Lemma 4.0.14

$$b_{2N-j} b_{2N-j-i} = \beta_{2N-j} \beta_{2N-j-i} \alpha_{N-j} \alpha_{2N-j-i}$$

$$= (-1)^{\frac{i(2j+i-2\delta+1)}{2}} \alpha_j \alpha_{j+i-N}$$

$$= -(-1)^{\frac{i(2j+i+2\delta-1)}{2}} \alpha_j \alpha_{j+i-N}$$

$$= -\beta_j \beta_{j+i} \alpha_j \alpha_{j+i-N} = -b_j b_{j+i}\,.$$

The second equality follows from the property that α is symmetric or antisymmetric. Therefore when $i + j \neq N$, the item $b_j b_{j+i}$ is canceled by $b_{2N-j} b_{2N-j-i}$. When $i + j = N$, $b_{2N-j} b_{2N-j-i} \in I_r$, so only $b_{N-i} b_N$ remains in I_m. From Lemma 4.0.14

$$b_{N-i} b_N = \beta_{N-i} \beta_N \alpha_{N-i} \alpha_0 = (-1)^{\frac{i(2N-i+2\delta-1)}{2}} \alpha_{N-i} \alpha_0$$

$$= (-1)^{N+\delta+\frac{i+1}{2}} \alpha_0 \alpha_{N-i} = (-1)^{\delta+\frac{i-1}{2}} \alpha_0 \alpha_{N-i}\,.$$

This proves the first part of Lemma 4.0.16. Now we prove the second part.

For $i \geq N$, if $j > 0$ then by Lemma 4.0.14, α is symmetric or antisymmetric, and i being odd,

$$b_j b_{j+i} = \beta_j \beta_{j+i} \alpha_j \alpha_{j+i-N} = (-1)^{\frac{i(2j+i+2\delta-1)}{2}} \alpha_{N-j} \alpha_{2N-j-i}$$

$$= -(-1)^{\frac{i(2j+i-2\delta+1)}{2}} \alpha_{N-j} \alpha_{2N-j-i}$$

$$= -(-1)^{\frac{i(2j+i-2\delta+1-4N)}{2}} \alpha_{N-j} \alpha_{2N-j-i}$$

$$= -\beta_{2N-j} \beta_{2N-j-i} \alpha_{N-j} \alpha_{2N-j-i} = -b_{2N-j} b_{2N-j-i} \,.$$

Therefore every term $b_j b_{j+i}$ is canceled by $b_{2N-j} b_{2N-j-i}$ except for the term

$$b_0 \; b_i = \beta_0 \; \beta_i \; \alpha_0 \; \alpha_{i-N} = (-1)^{\binom{i+\delta}{2}} \alpha_0 \alpha_{i-N}$$

$$= (-1)^{i\,\delta \,+\, i\,\frac{i-1}{2}} \alpha_0 \; \alpha_{i-N} = (-1)^{\delta \,+\, \frac{i-1}{2}} \alpha_0 \alpha_{i-N} \,,$$

where the last equality holds because i is odd. This proves the second part of Lemma 4.0.16. □

Lemma 4.0.17. *For an odd N, suppose $\alpha = (\alpha_0, \alpha_1, ... \alpha_{N-1})$ is a symmetric or antisymmetric binary sequence of length N. Let $b = \{\alpha \; ; \; \alpha\} * \beta$ be one of the sequences of Lemma 4.0.16. Then*

$$\sum_{k=1}^{2N-1} A_b^2(k) = N + \sum_{k=1}^{N-1} A_\alpha^2(k) + 2 \sum_{\substack{k=1 \\ even\, k}}^{N-1} P_\alpha(k) A_\alpha(k) + \sum_{\substack{k=1 \\ even\, k}}^{N-1} P_\alpha(k)^2 \,.$$

Proof. From Lemma 4.0.15 and Lemma 4.0.16, we have

$$\sum_{k=1}^{2N-1} A_b^2(k) = \sum_{\substack{k=1 \\ \text{odd } k}}^{2N-1} A_b^2(k) + \sum_{\substack{k=1 \\ \text{even } k}}^{2N-1} A_b^2(k)$$

$$= \sum_{\substack{k=1 \\ \text{odd } k}}^{2N-1} A_b^2(k) + \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} A_b^2(k) + \sum_{\substack{k=N+1 \\ \text{even } k}}^{2N-1} A_b^2(k)$$

$$= N + \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} [\, P_\alpha(k) + A_\alpha(k) \,]^2 + \sum_{\substack{k=N+1 \\ \text{even } k}}^{2N-1} A_\alpha^2(k-N)$$

$$= N + \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} A_\alpha^2(k) + \sum_{\substack{k=N+1 \\ \text{even } k}}^{2N-1} A_\alpha^2(k-N) + 2 \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha(k) A_\alpha(k)$$

$$+ \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha^2(k)$$

$$= N + \sum_{k=1}^{N-1} A_\alpha^2(k) + 2 \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha(k) A_\alpha(k) + \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha^2(k). \quad \square$$

Remark. From Lemma 4.0.17, we can see that if we have a family of binary sequences α of length N that at each N, α satisfies the following:

- α is symmetric or antisymmetric.
- $\sum_{k=1}^{N-1} P_\alpha^2(k)$ is smaller than than N^2.

Then for each N, we can construct an even length binary sequence b of length $2N$, so that the asymptotic merit factor of b is four times of the asymptotic merit factor of family of α. There is no rotation in the new families of sequences. In the following chapters, we will construct new families of α which satisfy the two features above. Then we can obtain sequences of even length binary sequences of high asymptotic merit factor 6.0.

Chapter 5

Sequences of Length $2p$ with Asymptotic Merit Factor 6.0

5.1 The Asymptotic Merit Factor of Doubled Legendre Sequences

In expression (2.3), it was shown that if F is the asymptotic merit factor of cyclically shifted Legendre sequences corresponding to the offset fraction f (the number of positions shifted divided by the length), then

$$1/F = 2/3 - 4|f| + 8f^2, \qquad |f| \leq 1/2. \tag{5.1}$$

In particular for the Legendre sequences α of length p with no shifting ($f = 0$) we have

Lemma 5.1.1. $\lim_{p\to\infty} \dfrac{p^2}{2\sum_{k=1}^{p-1} A_\alpha^2(k)} = \dfrac{3}{2}.$

□

Now we are ready to prove the main theorem of this chapter.

Theorem 5.1.2. *For each odd prime number p, let $\alpha = \alpha_p$ be the Legendre sequence of length p given in (2.1), and let $\beta = \beta_p$ be one of the binary sequences of length $2p$ from Definition 3.1.5. For each p, we further let $b = b_p$ be the length $2p$ sequence $\{\alpha\ ;\ \alpha\} * \beta$. Then the asymptotic merit factor $\lim_{p\to\infty}(F_{b_p})$ is 6.*

Proof. By Proposition 3.1.2, the Legendre sequence α is symmetric for $p \equiv 1 \pmod 4$ and antisymmetric for $p \equiv 3 \pmod 4$. Therefore by Lemma 4.0.17 we have

$$\sum_{k=1}^{2p-1} A_b^2(k) = p + \sum_{k=1}^{p-1} A_\alpha^2(k) + 2 \sum_{\substack{k=1 \\ \text{even } k}}^{p-1} c_k A_\alpha(k) + \sum_{\substack{k=1 \\ \text{even } k}}^{p-1} {c_k}^2,$$

where $c_k = P_\alpha(k) = \pm 1$ or -3 from Proposition 3.2.6.

As $|c_k| \le 3$,

$$\sum_{\substack{k=1 \\ \text{even } k}}^{p-1} {c_k}^2 = \mathrm{O}(p)\,.$$

By Lemma 5.1.1, $\sum_{k=1}^{p-1} A_\alpha^2(k) = \mathrm{O}(p^2)$; so by the Cauchy-Schwarz inequality

$$\left| \sum_{\substack{k=1 \\ \text{even } k}}^{p-1} c_k A_\alpha(k) \right| \le \sqrt{\left[\sum_{\substack{k=1 \\ \text{even } k}}^{p-1} A_\alpha^2(k) \right] \mathrm{O}(p)} \le \sqrt{\mathrm{O}(p^3)} = \mathrm{O}(p^{\frac{3}{2}})\,.$$

We combine these results with Lemma 5.1.1 to find

$$\lim_{p\to\infty} \frac{1}{F_{b_p}} = \lim_{p\to\infty} \frac{2(\sum_{k=1}^{2p-1} A_b^2(k))}{(2p)^2}$$

$$= \lim_{p\to\infty} \frac{2(p + \sum_{k=1}^{p-1} A_\alpha^2(k) + 2\sum_{\text{even } k=1}^{p-1} c_k A_\alpha(k) + \sum_{\text{even } k=1}^{p-1} {c_k}^2)}{(2p)^2}$$

$$= \lim_{p\to\infty} \frac{p}{2p^2} + \frac{\sum_{k=1}^{p-1} A_\alpha^2(k)}{2p^2} + \frac{2\sum_{\text{even } k=1}^{p-1} c_k A_\alpha(k)}{2p^2} + \frac{\sum_{\text{even } k=1}^{p-1} {c_k}^2}{2p^2}$$

$$= \lim_{p\to\infty} \frac{1}{4}\left(\frac{2\sum_{k=1}^{p-1} A_\alpha^2(k)}{p^2}\right) = \frac{1}{4}\times\frac{2}{3} = \frac{1}{6}.$$

That is, $\lim_{p\to\infty} F_{b_p} = 6$. □

Here we present some numerical experimentation inspired by similar results in [27].

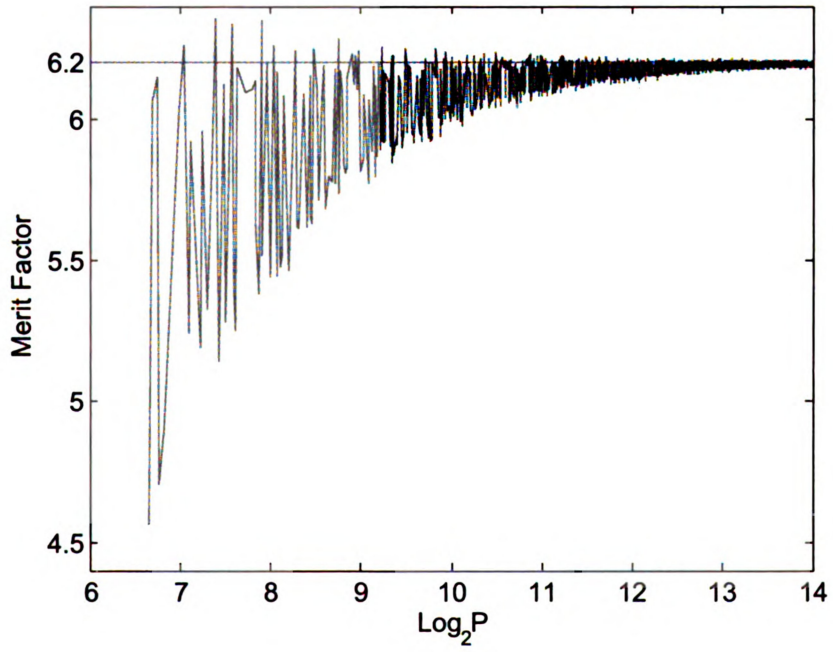

Figure 5.1: Merit factor for Parker's sequences with appending ratio 0.065.

For the sequence b of Theorem 5.1.2, we write $(-b)^f$ for the sequence $(-b_0, -b_1, \ldots, -b_{\lfloor fp\rfloor-1})$ obtained by truncating $-b$ to the fraction f of its length. Computer cal-

culation then indicated that

$$\limsup_{p\to\infty} F_{\{b:(-b)f\}} \geq 6.20$$

for $0.06 \leq f \leq 0.07$. Figure 5.1 shows the merit factor asymptote of $\left\{b\ ;\ (-b)^f\right\}$ when $f = 0.065$.

Jedwab [22] reports that Parker has done similar calculations.

5.2 The Asymptotic Merit Factor of Parker's Sequences

In [28] Parker gave a construction for sequences of length $N = 2p$, with p prime, which motivated the present investigations. We restate his results here. Let D_0 be the set of squares in GF$(p)\backslash 0$, and let D_1 be the set of nonsquares. First, Parker constructed a sequence of length $4p$ by specifying a subset C of Z_{2N}, then defined the characteristic sequence $s'(i)$ of C:

$$s'(i) = \begin{cases} 1, & \text{if } i \in C \\ 0, & \text{if } i \notin C \end{cases}$$

Let $C' = \left\{\{n\} \times C_n \,|\, C_n \subseteq Z_p^*, 0 \leq n < r\right\}$, $F = \{G \times 0 \,|\, G \subseteq Z_r\}$, and $C = C' \cup F$. Then Parker gave the concrete description of C as follows:

If prime $p = 4f + 1$,

$$\text{then let } C_0 = D_0,\ C_1 = D_0,\ C_2 = D_1,\ C_3 = D_1,\ G = \{1, 2\}.$$

If prime $p = 4f + 3$,

$$\text{then let } C_0 = D_0,\ C_1 = D_0,\ C_2 = D_1,\ C_3 = D_1,\ G = \{0, 1\}.$$

Under this construction, the characteristic sequence $s'(i)$ of $C = C' \cup F$ is of the form $s'(i) = s(i)$, for $0 \leq i < N$, and $s'(i) = s(i-N) + 1$, for $N \leq i < 2N$, where $s(i)$ is a $\{0,1\}$-sequence of length N. We convert $s(i)$ into ± 1 binary form by putting

$$b_i = (-1)^{s(i)},\ 0 \leq i \leq N-1\,. \tag{5.2}$$

Parker did computer calculations indicating that the aymptotic merit factor of the sequences b given by (5.2) is 6.0. We will show that Parker's sequence (5.2) is almost identical to the length $2p$ sequence b of Theorem 5.1.2 coming from the choice $\beta = -\beta^{(0)}$.

By the Chinese Remainder Theorem there exist n and m so that

$$n \equiv 1 \pmod 4,\ n \equiv 0 \pmod p;\ m \equiv 0 \pmod 4, \text{ and } m \equiv 1 \pmod p$$

Specifically, when $p = 4f+1$, $n = p$, $m = 3p+1$; when $p = 4f+3$, $n = 3p$, $m = p+1$. Thus the construction of $C = C' \cup F$ as above becomes

$$\begin{aligned}
(0, C_0) &= \{mD_0\} && \equiv 0 \pmod 4\,;\\
(1, C_1) &= \{n + mD_0\} && \equiv 1 \pmod 4\,;\\
(2, C_2) &= \{2n + mD_1\} && \equiv 2 \pmod 4\,;\\
(3, C_3) &= \{3n + mD_1\} && \equiv 3 \pmod 4\,.
\end{aligned}$$

Now let $j \in (0, 2p)$ with $j \neq p$:

1. Suppose $j \equiv 0 \pmod 4$. If $j = m\beta$ for some $\beta \in D_0$, then $j \in (0, C_0)$ and $b_j = (-1)^{s(j)} = -1$. At the same time, $\beta \in D_0$ implies that $\alpha_\beta = 1$. Therefore $b_j = (-1)^{s(j)} = -\alpha_\beta$ since $j \equiv \beta \pmod p$. If $j \neq m\beta$ for any $\beta \in D_0$, then $s(j) = 0$ and so $b_j = (-1)^{s(j)} = 1 = -\alpha_j$. That is, if $j \equiv 0 \pmod 4$ then $b_j = -\alpha_j$.

   Similarly, if $j \equiv 1 \pmod 4$ then $b_j = -\alpha_j$.

2. Suppose $j \equiv 2 \pmod 4$. If $j = 2n + m\beta$ for some $\beta \in D_1$, then $j \in (2, C_2)$ and $b_j = (-1)^{s(j)} = -1$. At the same time, $\beta \notin D_0$ implies that $\alpha_\beta = -1$. Therefore $b_j = \alpha_\beta$ since $j \equiv \beta \pmod p$. If $j \neq 2n + m\beta$ for any $\beta \in D_1$, then $s(j) = 0$ and so $b_j = (-1)^{s(j)} = 1 = \alpha_j$. That is, if $j \equiv 2 \pmod 4$ then $b_j = \alpha_j$.

   Similarly, if $j \equiv 3 \pmod 4$ then $b_j = \alpha_j$.

Finally, when $p = 4f + 1$, we have $F = \{p, 2p\}$ under Parker's construction, so $s(0) = 0$ and $b_0 = (-1)^{s(0)} = 1$. Then $s(p) = 1$ gives $b_p = (-1)^{s(p)} = -1$. When $p = 4f + 3$, we have $F = \{0, 3p\}$ under Parker's construction, so $s(0) = 1$ and $b_0 = (-1)^{s(0)} = -1$. Now $s(p) = 0$ gives $b_p = (-1)^{s(p)} = 1$. Therefore under Parker's construction the sequence b has the following form:

$$b_0 = (-1)^{\frac{p-1}{2}} \alpha_0, \quad b_i = \begin{cases} -\alpha_i, & if\ i \equiv 0\ or\ 1 \pmod 4,\ i \neq 0; \\ \alpha_i, & if\ i \equiv 2\ or\ 3 \pmod 4. \end{cases} \tag{5.3}$$

Comparing (5.3) with the $-\beta^{(0)}$ form of b in Theorem 5.1.2, we realize that the two sequences are exactly the same when $p = 4f + 3$. When $p = 4f + 1$ they are identical in every position except the first; Parker's sequence begins with α_0, while $-\beta^{(0)}$ sequence from Theorem 5.1.2 starts with $-\alpha_0$. From Property 3.2.12, we know that a change in one position of each sequence will not influence the aymptotic merit factor of a family (for instance. Therefore Parker's sequences have asymptotic merit factor 6 by Theorem 5.1.2.

Chapter 6

Sequences of Length $2pq$ with Asymptotic Merit Factor 6.0

This chapter is divided into three sections. In the first section, we will prove that for a character sequence χ_N with $N = pq$, we have freedom to put any new values at those position i's with $(i, N) > 1$ while the asymptotic merit factor of the new family of sequences still has the same form as in Theorem 2.3. In the second section, we will apply the doubling technique introduced in chapter 4 to the Jacobi and Modified Jacobi Sequences of length $N = pq$. In the third section, we will apply the doubling technique introduced in chapter 4 on some newly constructed sequences of length $N = pq$, so that we will obtain several families of binary sequences of length $N = 2pq$ with high asymptotic merit factor 6.0. In both sections 6.2 and 6.3, the new families of sequences are free of cyclic shifting.

Throughout this chapter, we simplify ξ_N^j as

$$\xi_j = \xi_N^j = e^{\frac{2\pi j}{N} i}$$

6.1 Theorem 6.1.1 and Proof

From the discussion in section 2.1 , we have seen that Legendre sequences, Jacobi or modified Jacobi sequences are modifications of character sequences by putting new values at positions i, with $(i, N) > 1$. When $N = pq$, the number of those positions is greater than $\sqrt{N}$. In view of Property 3.2.12, people have been hesitant to change the values at those positions. However, we show in the following theorem that we are free to put any new values at those position i's with $(i, N) > 1$.

Theorem 6.1.1. *Let $N = pq$, where $p < q$ are distinct odd primes. Then for each N, let the binary sequences $u^N = (u_0, u_1, \ldots, u_{N-1})$ satisfy*

$$u_i = \begin{cases} \chi_N(i), & \text{if } (i, N) = 1\ ; \\ \pm 1, & \text{otherwise}\ . \end{cases} \tag{6.1}$$

where the sequence χ_N is as defined in expression (2.7). Now construct any infinite sequence of such sequences

$$u = \{u^{N_1}, u^{N_2}, \ldots, u^{N_i}, \ldots\},$$

where $N_i = p_i q_i$ for $p_i < q_i$ distinct odd primes. Then u has the same asymptotic merit factor value F form as the character sequence χ, given by

$$\frac{1}{F} = \frac{2}{3} - 4|f| + 8f^2, \qquad |f| \le 1/2\ ,$$

whenever

$$\frac{N^\epsilon}{p_i} \to 0 \quad \text{when } N_i \to \infty, \tag{6.2}$$

where f is the fraction of shifting and ϵ is any positive number satisfying $0 < \epsilon < \frac{2}{5}$.

Given a sequence $x = (x_0, x_1, \ldots, x_{N-1})$ of length N, we have the *Discrete*

Fourier Transform (DFT) of the sequence, that is,

$$x[\xi_j] = \sum_{k=0}^{N-1} x_k \xi_j^k, \quad j = 0, 1, \ldots, N-1, \tag{6.3}$$

where $\xi_j = e^{\frac{2\pi j}{N} i}$.

Furthermore, for $0 \leq t < N$, let $x^t = (x_t, x_{t+1}, \ldots, x_{N-1}, x_0, x_1, \ldots, x_{t-1})$ be the offset x sequence arising from t cyclic left shifts of sequence x. The *Discrete Fourier Transform* (DFT) of x^t is then

$$x^t[\xi_j] = \sum_{k=0}^{N-1} x_{k+t} \xi_j^k, \quad j = 0, 1, \ldots, N-1, \tag{6.4}$$

where all the subscripts are taken modulo N.

Property 6.1.2. *Let $x = (x_0, x_1, \ldots, x_{N-1})$ be a real-valued sequence of length N, $\xi_j = e^{\frac{2\pi j}{N} i}$. For $x[\xi_j]$ the DFT of x as defined above,*

$$\sum_{j=0}^{N-1} |x[\xi_j]|^2 = N\|x\|^2 ,$$

where $\|x\|^2 = \sum_{k=0}^{N-1} x_k^2$.

Proof. There is a well-known trigonometric identity

$$\sum_{k=0}^{N-1} e^{\frac{2\pi k j}{N} i} = \begin{cases} N, & \text{if } N \mid j; \\ 0, & \textit{otherwise} \end{cases} \tag{6.5}$$

Then

$$\sum_{j=0}^{N-1} \left| x[\xi_j] \right|^2 = \sum_{j=0}^{N-1} \left| \sum_{k=0}^{N-1} x_k \, e^{\frac{2\,\pi\,k\,j}{N}\,i} \right|^2$$

$$= \sum_{j=0}^{N-1} \left(\sum_{k=0}^{N-1} x_k \, e^{\frac{2\,\pi\,k\,j}{N}\,i} \right) \left(\sum_{m=0}^{N-1} x_m \, e^{-\frac{2\,\pi\,m\,j}{N}\,i} \right)$$

$$= \sum_{k=0}^{N-1} \sum_{m=0}^{N-1} x_k \, x_m \sum_{j=0}^{N-1} e^{\frac{2\,\pi\,(\,k\,-\,m\,)\,j}{N}\,i}$$

$$= \sum_{\substack{k=0 \\ m=k}}^{N-1} x_k^2 \cdot N = N \, \|x\|^2$$

□

Property 6.1.3. *Suppose we have sequences* $a = (a_0, a_1, \ldots, a_{m-1})$, *and* $b = (b_0, b_1, \ldots, b_{n-1})$ *with* $(m, n) = 1$. *Let* $N = mn$ *and consider* $\sum_{j=0}^{N-1} a_j b_j$, *where the subscripts are taken modulo* m *and* n *respectively. Then*

$$\sum_{j=0}^{N-1} a_j b_j = (\sum_{k=0}^{m-1} a_k) \cdot (\sum_{s=0}^{n-1} b_s),$$

Proof.

$$\sum_{j=0}^{N-1} a_j b_j = \sum_{k=0}^{m-1} \sum_{s=0}^{n-1} a_{kn+s} b_s = \sum_{s=0}^{n-1} b_s \sum_{k=0}^{m-1} a_{kn+s} = (\sum_{k=0}^{m-1} a_k) \cdot (\sum_{s=0}^{n-1} b_s)$$

where the last equality follows from the fact that $(m, n) = 1$. □

Proof of Theorem 6.1.1

For each N, write $u^N = \chi_N + v^N$, where the sequence χ_N is the character sequence of (2.7) and u^N is as defined in (6.1). In the following proof, in order to simplify the notation, we write u, χ and v instead of u^N, χ_N and v^N. Then for each N, $0 \le t < N$, put $u^t = \chi^t + v^t$, where $u^t = (\, u_t, u_{t+1}, \ldots, u_{N-1}, u_0, u_1, \ldots, u_{t-1} \,)$ and similarly for χ^t and v^t.

For $\xi_j = e^{\frac{2\pi j}{N} i}$, where $0 \le j \le N-1$, for a fixed t, from the Discrete Fourier Transform as shown in (6.4),

$$u^t[\xi_j] = \chi^t[\xi_j] + v^t[\xi_j] = \chi^t[\xi_j] + a_j \,, \tag{6.6}$$

$$u^t[-\xi_j] = \chi^t[-\xi_j] + v^t[-\xi_j] = \chi^t[-\xi_j] + b_j \,, \tag{6.7}$$

where $a_j = v^t[\xi_j]$ and $b_j = v^t[-\xi_j]$.

Let $\widetilde{F}_t^N$ be the merit factor of χ^t. Then by Theorem 1.2 of [25] (page 35), when condition (6.2) is satisfied,

$$\lim_{N\to\infty} \frac{1}{\widetilde{F}_t^N} = \lim_{N\to\infty} \frac{1}{2N^3} \sum_{j=0}^{N-1} \Big(|\chi^t[\xi_j]|^4 + |\chi^t[-\xi_j]|^4 \Big) - 1 = \frac{2}{3} - 4|f| + 8f^2 \,,$$

where $f = \lfloor \frac{t}{N} \rfloor$ is the offset fraction.

Let F_t^N be the merit factor of u^t. Then from ([24], (5.4) page 624),

$$\frac{1}{F_t^N} = \frac{1}{2N^3} \sum_{j=0}^{N-1} \Big(|u^t[\xi_j]|^4 + |u^t[-\xi_j]|^4 \Big) - 1 \,.$$

Put $1/F_t^N - 1/\widetilde{F}_t^N = G/2N^3$. Our goal is to prove that the limit of F_t^N takes exactly the same form as $\widetilde{F}_t^N$. In other words,

$$\lim_{N\to\infty} \frac{1}{F_t^N} = \frac{2}{3} - 4|f| + 8f^2 \,,$$

provided condition (6.2) is satisfied, where $f = \lfloor \frac{t}{N} \rfloor$ is the offset fraction. So it suffices to prove that

$$G/2N^3 \to 0 \quad \text{as } N \to \infty.$$

Again, using the form ([24], (5.10), page 624),

$$\begin{aligned} |G| \le & \sum_{j=0}^{N-1} \left[|a_j|^4 + 6|\chi^t[\xi_j]|^2 \cdot |a_j|^2 + 4(|\chi^t[\xi_j]|^2 + |a_j|^2) \cdot |a_j| \cdot |\chi^t[\xi_j]| \right] \quad (6.8) \\ & + \sum_{j=0}^{N-1} \left[|b_j|^4 + 6|\chi^t[-\xi_j]|^2 \cdot |b_j|^2 + 4(|\chi^t[-\xi_j]|^2 + |b_j|^2) \cdot |b_j| \cdot |\chi^t[-\xi_j]| \right] . \end{aligned}$$

Now we look at the values of a_j and b_j, where $0 \le j \le N-1$.

$$\begin{aligned} a_j = v^t[\xi_j] = \xi_j^{-t} \left[\sum_{m=0}^{p-1} v_{mq} e^{\frac{2\pi m j}{p} i} + \sum_{k=1}^{q-1} v_{kp} e^{\frac{2\pi k j}{q} i} \right] , \\ b_j = v^t[-\xi_j] = \xi_j^{-t} \left[\sum_{m=0}^{p-1} v'_{mq} e^{\frac{2\pi m j}{p} i} + \sum_{k=1}^{q-1} v'_{kp} e^{\frac{2\pi k j}{q} i} \right] , \end{aligned} \quad (6.9)$$

where $v_{mq}, v_{kp}, v'_{mq}, v'_{kp} \in \{+1, -1\}$, for $1 \le m < q$, $1 \le k < p$. Denote

$$\left| \xi_j^{-t} \sum_{m=0}^{p-1} v_{mq} e^{\frac{2\pi m j}{p} i} \right| = |v_p^j|, \quad \left| \xi_j^{-t} \sum_{k=1}^{q-1} v_{kp} e^{\frac{2\pi k j}{q} i} \right| = |v_q^j|;$$

$$\left| \xi_j^{-t} \sum_{m=0}^{p-1} v'_{mq} e^{\frac{2\pi m j}{p} i} \right| = |\tilde{v}_p^j|, \quad \left| \xi_j^{-t} \sum_{k=1}^{q-1} v'_{kp} e^{\frac{2\pi k j}{q} i} \right| = |\tilde{v}_q^j|.$$

For any j,

$$e^{\frac{2\pi m(j+p)}{p} i} = e^{\frac{2\pi m j}{p} i} \quad \text{and} \quad e^{\frac{2\pi k(j+q)}{q} i} = e^{\frac{2\pi k j}{q} i},$$

so we have for any j,

$$|v_p^j| = |v_p^{j+p}|,\ |\widetilde{v}_p^j| = |\widetilde{v}_p^{j+p}|; \tag{6.10}$$
$$|v_q^j| = |v_q^{j+q}|,\ |\widetilde{v}_q^j| = |\widetilde{v}_q^{j+q}|.$$

From Property 6.1.2, we have

$$\sum_{j=0}^{p-1} |v_p^j|^2 = \sum_{j=0}^{p-1} |\widetilde{v}_p^j|^2 = p^2, \tag{6.11}$$

and

$$\sum_{j=0}^{q-1} |v_q^j|^2 = \sum_{j=0}^{q-1} |\widetilde{v}_q^j|^2 = q(q-1). \tag{6.12}$$

Now we estimate the sum within the first bracket in expression (7.41). Note that $|a_j| \le |v_p^j| + |v_q^j|$, $|b_j| \le |\widetilde{v}_p^j| + |\widetilde{v}_q^j|$. Then for $1 \le s \le 4$,

$$\sum_{j=0}^{N-1} |a_j|^s \le \sum_{j=0}^{N-1} (|v_p^j| + |v_q^j|)^s = \sum_{m=0}^{s} \sum_{j=0}^{N-1} \binom{s}{m} |v_p^j|^m \cdot |v_q^j|^{s-m},$$

$$\sum_{j=0}^{N-1} |b_j|^s \le \sum_{j=0}^{N-1} (|\widetilde{v}_p^j| + |\widetilde{v}_q^j|)^s = \sum_{m=0}^{s} \sum_{j=0}^{N-1} \binom{s}{m} |\widetilde{v}_p^j|^m \cdot |\widetilde{v}_q^j|^{s-m}.$$

The following calculations are the upper estimates to the values of

$$\sum_{m=0}^{s} \sum_{j=0}^{N-1} |v_p^j|^m \cdot |v_q^j|^{s-m},$$

for $1 \le s \le 4$. Suppose r is either p or q. Applying the result from (6.10), (6.11) and

(6.12), we have

$$\sum_{j=0}^{N-1} |v_r^j|^2 = \frac{N}{r} \cdot \sum_{k=0}^{r-1} |v_r^k|^2 \le Nr \; ; \tag{6.13}$$

$$\sum_{j=0}^{N-1} |v_r^j|^4 = \frac{N}{r} \cdot \sum_{k=0}^{r-1} |v_r^k|^4 \le \frac{N}{r} \cdot (\sum_{k=0}^{r-1} |v_r^k|^2)^2 \le Nr^3 \; ;$$

$$\sum_{j=0}^{N-1} |v_r^j| = \frac{N}{r} \cdot \sum_{k=0}^{r-1} |v_r^k| \le \frac{N}{r} \cdot \sqrt{\sum_{k=0}^{r-1} |v_r^k|^2 \cdot r} \le N\sqrt{r} \; .$$

Note that $(r, N/r) = 1$. By Property 6.1.3 we have

$$\sum_{j=0}^{N-1} |v_r^j| \cdot |v_{N/r}^j| = \left[\sum_{k=0}^{r-1} |v_r^k| \right] \cdot \left[\sum_{m=0}^{N/r-1} |v_{N/r}^m| \right] \tag{6.14}$$

$$\le \sqrt{\sum_{k=0}^{r-1} |v_r^k|^2 \cdot r} \times \sqrt{\sum_{m=0}^{N/r-1} |v_{N/r}^m|^2 \cdot \frac{N}{r}} \le N^{\frac{3}{2}} \; .$$

Furthermore, since $(r, N/r) = 1$, from (6.10), Property 6.1.3 and the estimate shown in (6.13) and (6.14), we obtain

$$\sum_{j=0}^{N-1} |v_r^j|^3 = \frac{N}{r} \cdot \sum_{k=0}^{r-1} |v_r^k|^3 \le \frac{N}{r} \cdot \left(\sum_{k=0}^{r-1} |v_r^k|^2 \right) \cdot \left(\sum_{k=0}^{r-1} |v_r^k| \right) \le Nr^{\frac{5}{2}} \; ; \tag{6.15}$$

$$\sum_{j=0}^{N-1} |v_r^j|^3 \cdot |v_{N/r}^j| = \left(\sum_{k=0}^{r-1} |v_r^k|^3 \right) \cdot \left(\sum_{m=0}^{N/r-1} |v_{N/r}^m| \right) \le N^{\frac{3}{2}} r^2 \; ;$$

$$\sum_{j=0}^{N-1} |v_r^j|^2 \cdot |v_{N/r}^j|^2 = \left(\sum_{k=0}^{r-1} |v_r^k|^2 \right) \cdot \left(\sum_{m=0}^{N/r-1} |v_{N/r}^m|^2 \right) \le N^2 \; ;$$

$$\sum_{j=0}^{N-1} |v_r^j|^2 \cdot |v_{N/r}^j| = \left(\sum_{k=0}^{r-1} |v_r^k|^2 \right) \cdot \left(\sum_{m=0}^{N/r-1} |v_{N/r}^m| \right) \leq N^{\frac{3}{2}} r^{\frac{1}{2}} .$$

Combine all the results above, noting that we assume $p < q$. Then when p and q are large enough, we have

$$\begin{aligned}
\sum_{j=0}^{N-1} |a_j|^4 &\leq \sum_{j=0}^{N-1} \left(|v_p^j| + |v_q^j| \right)^4 \\
&= \sum_{j=0}^{N-1} \left(|v_p^j|^4 + |v_q^j|^4 + 4|v_p^j|^3 \cdot |v_q^j| + 4|v_p^j| \cdot |v_q^j|^3 + 6|v_p^j|^2 \cdot |v_q^j|^2 \right) \\
&\leq Np^3 + Nq^3 + 4N^{\frac{3}{2}}(p^2 + q^2) + 6N^2 < 10Nq^3 . \qquad (6.16)
\end{aligned}$$

Similarly, under the same conditions for p and q, we get

$$\sum_{j=0}^{N-1} |a_j|^3 \leq \sum_{j=0}^{N-1} (|v_p^j| + |v_q^j|)^3 < 3Nq^{\frac{5}{2}} ; \qquad (6.17)$$

$$\sum_{j=0}^{N-1} |a_j|^2 \leq \sum_{j=0}^{N-1} (|v_p^j| + |v_q^j|)^2 < 4Nq ;$$

$$\sum_{j=0}^{N-1} |a_j| \leq \sum_{j=0}^{N-1} (|v_p^j| + |v_q^j|) < 2Nq^{\frac{1}{2}} .$$

In the calculation above, if we replace v_p^j with $\tilde{v}_p^j$, and v_q^j with $\tilde{v}_q^j$, then for $0 \leq m \leq s \leq 4$, the upper bounds for $\sum_{j=0}^{N-1} |v_p^j|^m \cdot |v_q^j|^{s-m}$ as in (6.13) and (6.15) are also the upper bounds for $\sum_{j=0}^{N-1} |\tilde{v}_p^j|^m \cdot |\tilde{v}_q^j|^{s-m}$. As a result, the upper bounds for $\sum_{j=0}^{N-1} |a_j|^s$ are also upper bounds for $\sum_{j=0}^{N-1} |b_j|^s$, for each $1 \leq s \leq 4$. By Theorem 3.2.7,

$$|\chi^t[\xi_j]| = |\xi_j^{-t} \chi_N[\xi_j]| = |\chi_N[\xi_j]| \leq \sqrt{N} . \qquad (6.18)$$

Using the interpolation formula ([23], (2.5), page 162)

$$\chi^t[-\xi_j] = \frac{2}{N} \sum_{k=0}^{N-1} \frac{\xi_k}{\xi_k + \xi_j} \chi^t[\xi_k] \,,$$

and the inequality (for instance, [24], page 625),

$$\sum_{k=0}^{N-1} \left| \frac{\xi_k}{\xi_k + \xi_j} \right| \leq N \log N \,,$$

combined with the result in (6.18), we have

$$|\chi^t[-\xi_j]| \leq 2\sqrt{N} \log N, \quad \text{for} \quad 0 \leq j \leq N-1 \,. \tag{6.19}$$

Combining the results from (6.18) and (6.19), we can write

$$|\chi^t[\pm\xi_j]| \leq 2\sqrt{N} \log N, \quad \text{for} \quad 0 \leq j \leq N-1 \,. \tag{6.20}$$

Now we give an upper bound to the two brackets of form (7.41) simultaneously. We use symbol c_j to represent either a_j or b_j. Using (6.16), (6.17) and (6.20), we have that there exists a positive constant C independent of N, such that

$$\sum_{j=0}^{N-1} |c_j|^4 < CNq^3 \,;$$

$$\sum_{j=0}^{N-1} 6|\chi^t(\pm\xi_j)|^2 \cdot |c_j|^2 \leq 24N \log^2 N \cdot \left(\sum_{j=0}^{N-1} |c_j|^2 \right) < CN^2 q \log^2 N \,;$$

$$\sum_{j=0}^{N-1} 4|\chi^t(\pm\xi_j)|^3 \cdot |c_j| \leq 32N^{\frac{3}{2}} \log^3 N \cdot \left(\sum_{j=0}^{N-1} |c_j| \right) < CN^{\frac{5}{2}} q^{\frac{1}{2}} \log^3 N \,;$$

$$\sum_{j=0}^{N-1} 4|\chi^t(\pm\xi_j)| \cdot |c_j|^3 \leq 8\sqrt{N}\log N \cdot \left(\sum_{j=0}^{N-1} |c_j|^3\right) < CN^{\frac{3}{2}}q^{\frac{5}{2}}\log N\,.$$

Thus the sum in the two brackets of form (7.41)

$$\sum_{j=0}^{N-1} [\ |c_j|^4 + 6|\chi^t(\pm\xi_j)|^2 \cdot |c_j|^2 + 4(\ |\chi^t(\pm\xi_j|^2 + |c_j|^2\ ) \cdot |c_j| \cdot |\chi^t(\pm\xi_j)|\ ] \sim o(N^3)\,,$$

provided the condition (6.2) is satisfied. This finishes the proof of Theorem 6.1.1. □

6.2 The Doubling of Known Sequences

Suppose the binary sequence z of length $N = pq$ is a Jacobi sequence as defined in expression (2.2). The correponding *modified Jacobi sequence* of length $N = pq$ is given by

$$m_j = \begin{cases} +1, & j = 0, q, 2q, \ldots, (p-1)q\,; \\ -1, & j = p, 2p, 3p, \ldots, (q-1)p\,; \\ \left[\frac{j}{N}\right], & gcd(j, N) = 1\,. \end{cases} \tag{6.21}$$

As defined in Section 2.1, the asymptotic merit factor F of Jacobi or modified Jacobi sequences of length $N = pq$ offset by the factor f is

$$1/F = 2/3 - 4|f| + 8f^2, \qquad |f| \leq 1/2\,, \tag{6.22}$$

provided p and q satisfy

$$\frac{(p+q)^5 \log^4 N}{N^3} \to 0, \quad for\ N \to \infty\,. \tag{6.23}$$

Particularly, for the sequence α (equal to the Jacobi sequence z or a modified Jacobi sequence m) with no shifting ($f = 0$):

Lemma 6.2.1. *Under condition (6.23), we have* $\lim_{N\to\infty} \dfrac{N^2}{2\sum_{k=1}^{N-1} A_\alpha^2(k)} = \dfrac{3}{2}$.

□

It is important to realize that under (6.23) both p and q go to infinity as N goes to infinity.

Theorem 6.2.2. *For each pair p and q of distinct primes with $p \equiv q \equiv 1 \pmod 4$, let $\alpha = \alpha_N$ be a Jacobi sequence or a modified Jacobi sequence of length $N = pq$; and let $\beta = \beta_N$ be one of the binary sequences of length $2N$ from Definition 3.1.5. For each such N, we further let $b = b_N$ be the length $2N$ sequence $\{\alpha\ ;\ \alpha\} * \beta$. Then the asymptotic merit factor $\lim_{N\to\infty}(F_{b_N})$ is 6 for $N = pq$ subject to (6.23).*

Proof. It was shown in [24] that a Jacobi or modified Jacobi sequence of length $N = pq$ is symmetric when $p \equiv q \equiv 1 \pmod 4$. By Lemma 4.0.17 we thus have

$$\sum_{k=1}^{2N-1} A_b^2(k) = N + \sum_{k=1}^{N-1} A_\alpha^2(k) + 2 \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha(k) A_\alpha(k) + \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha(k)^2 .$$

We may assume throughout that $q > p$.

For α a Jacobi sequence, the periodic correlation function $P_\alpha(k)$ has the following distribution [24, Theorem 4.2]:

$$\begin{aligned}
P_\alpha(k) = & p && \text{occurs } (q-1)/2 \text{ times};\\
& -3p && \text{occurs } (q-1)/2 \text{ times};\\
& q && \text{occurs } (p-1)/2 \text{ times};\\
& -3q && \text{occurs } (p-1)/2 \text{ times};\\
& 1 && \text{occurs } (p-1)(q-1)/4 \text{ times};
\end{aligned}$$

$$P_\alpha(k) = -3 \qquad \textit{occurs } (p-1)(q-1)/2 \textit{ times};$$
$$9 \qquad \textit{occurs } (p-1)(q-1)/4 \textit{ times}.$$

Therefore

$$\sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha(k)^2 = \mathrm{O}(pq^2)\,.$$

By Lemma 6.2.1, when p and q satisfy (6.23) we have $\sum_{k=1}^{N-1} A_\alpha^2(k) = \mathrm{O}(N^2)$. Therefore by the Cauchy-Schwarz inequality

$$\left| \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha(k) A_\alpha(k) \right| \le \sqrt{\left[\sum_{\substack{k=1 \\ \text{even } k}}^{N-1} A_\alpha^2(k) \right] \mathrm{O}\left(pq^2 \right)} \le \sqrt{\mathrm{O}\left(p^3 q^4 \right)} = \mathrm{O}\left(p^{\frac{3}{2}} q^2 \right)$$

Combining these results with Lemma 6.2.1, we calculate (as in Theorem 5.1.2) that, for p and q subject to (6.23), the asymptotic merit factor is

$$\begin{aligned} \lim_{N\to\infty}(F_b) &= \lim_{N\to\infty} \frac{(2N)^2}{2(\sum_{k=1}^{2N-1} A_b^2(k))} \\ &= \lim_{N\to\infty} \frac{4N^2}{2\sum_{k=1}^{N-1} A_\alpha^2(k)} \\ &= 4 \times \frac{3}{2} = 6\,. \end{aligned}$$

Similarly for α a modified Jacobi sequence, the periodic correlation function $P_\alpha(k)$ has the following distribution [31, p. 246]:

$$P_\alpha(k) = q-p-3 \qquad \textit{occurs } (q-1) \textit{ times};$$
$$p-q+1 \qquad \textit{occurs } (p-1) \textit{ times};$$
$$1 \qquad \textit{occurs } (p-1)(q-1)/2 \textit{ times};$$

$$P_\alpha(k) = -3 \qquad \textit{occurs } (p-1)(q-1)/2 \textit{ times}.$$

$$\text{Therefore} \qquad \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha(k)^2 = \mathrm{O}(pq) = \mathrm{O}(N).$$

By Lemma 6.2.1 when p and q satisfy (6.23) we have $\sum_{k=1}^{N-1} A_\alpha^2(k) = \mathrm{O}(N^2)$. Hence by the Cauchy-Schwarz inequality

$$\left| \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha(k) A_\alpha(k) \right| \le \sqrt{\left[\sum_{\substack{k=1 \\ \text{even } k}}^{N-1} A_\alpha^2(k) \right] \mathrm{O}(N)} \le \sqrt{\mathrm{O}\left(N^3\right)} = \mathrm{O}\left(N^{\frac{3}{2}}\right).$$

We again combine all the results above with Lemma 6.2.1 and find that, when p and q satisfy (6.23), the asymptotic merit factor is

$$\lim_{N\to\infty} F_b = \lim_{N\to\infty} \frac{(2N)^2}{2\left(\sum_{k=1}^{2N-1} A_b^2(k)\right)}$$

$$= \lim_{N\to\infty} \frac{4N^2}{2\left(\sum_{k=1}^{N-1} A_\alpha^2(k)\right)}$$

$$= 4 \times \frac{3}{2} = 6.$$

□

6.3 The Construction of New Sequences and Doubling

Throughout this section, we define the triple-valued sequence V of length N to be

$$V_j = \begin{cases} \chi_N(j) & , j = 1, \ldots, N-1; \\ 1 & , j = 0 \end{cases} \tag{6.24}$$

From Property 3.2.3, the sequence V is symmetric when $N \equiv 1 \pmod 4$ and antisymmetric when $N \equiv 3 \pmod 4$. Our goal is to construct specific families of binary sequences based on the triple-valued sequence V. These new sequences have the same symmetric type as the sequence V, depending upon the values of N modulo 4.

Definition 6.3.1. *Suppose $N = pq$, where p and q are distinct odd primes. Let the sequence V of length N be as defined in (6.24). Then we define the binary sequences x, y and z of length N with*

$$x_j = y_j = z_j = V_j, \qquad for\ j = 0 \ \ and \ \ (j, N) = 1.$$

Otherwise, for $\{r, d\} = \{p, q\}$ and $1 \le k \le r-1$, put

$$x_{kd} = \begin{cases} (-1)^{\overline{kr}} & , if\ N \equiv 3 \pmod 4\,; \\ (-1)^{\widetilde{kr}} & , if\ N \equiv 1 \pmod 4. \end{cases}$$

$$y_{kd} = \begin{cases} \chi_r(k) & , if\ k \le \frac{r-1}{2}\,; \\ \chi_d(-1) \cdot \chi_r(k) & , if\ k > \frac{r-1}{2}. \end{cases}$$

$$z_{kd} = \left(\chi_d(-1)\right)^k \cdot \chi_r(k).$$

To better understand the definitions of sequences x, y, and z, we will study a concrete example.

Example 1. *Suppose* $N = 3 \times 5 = 15$, *the sequence* V *of length* 15 *is as defined in expression (6.24), and the Jacobi sequence* J *of length* 15 *is as shown in Table 1. Then we have*

position j	0	1	2	3	4	5	6	7
V_j	+1	+1	+1	0	+1	0	0	−1
J_j	+1	+1	+1	+1	+1	+1	−1	−1
				↑			↑	
				$\chi_5(1)$			$\chi_5(2)$	

position j	8	9	10	11	12	13	14
V_j	+1	0	0	−1	0	−1	−1
J_j	+1	−1	−1	−1	+1	−1	−1
		↑			↑		
		$\chi_5(3)$			$\chi_5(4)$		

Here V is antisymmetric because $15 \equiv 3 \pmod 4$. But the Jacobi sequence J is neither symmetric nor antisymmetric; indeed, the positions 0, 3, 6, 9, and 12 give a subsequence $(1, \chi_5(1), \chi_5(2), \chi_5(3), \chi_5(4))$ which is symmetric since $5 \equiv 1 \pmod 4$. Definition 6.3.1 gives new values on positions j, with $(j, 15) > 1$:

j	3	5	6
J_j	$\chi_5(1) = 1$	$\chi_3(1) = 1$	$\chi_5(2) = -1$
x_j	$(-1)^{\overline{15}} = -1$	$(-1)^{\overline{13}} = -1$	$(-1)^{\overline{25}} = -1$
y_j	$\chi_5(1) = 1$	$\chi_3(1) = 1$	$\chi_5(2) = -1$
z_j	$(-1)^1\chi_5(1) = -1$	$\chi_3(1) = 1$	$(-1)^2\chi_5(2) = -1$

Note that in Example 1, x, y and z only differ at positions j, where $(j, N) > 1$, and all are antisymmetric, as is V. This is a concrete example of the following general result.

j	9	10	12
J_j	$\chi_5(3) = -1$	$\chi_3(2) = -1$	$\chi_5(4) = 1$
x_j	$(-1)^{\overline{35}} = 1$	$(-1)^{\overline{23}} = 1$	$(-1)^{\overline{45}} = 1$
y_j	$-\chi_5(3) = 1$	$\chi_3(2) = -1$	$-\chi_5(4) = -1$
z_j	$(-1)^3\chi_5(3) = 1$	$\chi_3(2) = -1$	$(-1)^4\chi_5(4) = 1$

Lemma 6.3.2. *Suppose $N = pq$, where p and q are distinct odd primes. Let the three binary sequences x, y and z of length N be as defined in Definition 6.3.1. Then x, y and z are symmetric if $N \equiv 1(\ mod\ 4)$, and antisymmetric if $N \equiv 3(\ mod\ 4)$.*

Proof. To shorten the proof, we use the notation u_j to represent one of x_j, y_j, or z_j.

If $(j, N) = 1$, $u_j = V_j$, thus by Lemma 3.2.3, we have

$$u_j = u_{N-j}, \text{ if } N \equiv 1 \pmod 4 ;$$
$$u_j = -u_{N-j}, \text{ if } N \equiv 3 \pmod 4 .$$

We wish to prove this for all j's with $1 \leq j \leq N-1$.

By Lemma 3.2.3, for $m \in \{p, q, N\}$, we have $\chi_m(-1) = (-1)^{\frac{m-1}{2}}$. In particular, the two equalities above are equivalent to the single equality

$$u_j \cdot u_{N-j} = \chi_N(-1).$$

Let $\{r, d\} = \{p, q\}$, so that $N = rd$ and $N - kd = (r-k)\cdot d$. Therefore to complete the proof of the lemma, it is enough to verify

$$u_{kd} \cdot u_{(r-k)d} = \chi_N(-1).$$

for all $1 \leq k \leq \frac{r-1}{2}$. We do this in cases.

First,

$$\begin{aligned} y_{kd} \cdot y_{(r-k)d} &= \chi_r(k) \cdot \chi_d(-1) \cdot \chi_r(r-k) \\ &= \chi_d(-1) \cdot \chi_r(k) \cdot \chi_r(-k) \\ &= \chi_d(-1) \cdot \chi_r(-1) \cdot (\chi_r(k))^2 = \chi_N(-1). \end{aligned}$$

Next,

$$\begin{aligned} z_{kd} \cdot z_{(r-k)d} &= (\chi_d(-1))^k \cdot \chi_r(k) \cdot (\chi_d(-1))^{r-k} \cdot \chi_r(r-k) \\ &= (\chi_d(-1))^r \cdot \chi_r(k) \cdot \chi_r(-k) \\ &= \chi_d(-1) \cdot \chi_r(-1) \cdot (\chi_r(k))^2 = \chi_N(-1), \end{aligned}$$

since when r is odd, $(\chi_d(-1))^r = \chi_d(-1)$.

Finally, if $N \equiv 1 \pmod 4$,

$$\begin{aligned} x_{kd} \cdot x_{(r-k)d} &= (-1)^{\widetilde{kr}} \cdot (-1)^{\widetilde{(r-k)r}} \\ &= (-1)^{\overline{kr}} \cdot (-1)^{\overline{kr}} = 1 = \chi_N(-1)\,, \end{aligned}$$

while if $N \equiv 3 \pmod 4$, then by Lemma 3.1.7

$$\begin{aligned} x_{kd} \cdot x_{(r-k)d} &= (-1)^{\overline{kr}} \cdot (-1)^{\overline{(r-k)r}} \\ &= (-1)^{\overline{kr}} \cdot (-1)^{r-\overline{kr}} \\ &= (-1)^r = -1 = \chi_N(-1). \end{aligned}$$

Combing all the results above, we have that x, y and z are symmetric when $N \equiv 1(\bmod 4)$, and antisymmetric when $N \equiv 3(\bmod 4)$. In other words, x, y and z have the same symmetric type as the sequence V. □

Recall that the product of sequences "$*$" and sequence $\beta^{(\delta)}$ are as defined in Definition 3.1.1 and Definition 3.1.5. In [39], certain sequences $b = (u, u) * (\pm\beta^{(\delta)})$ give rise to sequences with asymptotic merit factor $4 \times F$ once the following are demonstrated:

(a) u is symmetric or antisymmetric ;

(b) the sequences u have asymptotic merit factor F ;

(c) the periodic autocorrelations have $\sum_{i=1}^{N-1} P_u^2(i) \sim o(N^2)$.

Here Lemma 6.3.2 provides (a), and Theorem 6.1.1 gives (b) with $F = 1.5$. Therefore we will be able to prove the following theorem, once we have studied autocorrelations in the next section. Based on the new constructions, we will prove the following Theorem.

Theorem 6.3.3. *For each $N = p_N q_N$, where $p_N < q_N$ are distinct odd primes, let u^N be any one of the binary sequences x, y and z as in Definition 6.3.1. Let the sequence β^N of length $2N$ be one of the four sequences $\pm\beta^{(\delta)}$ from the Definition 3.1.5. Let $b_N = \{u^N, u^N\} * \beta^N$, be a sequence of length $2N$. Then the sequence of sequences $\{b_N\}$ has asymptotic merit factor 6.0 provided*

$$\frac{N^\epsilon}{p_N} \to 0 \quad \textit{when } N \to \infty \,, \tag{6.25}$$

where ϵ satisfies $0 < \epsilon < \frac{2}{5}$.

We will prove Theorem 6.3.3 in steps.

From Lemma 3.2.5 and Property 6.1.3, the periodic autocorrelations of χ_N are

$$P_{\chi_N}(j) = P_{\chi_p}(j) \times P_{\chi_q}(j) = \begin{cases} 1-p & , \textit{if } p \mid j \,; \\ 1-q & , \textit{if } q \mid j \,; \\ +1 & , \textit{otherwise} \,. \end{cases}$$

Therefore, the periodic autocorrelations of the sequence V of (6.24) satisfy

$$|P_V(j)| \leq \begin{cases} 1+p & , \textit{if } p \mid j \ ; \\ 1+q & , \textit{if } q \mid j \ ; \\ +3 & , \textit{otherwise} \ . \end{cases} \tag{6.26}$$

where V is as defined in (6.24).

Property 6.3.4. *For p an odd primes, let χ_p be the primitive character mod p as defined in (2.6). Then for any k, we have*

$$|\sum_{n=0}^{p-1}(-1)^n\chi_p(n)\chi_p(n+k)| \leq \begin{cases} 36p^{\frac{1}{2}}\log p + 1 & , \textit{if } p \nmid k \\ 0 & , \textit{if } p \mid k \end{cases}$$

Proof. The result is obviously correct when $p|k$. Now suppose $p \nmid k$. From Lemma 3.2.5,

$$\begin{aligned} & |\sum_{n=0}^{p-1}(-1)^n\chi_p(n)\chi_p(n+k)| \\ = \ & |\sum_{j=1}^{\frac{p-1}{2}}\chi_p(2j)\chi_p(2j+k) - \sum_{j=1}^{\frac{p-1}{2}}\chi_p(2j-1)\chi_p(2j-1+k)| \\ \leq \ & |\sum_{j=1}^{\frac{p-1}{2}}\chi_p(2j)\chi_p(2j+k)| + |\sum_{j=1}^{\frac{p-1}{2}}\chi_p(2j-1)\chi_p(2j-1+k)| \\ \leq \ & 2|\sum_{j=1}^{\frac{p-1}{2}}\chi_p(2j)\chi_p(2j+k)| + 1 \\ = \ & 2|\sum_{j=1}^{\frac{p-1}{2}}\chi_p(j(j+2^{-1}k))| + 1 \ . \end{aligned}$$

Weil [34] proved that the Riemann Hypothesis is true for the zeta-function of an algebraic function field over a finite field. A specifically useful consequence is that, for any integers u and v with $v > 0$,

$$|\sum_{u<j<u+v} \chi_p(f(j))| \leq 9mp^{\frac{1}{2}} \log p\,, \tag{6.27}$$

where $f(x) \in F_p[x]$ is a polynomial of degree m not of the form $b(g(x))^2$ with $b \in F_p$, $g(x) \in F_p[x]$. (The readers can find a detailed proof for equation (6.27) in [37] Corollary 1.) When $p \nmid k$, the polynomial $x(x + 2^{-1}k)$ is not the square of any polynomial over $F_p[x]$, so

$$|\sum_{j=1}^{\frac{p-1}{2}} \chi_p(j(j + 2^{-1}k))| \leq 18p^{\frac{1}{2}} \log p\,,$$

hence

$$|\sum_{n=0}^{p-1} (-1)^n \chi_p(n)\chi_p(n+k)| \leq 36p^{\frac{1}{2}} \log p + 1\,.$$

□

For the triple-valued sequence V defined in (6.24), write $u_j = V_j + v_j^u$, where u could be any one of the binary sequences x, y or z of length N as defined in Definition 6.3.1. For instance, for $\{r, d\} = \{p, q\}$ and $1 \leq k \leq r-1$, when $u = x$,

$$v_j^x = \begin{cases} (-1)^{\overline{kr}} & , \textit{if } j = kd, \text{ and } N \equiv 3 \pmod 4\,; \\ (-1)^{\widetilde{kr}} & , \textit{if } j = kd, \text{ and } N \equiv 1 \pmod 4\,; \\ 0 & , \textit{otherwise}; \end{cases}$$

and if $u = z$,

$$v_j^z = \begin{cases} \left(\chi_d(-1)\right)^k \cdot \chi_r(k) & , \text{ if } j = kd\,; \\ 0 & , \text{ otherwise.} \end{cases} \tag{6.28}$$

In all three cases, we have

$$\sum_{j=0}^{N-1} |v_j^u| \leq pq - (p-1)(q-1) = p + q - 1 < 2q\,. \tag{6.29}$$

as $p < q$. As remarked in the previous section, we wish to prove that $\sum_{i=1}^{N-1} P_u^2(i) \sim o(N^2)$. The most important part of that is the following technical lemma.

Lemma 6.3.5. *Suppose $N = pq$, where p, q are distinct odd primes with $p < q$. Let the sequence V be as defined in form (6.24), and write $u_j = V_j + v_j^u$, where u could be any one of the binary sequences x, y or z of length N as defined in Definition 6.3.1. Then when p and q are large enough, for $\{r, d\} = \{p, q\}$, we have*

$$|P_v u(i)| \leq \begin{cases} 2, & \text{if } (i, N) = 1, \\ 4r^{\frac{1}{2}} \log^3(r), & \text{if } (i, N) = d. \end{cases}$$

Proof. For any $1 \leq i \leq N-1$, $P_v u(i) = \sum_{j=0}^{N-1} v_j^u v_{j+i}^u$, while from the definition

$$v_j^u v_{j+i}^u \neq 0 \Leftrightarrow (j, N) = m_1 > 1, \quad \text{and} \quad (j+i, N) = m_2 > 1\,.$$

We break the proof into cases:

Case 1 $m_1 \neq m_2$, and $(i, N) = 1$.

Case 2 $m_1 = m_2 = (i, N) = d$, with $\{r, d\} = \{p, q\}$.

We first note that this handles all situations in which nonzero coefficients occur.

Clearly if $m_1 = m_2$, then $(i, N) = m_1 = m_2$. If $m_1 \neq m_2$, there must be $0 < k < r$ and $0 < s < d$ with

$$kd \pm i = j \pm i \equiv sr \pmod{N},$$

As $d \nmid s$ we have $d \nmid i$, and similarly $r \nmid i$ as $d \nmid k$. Therefore $m_1 \neq m_2$ implies $(i, N) = 1$.

Case 1 $m_1 \neq m_2$, and $(i, N) = 1$.

First suppose $d = m_1$, $r = m_2$. Then as above there exist $0 < k < r$ and $0 < s < d$, such that

$$kd + i = j + i \equiv sr \pmod{N}, \tag{6.30}$$

Such a pair k and s is unique. Indeed if there exists another pair $0 < k' < r$ and $0 < s' < d$, such that

$$k'd + i \equiv s'r \pmod{N},$$

then $(k - k')d \equiv (s - s')r \pmod{N}$. As $d|N$ and $d|(k - k')d$, we find $d|(s - s')$ with $0 < s, s' < d$. Therefore, $s = s'$, and similarly, $k = k'$.

In addition, if expression (6.30) is satisfied, then $kd + i \equiv sr \pmod{N}$ implies $(d - s)r + i \equiv (r - k)d \pmod{N}$, and this must give the unique solution pair when $r = m_1$ and $d = m_2$. Therefore, when $(i, N) = 1$,

$$|P_v^u(i)| \leq |v_{kd}^u v_{sr}^u + v_{-kd}^u v_{-sr}^u| \leq 2 .$$

Case 2 $m_1 = m_2 = (i, N) = d$, with $\{r, d\} = \{p, q\}$.

There is an s with $0 < s < r$, and

$$P_v u(i) = \sum_{j=1}^{r-1} v_{jd}^u v_{(s+j)d}^u . \tag{6.31}$$

Case 2.1 $(i, N) = d$ and $u = x$.

In 1998, W. Zhang [32] proved that for any integer t,

$$\sum_{\substack{n=1 \\ r\nmid n+t}}^{r-1} (-1)^{\overline{nr}+\overline{(n+t)r}} \leq \sqrt{r}\ \log^2 r\ . \tag{6.32}$$

where $\overline{nr}$ is as in Definition 3.1.6.

More generally, for any integers t, t_1 and t_2 with $t > 0$, H. Liu proved [33]

$$|\sum_{\substack{t1<n<t2 \\ r\nmid n,n+t}} (-1)^{\overline{nr}+\overline{(n+t)r}}| \leq \sqrt{r}\ \log^3 r\ . \tag{6.33}$$

In the following proof, to simplify the notations, we use notation $\overline{j}$ instead of $\overline{jr}$.

When $N \equiv 3 \pmod 4$, from (6.32),

$$P_v x(i) = \sum_{j=1}^{r-1} v_{jd}^x v_{(s+j)d}^x = \sum_{\substack{j=1 \\ r\nmid j+s}}^{r-1} (-1)^{\overline{j}+\overline{s+j}} \leq \sqrt{r}\ \log^2 r\ ,$$

When $N \equiv 1 \pmod 4$, suppose $s \leq (r-1)/2$. Then from Lemma 3.1.7 and expression (6.33),

$$|P_v x(i)| = \left|\sum_{j=1}^{r-1} v_{jd}^x v_{(s+j)d}^x\right|$$

$$= \left|\left(\sum_{j=1}^{\frac{r-1}{2}-s} + \sum_{j=\frac{r-1}{2}-s+1}^{\frac{r-1}{2}} + \sum_{j=\frac{r-1}{2}+1}^{r-1-s} + \sum_{j=r-s}^{r-1}\right) v_{jd}^x v_{(s+j)d}^x\right|$$

$$
\begin{aligned}
=| &\sum_{j=1}^{\frac{r-1}{2}-s} (-1)^{\bar{j}+\overline{s+j}} - \sum_{j=\frac{r-1}{2}-s+1}^{\frac{r-1}{2}} (-1)^{\bar{j}+\overline{s+j}} \\
&+ \sum_{j=\frac{r-1}{2}+1}^{r-1-s} (-1)^{\bar{j}+\overline{s+j}} - \sum_{j=r-s}^{r-1} (-1)^{\bar{j}+\overline{s+j}} |
\end{aligned}
$$

$$
\begin{aligned}
\leq &\left| \sum_{j=1}^{\frac{r-1}{2}-s} (-1)^{\bar{j}+\overline{s+j}} \right| + \left| \sum_{j=\frac{r-1}{2}-s+1}^{\frac{r-1}{2}} (-1)^{\bar{j}+\overline{s+j}} \right| \\
&+ \left| \sum_{j=\frac{r-1}{2}+1}^{r-1-s} (-1)^{\bar{j}+\overline{s+j}} \right| + \left| \sum_{j=r-s}^{r-1} (-1)^{\bar{j}+\overline{s+j}} \right| \\
\leq &4\sqrt{r}\ \log^3 r\ .
\end{aligned}
$$

Case 2.2 $(i, N) = d$ and $u = y$.

If $d \equiv 1 \pmod 4$, then from Lemma 3.2.5, expression (6.31) is

$$
P_v y(i) = \sum_{j=1}^{r-1} v^y_{jd} v^y_{(s+j)d} = \sum_{j=1}^{r-1} \chi_r(j)\chi_r(j+s) = -1\ .
$$

If $d \equiv 3 \pmod 4$, then expression (6.31) becomes

$$
|P_v y(i)| = \left| \sum_{j=1}^{r-1} v^y_{jd} v^y_{(s+j)d} \right|
$$

$$
= \left| (\sum_{j=1}^{\frac{r-1}{2}-s} + \sum_{j=\frac{r-1}{2}-s+1}^{\frac{r-1}{2}} + \sum_{j=\frac{r-1}{2}+1}^{r-1-s} + \sum_{j=r-s}^{r-1}) v^y_{jd} v^y_{(s+j)d} \right|
$$

$$\leq \left| \sum_{j=1}^{\frac{r-1}{2}-s} \chi_r(j)\chi_r(s+j) \right| + \left| \sum_{j=\frac{r-1}{2}-s+1}^{\frac{r-1}{2}} \chi_r(j)\chi_r(s+j) \right|$$

$$+ \left| \sum_{j=\frac{r-1}{2}+1}^{r-1-s} \chi_r(j)\chi_r(s+j) \right| + \left| \sum_{j=r-s}^{r-1} \chi_r(j)\chi_r(s+j) \right|$$

$$\leq 72\sqrt{r}\,\log r\,,$$

The last inequality follows from equation (6.27) by taking the degree $m = 2$.

Case 2.3 $(i, N) = d$ and $u = z$.

Equation (6.31) becomes

$$|P_v z(i)| = |\sum_{j=1}^{r-1} v_{jd}^z v_{(s+j)d}^z| = |\sum_{j=1}^{r-1} (\chi_d(-1))^j \cdot \chi_r(j) \cdot (\chi_d(-1))^{(s+j)_r} \cdot \chi_r(s+j)|,$$

where $0 \leq (s+j)_r \leq r-1$, and $(s+j)_r \equiv s+j \pmod{r}$.

Now we study the values of $\zeta_j = (\chi_d(-1))^{j+(s+j)_r}$. From Definition 6.3.1, we have

1. $\zeta_j = 1$, if $d \equiv 1 \pmod 4$.

2. $\zeta_j = (-1)^{j+(s+j)_r}$, if $d \equiv 3 \pmod 4$.

If $d \equiv 1 \pmod 4$,

$$|\sum_{j=1}^{r-1} \chi_r(j) \cdot \chi_r(s+j)| = 1\,, \quad \text{since } d \nmid s.$$

If $d \equiv 3 \pmod 4$, let j_1 be the number such that $s + j_1 < r$, but $s + j_1 + 1 \geq r$.

Then

$$
\begin{aligned}
|P_v z(i)| &= |\sum_{j=1}^{j_1} \chi_r(j)\chi_r(s+j) - \sum_{j=j_1+1}^{r-1} \chi_r(j)\chi_r(s+j)| \\
&\leq |\sum_{j=1}^{j_1} \chi_r(j)\chi_r(s+j)| + |\sum_{j=j_1+1}^{r-1} \chi_r(j)\chi_r(s+j)| \\
&\leq 36\sqrt{r}\ \log r\ .
\end{aligned}
$$

Again, the last inequality comes from equation (6.27) by putting the degree $m = 2$. □

Now we are ready to prove that $\sum_{i=1}^{N-1} P_u^2(i) \sim o(N^2)$:

Lemma 6.3.6. *Suppose $N = pq$, where $p < q$ are distinct odd primes. Then when $q \leq p^2$, and both p and q are large enough, we have*

$$\sum_{i=1}^{N-1} P_u^2(i) \leq cNq$$

where u may be any one of binary sequences x, y and z of length N as defined in Definition 6.3.1 and c is a constant independent of N.

Proof. Again, using the notation of Lemma 6.3.5, we write $u = V + v$, where v may be any one of sequences v^x, v^y, or v^z. Then by Property 3.2.13, we have

$$\sum_{i=1}^{N-1} P_u^2(i) = A + B + C + D + E + F \tag{6.34}$$

In expression (6.34), we have separated the summands into six groups. For instance $A = \sum_{i=1}^{N-1} P_V^2(i)$, and $F = \sum_{i=1}^{N-1} [\ 2P_{V,v}(i)P_{v,V}(i) + P_{V,v}^2(i) + P_{v,V}^2(i)\ ]$. In the following, each of the sums $X \in \{A, B, C, D, E, F\}$ will be bounded above by $c_X \cdot N \cdot q$ for appropriate constants c_X. To simplify the notation, it should be understood that

all of the following statements are valid when p and q are **large enough**.

For group A, from equation (6.26),

$$\sum_{i=1}^{N-1} P_V^2(i) = \sum_{(i,N)=1}^{N-1} P_V^2(i) + \sum_{(i,N)=p}^{N-1} P_V^2(i) + \sum_{(i,N)=q}^{N-1} P_V^2(i) \qquad (6.35)$$

$$\leq 9\phi(N) + q \times (1+p)^2 + p \times (1+q)^2 < 3Nq\,.$$

For group B, using Lemma 6.3.5, we have

$$\sum_{i=1}^{N-1} P_v^2(i) = \sum_{(i,N)=1} P_v^2(i) + \sum_{(i,N)=p} P_v^2(i) + \sum_{(i,N)=q} P_v^2(i)$$

$$\leq 4\phi(N) + 16q^2 \log^6 q + 16p^2 \log^6 p < Nq\,.$$

Also from Lemma 6.3.5,

$$|C| = 2|\sum_{i=1}^{N-1} P_V(i)P_v(i)| \leq 2\sum_{i=1}^{N-1} |P_V(i)P_v(i)|$$

$$= 2\sum_{(i,N)=1} |P_V(i)P_v(i)| + 2\sum_{(i,N)=p} |P_V(i)P_v(i)| + 2\sum_{(i,N)=q} |P_V(i)P_v(i)|$$

$$\leq 12\phi(N) + 9Np^{\frac{1}{2}} \log^3 p + 9Nq^{\frac{1}{2}} \log^3 q$$

$$< 19Nq^{\frac{1}{2}} \log^3 q < Nq\,.$$

For group D, by equations (6.26) and (6.29), the absolute value of the first item is

$$|\sum_{i=1}^{N-1} P_V(i)P_{V,v}(i)| = \left|\sum_{i=1}^{N-1} P_V(i)\left(\sum_{m=0}^{N-1} v_m V_{m-i}\right)\right|$$

$$\leq \sum_{i=1}^{N-1} |P_V(i)| \sum_{m=0}^{N-1} |v_m| < 2q \times \sum_{i=1}^{N-1} |P_V(i)|\,;$$

Similarly, we can show that any other item in group D is bounded above by

$$2q \times \sum_{i=1}^{N-1} |P_V(i)|.$$

Again from (6.26), we have

$$|D| \leq 8q \times \sum_{i=1}^{N-1} |P_V(i)| = 8q \times [\sum_{\substack{i=1 \\ (i,N)=1}}^{N-1} |P_V(i)| + \sum_{\substack{i=1 \\ (i,N)>1}}^{N-1} |P_V(i)| \ ]$$

$$\leq 8q \times [3\phi(N) + 3N] < 48Nq\,.$$

Now for group E. Again, consider the absolute value of item

$$|\sum_{i=1}^{N-1} P_{v,V}(i)P_v(i)| = |\sum_{i=1}^{N-1} P_v(i)(\sum_{j=0}^{N-1} v_j V_{j+i})|$$

$$\leq \sum_{i=1}^{N-1} |P_v(i)| \left(\sum_{j=0}^{N-1} |v_j|\right) < 2q \sum_{i=1}^{N-1} |P_v(i)|\,.$$

Similarly any other item in group E has absolute value bounded above by

$$2q \sum_{i=1}^{N-1} |P_v(i)|.$$

Thus using Lemma 6.3.5 and expression (6.29),

$$
\begin{aligned}
|E| &\le 8q \sum_{i=1}^{N-1} |P_v(i)| = 8q \times [\sum_{(i,N)=1} |P_v(i)| + \sum_{(i,N)=p} |P_v(i)| + \sum_{(i,N)=q} |P_v(i)|\,] \\
&\le 8q \times [2\phi(N) + 4p^{\frac{3}{2}} \log^3 p + 4q^{\frac{3}{2}} \log^3 q] \\
&\le 17Nq\,,
\end{aligned}
$$

where the last inequality follows from the assumption that $q \le p^2$.

Finally, consider the first item in group F.

$$
\begin{aligned}
|\sum_{i=1}^{N-1} P_{V,v}(i) P_{v,V}(i)| &= |\sum_{i=1}^{N-1} \sum_{j=0}^{N-1} \sum_{m=0}^{N-1} V_j v_{j+i} v_m V_{m+i}| \\
&= |\sum_{i=1}^{N-1} \sum_{j=0}^{N-1} \sum_{m=0}^{N-1} v_j v_m V_{j-i} V_{m+i}| \\
&= |\chi_N(-1) \sum_{j=0}^{N-1} \sum_{m=0}^{N-1} v_j v_m (\sum_{i=1}^{N-1} V_{i-j} V_{m+i})| \\
&= |\chi_N(-1) \sum_{j=0}^{N-1} \sum_{m=0}^{N-1} v_j v_m P_V(m+j)| \\
&= |\sum_{s=0}^{N-1} \sum_{j=0}^{N-1} v_{-j} v_{s-j} P_V(s)| \qquad \text{where } s = m+j \\
&= |\sum_{s=0}^{N-1} P_v(s) P_V(s)|\,.
\end{aligned}
$$

Similarly, we can prove that any other item in group F has the same absolute value

$|\sum_{s=0}^{N-1} P_v(s)P_V(s)|$. So

$$|F| \leq 4|\sum_{s=0}^{N-1} P_v(s)P_V(s)| \leq 4 \times \left(|P_v(0)P_V(0)| + |\sum_{s=1}^{N-1} P_v(s)P_V(s)| \right) .$$

From equation (6.29),

$$P_v(0)P_V(0) < 2Nq \; ; \tag{6.36}$$

From the estimate for group C, we know that

$$|\sum_{s=1}^{N-1} P_v(s)P_V(s)| < 19Nq^{\frac{1}{2}} \log^3 q < Nq \; ; \tag{6.37}$$

Now (7.27) and (7.28) imply that

$$|F| < 12Nq \; .$$

Combining all of the inequalities above, we obtain the desired result. □

Lemma 7.2.7 shows that when condition (6.25) is satisfied, $\sum_{i=1}^{N-1} P_u^2(i) \sim o(N^2)$, where u may be any one of the binary sequences x, y and z as defined in Definition 6.3.1. Therefore, as remarked at the end of the previous section, we are now ready to prove Theorem 6.3.3.

Proof of Theorem 6.3.3.

For each odd $N = p_N q_N$ with $p_N < q_N$, Lemma 6.3.2 shows that each of the three sequences x, y and z is symmetric or antisymmetric. Let

$$b_N = \left\{ u^N \; ; \; u^N \right\} * \beta$$

where $u^N = x, y$ or z as defined in definition 6.3.1. In the following, without confu-

sion, we use b and u instead of b_N and u^N. Then lemma 4.0.17 gives

$$\sum_{k=1}^{2N-1} A_b^2(k) = N + \sum_{k=1}^{N-1} A_u^2(k) + 2 \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_u(k)A_u(k) + \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_u(k)^2 .$$

When condition (6.2) holds, Theorem 6.1.1 shows that

$$2 \sum_{k=1}^{N-1} A_u^2(k) \sim \frac{2}{3}N^2 . \tag{6.38}$$

If the condition (6.2) holds, Lemma 7.2.7 shows that

$$\sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_u^2(k) \leq \sum_{k=1}^{N-1} P_u^2(k) = O(Nq) .$$

Then given condition (6.2), by the Cauchy-Schwarz inequality

$$\left| \sum_{k=1}^{N-1} P_u(k)A_u(k) \right| \leq \sqrt{\left[\sum_{k=1}^{N-1} A_u^2(k) \right] \mathrm{O}(Nq)} \sim N^{\frac{3}{2}} q^{\frac{1}{2}} = o(N^2) .$$

Therefore, for p and q subject to (6.2), the asymptotic merit factor of b is

$$\begin{aligned} \lim_{N\to\infty} (F_{b_N}) &= \lim_{N\to\infty} \frac{(2N)^2}{2(\sum_{k=1}^{2N-1} A_{b_N}^2(k))} \\ &= \lim_{N\to\infty} \frac{4N^2}{2\sum_{k=1}^{N-1} A_u^2(k)} \\ &= 4 \times \frac{3}{2} = 6 . \end{aligned}$$

This finishes the proof of Theorem 6.3.3. □

6.3.1 Conclusion

For a character sequence of length $N = pq$, the number of positions j with $(j, N) > 1$ is larger than $\sqrt{N}$, so those "modified" positions are large enough to make a difference in the merit factor. However, Theorem 6.1.1 shows that subject to condition (6.2), any modification on these positions will give the same asymptotic merit factor values as the character sequences. The authors were informed recently that Jedwab and Schmidt have obtained the same result independently under an improved condition ([40]). In [39], the doubling technique shown in Lemma 4.0.17 was only applied to some of the Jacobi or modified Jacobi sequences with additional restriction to the values of $p, q \pmod 4$. Here we have constructed new sequences considerably different from the canonical Jacobi or modified Jacobi sequences and with no restrictions on the values of $p, q \pmod 4$, yet achieving the same asymptotic merit factor, as seen in Theorem 6.3.3.

Chapter 7

Sequences of Length $2p_1p_2\ldots p_r$ with Asymptotic Merit Factor 6.0

In this chapter, we will give a new modification to the character sequences χ_N, where $N = p_1p_2\ldots p_r$, for p_i's distinct odd primes and $r \geq 2$. In Section 7.1, we will give the definition of the new families of binary sequences z. In Section 7.2, we will give an estimate to the periodic autocorrelations of z. And in Section 7.3, we will prove the asymptotic merit factor of z satisfies formula (5.1), and we will construct a family of binary sequences of length $2p_1p_2\ldots p_r$ with asymptotic merit factor 6.0.

7.1 Construction

Definition 7.1.1. *Let $N = p_1p_2\ldots p_r$, where p_i's are distinct odd primes and $r \geq 2$, for $1 \leq j \leq N-1$, define*

$$v_j = \begin{cases} (\chi_d(-1))^k \cdot \chi_{N/d}(k) & , \text{ if } (j,N) = d > 1 \text{ and } j = kd\,; \\ 0 & , \text{ otherwise.} \end{cases} \tag{7.1}$$

and

$$z_j = \begin{cases} 1 & , \; if \; j = 0; \\ v_j & , \; if \; (j, N) > 1; \\ V_j & , \; otherwise \end{cases} \tag{7.2}$$

where V is character sequences defined in expression (6.24).

To see the definition of sequence z more clearly, let's consider a concrete example. Suppose $N = 3 \times 5 = 15$, so $p = 3 \equiv 3(\bmod 4)$, $q = 5 \equiv 1(\bmod 4)$. Let V denote the character sequence as in (6.24), then

$$V = \{\, 0\, , +1, +1,\ \boldsymbol{0}\ , +1,\ \boldsymbol{0}\ ,\ \boldsymbol{0}, -1, +1,\ \boldsymbol{0}\ ,\ \boldsymbol{0}\ , -1,\ \boldsymbol{0}, -1, -1\}$$

$$z = \{+1, +1, +1,\ \boldsymbol{-1}, +1, \boldsymbol{+1}, \boldsymbol{-1}, -1, +1, \boldsymbol{+1}, \boldsymbol{-1}, -1, \boldsymbol{+1}, -1, -1\}$$

Note that in the above example, we put in italic type those entries at j-th positions where $(j, N) > 1$.

It is obvious that when $r = 2$, the sequence defined in Definition 7.1.1 is exactly the same sequence z as in Definition 6.3.1. Therefore Definition 7.1.1 is a generalization of Definition 6.3.1 for length $N = pq$. Then similar to Lemma 6.3.2, we will prove that the sequence z defined in Definition 7.1.1, is symmetric or antisymmetric depending on N.

Lemma 7.1.2. *Suppose $N = p_1 p_2 \ldots p_r$, where p_i's are distinct odd primes, and the binary sequence z of length N is as defined in Definition 7.1.1. Then z is symmetric if $N \equiv 1 \pmod 4$, and z is antisymmetric if $N \equiv 3 \pmod 4$.*

Proof. If $(j, N) = 1$, $z_j = v_j$, thus from Property 3.2.3,

$$z_j = z_{N-j}, \text{ if } N \equiv 1 \pmod 4 \quad \text{and} \quad z_j = -z_{N-j}, \text{ if } N \equiv 3 \pmod 4$$

Now suppose $(j, N) = d > 1$, and $j = kd$ with $1 \leq k < N/d$. For the similar reason

stated in the proof of Lemma 6.3.2, it is enough to prove that

$$z_{kd} \cdot z_{N-kd} = \chi_N(-1).$$

$$\begin{aligned} z_{kd} \cdot z_{(r-k)d} &= (\chi_d(-1))^k \cdot \chi_r(k) \cdot (\chi_d(-1))^{r-k} \cdot \chi_r(r-k) \\ &= (\chi_d(-1))^r \cdot \chi_r(k) \cdot \chi_r(-k) \\ &= \chi_d(-1) \cdot \chi_r(-1) \cdot (\chi_r(k))^2 = \chi_N(-1), \end{aligned}$$

since when r is odd, $(\chi_d(-1))^r = \chi_d(-1)$. □

The main theorem of this chapter is as follows:

Theorem 7.1.3. *For any positive integer $r \geq 2$, suppose $N = p_1 p_2 \ldots p_r$, where $p_1 < p_2 < \ldots p_r$ are distinct odd primes. Then for each N, let z^N be the binary sequence defined in Definition 7.1.1. Now construct any infinite sequence of such sequences*

$$z = \{z^{N_1}, z^{N_2}, \ldots, z^{N_i}, \ldots\},$$

with increasing lengths $N_1 < N_2 < \cdots < N_i < \ldots$.

(1) Let F be the asymptotic merit factor of z, f be the offset fraction. Then we have

$$1/F = 2/3 - 4|f| + 8f^2, \qquad |f| \leq 1/2, \text{ given}$$

$$\frac{N^\epsilon}{p_1} \to \infty \text{ for any } \epsilon \text{ small enough as } N \to \infty. \tag{7.3}$$

(2) Let the sequence β of length $2N$ be one of the four sequences $\pm\beta^{(\delta)}$ from the Definition 3.1.5. The new sequence $b = \{z\ ;\ z\} * \beta$ of length $2N$ has asymptotic merit factor 6.0 *given (7.3) is satisfied.*

We will prove Theorem 7.1.3 in steps. First of all, we will estimate the periodic

autocorrelations of sequence z in the following section.

7.2 Periodic Autocorrelations of Sequences z

First, we review some simple properties from number theory.

Lemma 7.2.1. *Let* $y^1 = (\ y_0^1, \ldots, y_{N_1-1}^1\ )$, $y^2 = (\ y_0^2, \ldots, y_{N_2-1}^2\ )$, ..., $y^r = (\ y_0^r, \ldots, y_{N_r-1}^r\ )$ *be* r *sequences (not necessarily binary) of length* $N_1, N_2, \ldots N_r$ *respectively, such that* $(N_i, N_j) = 1$ *for any* $1 \leq i < j \leq r$. *Let* $N = N_1 \times N_2 \cdots \times N_r$, *define a new sequence* $u = y^1 \otimes y^2 \otimes \ldots y^r$ *of length* N *via*

$$u_j = \prod_{i=1}^{r} y_j^i$$

Then the periodic autocorrelations of u *is*

$$P_u(j) = \prod_{i=1}^{r} P_{y^i}(j).$$

Furthermore, let $\xi_N^j = e^{\frac{2\pi j}{N} i}$, *let* $u[\xi_N^j] = \sum_{k=0}^{N-1} u_k(\xi_N^{jk})$ *be the DFT of* u *as defined in (3.1). Then there exist integers* $s_1, s_2, \ldots, s_r$ *with* $(s_i, N_i) = 1$ *for* $1 \leq i \leq r$, *and*

$$u\ [\ \xi_N^j] = \prod_{i=1}^{r} y^i[\ \xi_{N_i}^{js_i}]$$

Proof. We will prove the two results simultaneously by the induction on r. When $r = 1$, the result is trivial. Now suppose Lemma 7.2.1 holds for $r = k - 1$, where $k \geq 2$. Then for $r = k$, suppose $y^1, y^2, \ldots y^{k-1}, y^k$ is a series of sequences, where for each i, sequence y^i has length N_i, and $(N_i, N_j) = 1$ for any $1 \leq i < j \leq k$. Now denote $N' = N_1 \times N_2 \cdots \times N_{k-1}$, $u_1 = y^1 \otimes y^2 \otimes \ldots y^{k-1}$, then $u = u_1 \otimes y^k$. By

induction,

$$P_u(j) = P_{u_1}(j) P_{y^k}(j)$$

$$u[\,\xi_N^j] = u_1[\,\xi_{N'}^{js'}] \cdot y^k[\,\xi_{N_k}^{js_k}]$$

where $(s', N') = 1$ and $(s_k, N_k) = 1$. Then by induction

$$P_u(j) = P_{u_1}(j) P_{y^k}(j) = \prod_{i=1}^{k} P_{y^i}(j)$$

On the other hand, by induction,

$$u_1[\,\xi_{N'}^{js'}] = \prod_{j=1}^{k-1} y^j[\,\xi_{N_j}^{js's_j}]$$

where $(s_j, N_j) = 1)$, for $j = 1, 2, \ldots k-1$. Since $(s', N') = 1$, we have $(s', N_j) = 1$, for $j = 1, 2, \ldots k-1$. Thus $(s's_j, N_j) = 1$, which finishes the proof of the Lemma. □

We consider a simple example of Lemma 7.2.1. Let sequence V be as defined in form (6.24), for $r = 2$, so $N = pq$, where p and q are different odd primes. Then from Lemma 7.2.1

$$P_V(j) = \begin{cases} 1-p & , if\ p \mid j \\ 1-q & , if\ q \mid j \\ +1 & , otherwise \end{cases} \quad , \ 1 \le j \le N-1. \tag{7.4}$$

Expression (7.4) is exactly the same as the form (6.26).

Generally, for $r \ge 2$, $N = p_1 p_2 \ldots p_r$, where p_i's are distinct odd primes, we have the following upper estimate for the periodic autocorrelation for V.

Lemma 7.2.2. *Let $N = p_1 p_2 \ldots p_r$, where $p_1 < p_2 < \cdots < p_r$ are distinct odd*

primes, r is finite. Let the sequence V of entries $\{0, \pm 1\}$ be as defined in form (6.24), then we have

1. $|P_V(i)| \leq (i, N)$;

2. $\sum_{i=1}^{N-1} P_V^2(i) \leq C \cdot \frac{N^2}{p_1}$, *where C is a constant only depending on r.*

Proof. For part *1*, if $(i, N) = 1$, then $(i, p_j) = 1$ for $j = 1, 2, \ldots, r$. From Lemma 3.2.5 and 7.2.1,

$$P_V(i) = \prod_{j=1}^{r} P_{\chi p_j}(i) = \pm 1 \, .$$

Now if $(i, N) = N_1 > 1$, then $(i, N/N_1) = 1$. Use the above result and Lemma 7.2.1,

$$|P_V(i)| = |P_{\chi_{N_1}}(0) \times P_{\chi_{\frac{N}{N_1}}}(i)| \leq |P_{\chi_{N_1}}(0)| \leq (i, N) \, .$$

So part *1* is true.

For part *2*, by Lemma 7.2.1,

$$\begin{aligned}
\sum_{i=1}^{N-1} P_V^2(i) &= \sum_{(i,N)=1} P_V^2(i) + \sum_{(i,N)>1} P_V^2(i) \\
&\leq \sum_{(i,N)=1} \prod_{j=1}^{r} P_{\chi p_j}^2(i) + \sum_{d|N} {\sum_{s=1}^{\frac{N}{d}}}' P_{\chi_d}^2(sd) \; P_{\chi_{N/d}}^2(sd) \\
&\leq \sum_{(i,N)=1} 1 + \sum_{d|N} d^2 \cdot \frac{N}{d} = \phi(N) + \sum_{d|N} N \cdot d \\
&\leq C_1 \cdot \frac{N^2}{p_1},
\end{aligned}$$

where $\phi(N)$ is the Euler function of N, and C_1 is a constant only depending on r. □

Before we can give an upper bound of the periodic autocorrelations of sequence v, we still need one more property.

Lemma 7.2.3. *Let* $\xi_N = e^{\frac{2\pi i}{N}}$, *suppose* $N = N_1 \times N_2 \cdots \times N_r$, *where* $(N_i, N_j) = 1$, *for any* $1 \leq i < j \leq r$, *then for any integer* k, *there exist integers* $k_1, k_2, \ldots, k_r$, *such that* $(k_i, N_i) = 1$, *and*

$$\xi_N^k = \prod_{i=1}^{r} \xi_{N_i}^{kk_i}$$

Proof. We will prove the lemma by the induction on r. When $r = 1$, the result is obviously true if we choose $k_1 = 1$. Suppose the result is correct for $r = s - 1$, where $s \geq 2$. Then for $r = s$, so $N = N_1 \times N_2 \cdots \times N_{s-1} \times N_s$, where $(N_i, N_j) = 1$, for any $1 \leq i < j \leq s$. Denote $N' = N_1 \times N_2 \cdots \times N_{s-1}$, so $(N', N_s) = 1$. Then there exist integers k' and k_s, such that

$$\begin{aligned} k_s N' + k' N_s = 1 \Rightarrow k \equiv k k_s N' + k k' N_s \pmod{N} \\ \Rightarrow \xi_N^k = \xi_{N'}^{kk'} \cdot \xi_{N_s}^{kk_s} \end{aligned}$$

by induction

$$\xi_{N'}^{kk'} = \prod_{i=1}^{s-1} \xi_{N_i}^{kk's_i}$$

where $(s_i, N_i) = 1$, for $1 \leq i \leq s - 1$. Now

$$k_s N' + k' N_s = 1 \Rightarrow (k', N') = 1 \Rightarrow (k', N_i) = 1 \text{ for } 1 \leq i \leq s - 1$$

Let $k_i = k' s_i$, for $1 \leq i \leq s - 1$. Similarly, $k_s N' + k' N_s = 1 \Rightarrow (k_s, N_s) = 1$, then we have the desired result. □

Lemma 7.2.4. *Suppose* $N = p_1 p_2 \ldots p_r$, *where* p_i*'s are distinct odd primes for* $i = 1, 2, \ldots, r$. *Let* χ_N *be the primitive character mod* N, $f(x)$ *be a polynomial of degree* k. *If for each* p_a, $1 \leq a \leq r$, *there is a factorization* $f(x) = b(x - x_1)^{d_1} \ldots (x - x_s)^{d_s}$

in $\overline{F}_{p_a}$, *where* $x_i \neq x_j$, *for* $i \neq j$ *with*

$$(p_a - 1, d_1, \ldots, d_s) = 1 \ ,$$

then

$$| \sum_{u<n\leq u+t} \chi_N(f(n)) \ | < 2k^r N^{\frac{1}{2}} \log(N)$$

where u *and* t *are integers and* $t > 0$.

Proof. From Lemma 3 in [37] (Page 374), we know that for each p_j, $1 \leq j \leq r$,

$$\left| \sum_{x \in F_{p_j}} \chi_{p_j}(f(x)) e^{\frac{2b\pi}{p_j} i} \right| \leq k p_j^{\frac{1}{2}} \tag{7.5}$$

for any $b \in \mathbb{Z}$. At the same time, one form of the Erdős-Turán inequality ([37] Lemma 4, Page 375) is presented as following

If $m \in \mathbb{N}$, the function $g(x)$: $\mathbb{Z} \rightarrow \mathbb{C}$ is periodic with period m, and u and t are real numbers with $0 \leq t < m$, then

$$| \sum_{u<n\leq u+t} g(n) \ | \leq \frac{t+1}{m} | \sum_{n=1}^{m} g(n) \ | + \sum_{1\leq |h| \leq m/2} |h|^{-1} | \sum_{n=1}^{m} g(n) e^{\frac{hn2\pi}{m} i} \ | \tag{7.6}$$

Now apply equation (7.6) with N and $\chi_N(f(n))$ in place of m and $g(n)$ respectively,

and use Lemma 7.2.3 and equation (7.5):

$$\left| \sum_{u<n\leq u+t} \chi_N(f(n)) \right|$$

$$\leq \frac{t+1}{N} \left| \sum_{n=1}^{N} \chi_N(f(n)) \right| + \sum_{1\leq|h|\leq N/2} |h|^{-1} \left| \sum_{n=1}^{N} \chi_N(f(n)) e^{\frac{hn2\pi}{N} i} \right| \tag{7.7}$$

$$= \frac{t+1}{N} \prod_{j=1}^{r} \left| \sum_{n=1}^{p_j} \chi_{p_j}(f(n)) \right| + \sum_{1\leq|h|\leq N/2} |h|^{-1} \prod_{j=1}^{r} \left| \sum_{n=1}^{p_j} \chi_{p_j}(f(n)) e^{\frac{hk_j n2\pi}{p_j} i} \right|$$

and $$\frac{t+1}{N} \prod_{j=1}^{r} \left| \sum_{n=1}^{p_j} \chi_{p_j}(f(n)) \right| \leq 2 \times \frac{t+1}{N} \prod_{j=1}^{r} p_j^{\frac{1}{2}} \leq 2 \times N^{\frac{1}{2}}.$$

The last inequality follows from equation (7.5).

The calculations above follow from the fact that k_j's are integers such that $(k_j, p_j) = 1$.

For the second item in (7.7), from equation (7.5), we have

$$\sum_{1\leq|h|\leq N/2} |h|^{-1} \prod_{j=1}^{r} \left| \sum_{n=1}^{p_j} \chi_{p_j}(f(n)) e^{\frac{hk_j n2\pi}{p_j} i} \right| \leq 2 \times \sum_{1\leq|h|\leq N/2} |h|^{-1} N^{\frac{1}{2}}$$

Again the last inequality follows from equation (7.5). Therefore we obtain

$$|\sum_{u<n\leq u+t} \chi_N(f(n))|$$

$$\leq \frac{t+1}{N} \prod_{j=1}^{r} \left| \sum_{n=1}^{p_j} \chi_{p_j}(f(n)) \right| + \sum_{1\leq|h|\leq N/2} |h|^{-1} \prod_{j=1}^{r} \left| \sum_{n=1}^{p_j} \chi_{p_j}(f(n)) e^{\frac{hk_j n 2\pi}{p_j} i} \right|$$

$$\leq k^r N^{\frac{1}{2}} + k^r N^{\frac{1}{2}} \sum_{1\leq|h|\leq N/2} |h|^{-1} < 2k^r N^{\frac{1}{2}} \log(N)$$

which is the desired result. □

Remark 1. *In the hypothesis of Lemma 7.2.4, for each p_j, $1 \leq j \leq r$, $f(x)$ can't be a perfect square over $\overline{F}_{p_j}$. As an application of Lemma 7.2.4, the following property gives a general estimate for all $f(x)$ of degree 2.*

Property 7.2.5. *Suppose $N = p_1 p_2 \dots p_r$, where p_i's are distinct odd primes and r is finite. Let χ be the primitive character mod N. Let u and t be integers such that $0 \leq t < N$, then for any $1 \leq k_1 \neq k_2 \leq N-1$, we have*

1. $|\sum_{u<n\leq u+t} \chi_N(n+k_1)\chi_N(n+k_2)| \leq 2 \cdot max\{\lfloor \frac{td}{N} \rfloor, 2^r \sqrt{N/d} \log(N/d)\}$

2. $|\sum_{u<n\leq u+t} (-1)^n \chi_N(n+k_1)\chi_N(n+k_2)| \leq 4 \cdot max\{\lfloor \frac{td}{N} \rfloor, 2^r \sqrt{N/d} \log(N/d)\}$

where $d = (k_2 - k_1, N)$.

Proof. We will prove part 1 first. For $d = (k_2 - k_1, N)$, write $N = ds$, thus $(k_2 -$

$k_1, s) = 1$. Then

$$|\sum_{u<n\leq u+t} \chi_N(n+k_1)\cdot\chi_N(n+k_2)|$$

$$=|\sum_{u+k_1<n\leq u+t+k_1} \chi_N(n)\cdot\chi_N(n+k_2-k_1)|$$

$$=|\sum_{u'<n\leq u'+t} \chi_d^2(n)\cdot\chi_s(n)\cdot\chi_s(n+k_2-k_1)|,$$

where $u' = u + k_1$. Let $m = \lfloor\frac{t}{s}\rfloor = \lfloor\frac{td}{N}\rfloor$. Then from Lemma 7.2.4, we have

$$|\sum_{u'<n\leq u'+t} \chi_N(n)\cdot\chi_N(n+k_2-k_1)|$$

$$\leq \sum_{j=1}^{m} |P_{\chi s}(k_2-k_1)| + |\sum_{u'+ms<n\leq u'+t} \chi_s(n)\cdot\chi_s(n+k_2-k_1)|$$

$$\leq m + 2^r\cdot\sqrt{s}\cdot\log(s) \leq 2\cdot max\{\lfloor\frac{td}{N}\rfloor, 2^r\cdot\sqrt{N/d}\cdot\log(N/d)\},$$

where the second inequality follows from the fact that $(k_2-k_1, s) = 1$, thus $P_{\chi s}(k_2-k_1) = -1$, and Lemma 7.2.4.

For part 2,

$$\left|\sum_{u<n\leq u+t}(-1)^n\chi_N(n+k_1)\chi_N(n+k_2)\right|$$

$$\leq | \sum_{\lfloor \frac{u}{2} \rfloor < n \leq \lfloor \frac{u+t}{2} \rfloor} (-1)^{2n} \chi_N(2n+k_1)\chi_N(2n+k_2) \tag{7.8}$$

$$+ \sum_{\lfloor \frac{u}{2} \rfloor < n \leq \lfloor \frac{u+t}{2} \rfloor} (-1)^{2n-1} \chi_N(2n-1+k_1)\chi_N(2n-1+k_2) \; | + 2$$

$$\leq | \sum_{\lfloor \frac{u}{2} \rfloor < n \leq \lfloor \frac{u+t}{2} \rfloor} \chi_N(2n+k_1)\chi_N(2n+k_2) \; |$$

$$+ | \sum_{\lfloor \frac{u}{2} \rfloor < n \leq \lfloor \frac{u+t}{2} \rfloor} \chi_N(2n-1+k_1)\chi_N(2n-1+k_2) \; | + 2$$

For the first item in expression (7.8),

$$| \sum_{\lfloor \frac{u}{2} \rfloor < n \leq \lfloor \frac{u+t}{2} \rfloor} \chi_N(2n+k_1)\chi_N(2n+k_2)| \tag{7.9}$$

$$= | \sum_{\lfloor \frac{u}{2} \rfloor < n \leq \lfloor \frac{u+t}{2} \rfloor} \chi_N(n+2^{-1}k_1)\chi_N(n+2^{-1}k_2)|$$

$$\leq 2 \cdot max \left\{ \lfloor \frac{td}{N} \rfloor, 2^r \sqrt{N/d} \; \log(N/d) \right\}$$

from part 1. Similarly, from part 1, the second item in expression (7.8),

$$| \sum_{\lfloor \frac{u}{2} \rfloor < n \leq \lfloor \frac{u+t}{2} \rfloor} \chi_N(2n-1+k_1)\chi_N(2n-1+k_2)| \tag{7.10}$$

$$= | \sum_{\lfloor \frac{u}{2} \rfloor < n \leq \lfloor \frac{u+t}{2} \rfloor} \chi_N(n+2^{-1}(k_1-1))\chi_N(n+2^{-1}(k_2-1))|$$

$$\leq 2 \cdot max \left\{ \lfloor \frac{td}{N} \rfloor, 2^r \sqrt{N/d} \; \log(N/d) \right\}$$

Plug the result from expressions (7.9) and (7.10) into (7.8). Then we get the result we want to prove. □

Based on Property 7.2.5, we will give an estimate of the upper bound of the $P_v(i)$, where the sequence v is as defined in Definition 7.1.1.

Lemma 7.2.6. *Suppose $N = p_1 p_2 \dots p_r$, where $p_1 < p_2 < \cdots < p_r$ are distinct odd primes and $r \geq 2$ is finite. Let ω be the function as defined in Definition 3.1.10. Then for the sequence v as defined in Definition 7.1.1, for each $1 \leq i \leq N-1$, given condition (7.3) holds, we have*

$$\frac{|P_v(i)|}{C} \leq \begin{cases} \sqrt{N/(p_1 p_2)}\ \log(\frac{N}{p_1 p_2}) & , \ if \ \ d = 1\ ; \\ d/p_1 & , \ if \ \ \omega(d) = r-1\ ; \\ max\left\{d, \sqrt{N/d}\ \log(\frac{N}{d})\right\} & , \ otherwise\ ; \end{cases} \tag{7.11}$$

where $d = (i, N)$, and C is a constant only depending on r.

Proof. For any $1 \leq i \leq N-1$, $P_v(i) = \sum_{j=0}^{N-1} v_j v_{j+i}$, while from the definition

$$v_j v_{j+i} \neq 0 \Leftrightarrow (j, N) = m_1 > 1, \ \text{ and } \ (j+i, N) = m_2 > 1.$$

Suppose $v_j v_{j+i} \neq 0$, and put $(m_1, m_2) = d_1$. Then $m_1 = d_1 d_2$, $m_2 = d_1 d_3$, and $d_1 d_2 d_3 | N$. In the following proof, we put $D = d_1 d_2 d_3$. Write $j = k d_1 d_2$, $j + i = s d_1 d_3$. Then

$$k d_1 d_2 + i = s d_1 d_3, \quad \text{and } \ (k, \frac{N}{d_1 d_2}) = (s, \frac{N}{d_1 d_3}) = 1. \tag{7.12}$$

Actually, starting with equality (7.12), we can obtain a series of equalities as following

$$\begin{aligned}
(k+d_3)d_1d_2+i &= (s+d_2)d_1d_3 \pmod N,\\
(k+2d_3)d_1d_2+i &= (s+2d_2)d_1d_3 \pmod N,\\
&\cdot\\
(k+Md_3)d_1d_2+i &= (s+Md_2)d_1d_3 \pmod N.
\end{aligned} \tag{7.13}$$

where $M=\frac{N}{D}-1$. Note that all the values in (7.13) are taken modulo N.

Denote $(k+nd_3, N/d_1d_2) = g_1$, and $(s+nd_2, N/d_1d_3) = g_2$. Then all of the equalities above give us the following partial sum in P_v.

$$\begin{aligned}
&\sum_{n=0}^{M} v[\,(k+nd_3)d_1d_2\,]\cdot v[\,(s+nd_2)d_1d_3\,]\\
&= \sum_{\substack{n=0\\ g_1\cdot g_2>1}}^{M} v[\,(k+nd_3)d_1d_2\,]\cdot v[\,(s+nd_2)d_1d_3\,]\\
&\qquad + \sum_{\substack{n=0\\ g_1=g_2=1}}^{M} v[\,(k+nd_3)d_1d_2\,]\cdot v[\,(s+nd_2)d_1d_3\,]\\
&= \sum_{\substack{n=0\\ g_1\cdot g_2>1}}^{M} v[\,(k+nd_3)d_1d_2\,]\cdot v[\,(s+nd_2)d_1d_3\,]\\
&\qquad + \sum_{\substack{n=0\\ g_1=g_2=1}}^{M} \zeta_n\cdot\chi_{\frac{N}{d_1d_2}}(k+nd_3)\cdot\chi_{\frac{N}{d_1d_3}}(s+nd_2)
\end{aligned} \tag{7.14}$$

where $\zeta_n = (\chi_{d_1d_2}(-1))^{(k+nd_3)}\cdot(\chi_{d_1d_3}(-1))^{(s+nd_2)}$ from Definition 7.1.1.

Therefore,

$$\sum_{n=0}^{M} \zeta_n \cdot \chi_{\frac{N}{d_1 d_2}}(k+nd_3) \cdot \chi_{\frac{N}{d_1 d_3}}(s+nd_2) \tag{7.15}$$

$$= \sum_{n=0}^{M} \zeta_n \cdot \chi_{N/D}(k+nd_3) \cdot \chi_{d_3}(k+nd_3) \cdot \chi_{N/D}(s+nd_2) \cdot \chi_{d_2}(s+nd_2)$$

$$= \sum_{n=0}^{M} \zeta_n \cdot \chi_{N/D}(k+nd_3) \cdot \chi_{N/D}(s+nd_2) \cdot \chi_{d_3}(k) \cdot \chi_{d_2}(s)$$

$$= \chi_{d_3}(k) \cdot \chi_{d_2}(s) \cdot \chi_{N/D}(d_3) \cdot \chi_{N/D}(d_2) \cdot$$

$$\left[\sum_{n=0}^{M} \zeta_n \cdot \chi_{N/D}(n+kd_3^{-1}) \cdot \chi_{N/D}(n+sd_2^{-1}) \right]$$

where $d_2 d_2^{-1} \equiv d_3 d_3^{-1} \equiv 1 \pmod{N/D}$. So we have

$$\left| \sum_{\substack{n=0 \\ g_1=g_2=1}}^{M} \zeta_n \cdot \chi_{\frac{N}{d_1 d_2}}(k+nd_3) \cdot \chi_{\frac{N}{d_1 d_3}}(s+nd_2) \right| \tag{7.16}$$

$$= \left| \sum_{n=0}^{M} \zeta_n \cdot \chi_{N/D}(n+kd_3^{-1}) \cdot \chi_{N/D}(n+sd_2^{-1}) \right|$$

Now we take a closer look at the ζ_n values. From the Definition 7.1.1,

1. $\zeta_n = 1$, if $\chi_{d_1 d_2}(-1) = \chi_{d_1 d_3}(-1) = 1$;

2. $\zeta_n = (-1)^{(kn+sn)}$, if $\chi_{d_1 d_2}(-1) = \chi_{d_1 d_3}(-1) = -1$;

3. $\zeta_n = (-1)^{kn}$, if $\chi_{d_1 d_2}(-1) = -1$, $\chi_{d_1 d_3}(-1) = 1$;

4. $\zeta_n = (-1)^{sn}$, if $\chi_{d_1 d_2}(-1) = 1$, $\chi_{d_1 d_3}(-1) = -1$.

where $k_n \equiv k + nd_3 \pmod{\frac{N}{d_1 d_2}}$, $s_n \equiv s + nd_2 \pmod{\frac{N}{d_1 d_3}}$.

Now we study each case separately. In the following cases, we let n_1 be the first number that $k + n_1 d_3 \geq \frac{N}{d_1 d_2}$, and n_2 be the first number that $s + n_2 d_2 \geq \frac{N}{d_1 d_3}$.

For case 1,

$$\begin{aligned} & |\sum_{n=0}^{M} \zeta_n \cdot \chi_{N/D}(n + kd_3^{-1}) \cdot \chi_{N/D}(n + sd_2^{-1})| \qquad (7.17) \\ = & |\sum_{n=0}^{M} \chi_{N/D}(n + kd_3^{-1}) \cdot \chi_{N/D}(n + sd_2^{-1})| \\ = & |P_{\chi_{N/D}}(sd_2^{-1} - kd_3^{-1})| \end{aligned}$$

For case 2, if $n_1 = n_2$, then we still have

$$|\sum_{n=0}^{M} \zeta_n \cdot \chi_{N/D}(n + kd_3^{-1}) \cdot \chi_{N/D}(n + sd_2^{-1})| = |P_{\chi_{N/D}}(sd_2^{-1} - kd_3^{-1})|$$

So suppose $n_1 \neq n_2$. Without loss, suppose $n_1 < n_2$, noting that all of d_2, d_3, $\frac{N}{d_1 d_2}$ and $\frac{N}{d_1 d_3}$ are odd. Then we have

$$|\sum_{n=0}^{M} \zeta_n \cdot \chi_{N/D}(n + kd_3^{-1}) \cdot \chi_{N/D}(n + sd_2^{-1})| \qquad (7.18)$$

$$\leq 2 \, |\sum_{n_1 - 1 < n \leq n_2 - 1} \chi_{N/D}(n + kd_3^{-1}) \cdot \chi_{N/D}(n + sd_2^{-1})|$$

$$+ |P_{\chi_{N/D}}(sd_2^{-1} - kd_3^{-1})|$$

Since cases 3 are 4 are similar, we consider case 3. Then $\zeta_n = (-1)^{kn}$, we have

$$|\sum_{n=0}^{M} \zeta_n \cdot \chi_{N/D}(n + kd_3^{-1}) \cdot \chi_{N/D}(n + sd_2^{-1})|$$

$$= |\sum_{0<n\leq n_1-1} (-1)^n \cdot \chi_{N/D}(n + kd_3^{-1}) \cdot \chi_{N/D}(n + sd_2^{-1})$$

$$- \sum_{n_1-1<n\leq M} (-1)^n \cdot \chi_{N/D}(n + kd_3^{-1}) \cdot \chi_{N/D}(n + sd_2^{-1})|$$

$$\leq |\sum_{0<n\leq n_1-1} (-1)^n \cdot \chi_{N/D}(n + kd_3^{-1}) \cdot \chi_{N/D}(n + sd_2^{-1})|$$

$$+ |\sum_{n_1-1<n\leq M} (-1)^n \cdot \chi_{N/D}(n + kd_3^{-1}) \cdot \chi_{N/D}(n + sd_2^{-1})| \qquad (7.19)$$

If $N/D = 1$, then all of the expressions (7.17), (7.18) and (7.19) are $o(1)$. So suppose $N/D > 1$.

Put $(i, N/D) = i_1$, and $(sd_2^{-1} - kd_3^{-1}, N/D) = i_2$. Then we will prove that $i_1 = i_2$.

Suppose $d_2 d_2^{-1} = k_1 \cdot \frac{N}{D} + 1$, and $d_3 d_3^{-1} = k_2 \cdot \frac{N}{D} + 1$ for some integers k_1 and k_2. Then from (7.12), we have

$$\begin{aligned}(sd_2^{-1} - kd_3^{-1})D &= sd_1d_3(k_1 \cdot \frac{N}{D} + 1) - kd_1d_2(k_2 \cdot \frac{N}{D} + 1) \\ &= \frac{N}{D} \cdot (sk_1d_1d_3 - kk_2d_1d_2) + (sd_1d_3 - kd_1d_2) \\ &= \frac{N}{D} \cdot (sk_1d_1d_3 - kk_2d_1d_2) + i\end{aligned}$$

$$(i, \frac{N}{D}) = d \Rightarrow i_1 \mid [\, \frac{N}{D} \cdot (sk_1d_1d_3 - kk_2d_1d_2) + i \,]$$
$$\Rightarrow i_1 \mid (sd_2^{-1} - kd_3^{-1})D \Rightarrow i_1 \mid (sd_2^{-1} - kd_3^{-1}) \qquad \text{since } (i_1, D) = 1$$
$$\Rightarrow i_1 \mid \frac{N}{D} \Rightarrow i_1 \mid i_2.$$

On the other hand,

$$i_2 \mid (sd_2^{-1} - kd_3^{-1}) \Rightarrow i_2 \mid [\, \frac{N}{D}(sk_1d_1d_3 - kk_2d_1d_2) + i \,]$$
$$i_2 \mid \frac{N}{D} \Rightarrow i_2 \mid i_1.$$

So we have $(i, N/D) = (sd_2^{-1} - kd_3^{-1}, N/D)$.

Put $(i, N/D) = i_D$, so $(sd_2^{-1} - kd_3^{-1}, N/D) = i_D$.

By lemma 3.2.5 and 7.2.1, expressions (7.17) satisfies

$$\left| P\chi_{N/D}(sd_2^{-1} - kd_3^{-1}) \right| \leq i_D \tag{7.20}$$

From Property 7.2.5, equations (7.18) and (7.19) satisfy

$$\left| \sum_{n=0}^{M} \zeta n \cdot \chi_{N/D}(n + kd_3^{-1}) \cdot \chi_{N/D}(n + sd_2^{-1}) \right| \tag{7.21}$$
$$\leq 4 \cdot max \left\{ i_D, 2^r \sqrt{\frac{N}{D \cdot i_D}} \log \left(\frac{N}{D \cdot i_D} \right) \right\}$$

If $(i, N) = d = 1$, then $i_D = 1$. We want to show that $\omega(D) \geq 2$. If $\omega(D) = 1$, then $d_1 = p_j$ for some $1 \leq j \leq r$, $d_2 = d_3 = 1$. Then expression (7.12) becomes

$$kp_j + i = sp_j \;\Rightarrow\; p_j \mid i \Rightarrow\; d \geq p_j$$

which contradicts to the hypothesis that $d = 1$.

If $d = i_D = 1$, and $\omega(D) \geq 2$, then expression (7.21) satisfies

$$\left| \sum_{n=0}^{M} \zeta_n \cdot \chi_{N/D}(n + kd_3^{-1}) \cdot \chi_{N/D}(n + sd_2^{-1}) \right| \leq 2^{r-2} \sqrt{\frac{N}{p_1 p_2}} \cdot \log\left(\frac{N}{p_1 p_2}\right)$$

And $d = 1$ implies expression (7.20)

$$\left| P_{\chi_{N/D}}(sd_2^{-1} - kd_3^{-1}) \right| = 1.$$

So we have proved that when $d = 1$,

$$\left| \sum_{\substack{n=0 \\ g_1 = g_2 = 1}}^{M} \zeta_n \cdot \chi_{\frac{N}{d_1 d_2}}(k + nd_3) \cdot \chi_{\frac{N}{d_1 d_3}}(s + nd_2) \right| < 1 + 2^{r-1} \sqrt{\frac{N}{p_1 p_2}} \log\left(\frac{N}{p_1 p_2}\right)$$

Next we want to show that $\omega(i_D) \leq r - 2$. If $\omega(i_D) = r - 1$, then $i_D = N/p_j$, for some $1 \leq j \leq r$, $d_1 = p_j$ and $d_2 = d_3 = 1$. Then equation (7.12) becomes

$$kp_j + i = sp_j \;\Rightarrow\; p_j \mid i \Rightarrow\; N \mid i\,.$$

This contradicts to the hypothesis that $i < N$. Thus $\omega(i_D) \leq r - 2$.

For $d = (i, N)$, suppose $\omega(d) = r - 1$. Then from the above statement we have just proved,

$$i_D = (i, \frac{N}{D}) \leq \frac{(i, N)}{p_1} \leq \frac{d}{p_1}\,.$$

Thus

$$\left| P_{\chi_{N/D}}\left(sd_2^{-1} - kd_3^{-1}\right) \right| = \left(sd_2^{-1} - kd_3^{-1}, N/D\right) = i_D \leq d/p_1\,.$$

When $\omega(d) = r - 1$,

$$(i, N/D) = i_D \geq \frac{N}{D \cdot i_D} \geq \sqrt{\frac{N}{D \cdot i_D}} \cdot \log\left(\frac{N}{D \cdot i_D}\right)$$

when N is large. So expression (7.21) satisfies

$$\left| \sum_{n=0}^{M} \zeta n \cdot \chi_{N/D}(n + kd_3^{-1}) \cdot \chi_{N/D}(n + sd_2^{-1}) \right|$$

$$\leq 4 \cdot max \left\{ i_D,\ 2^r \sqrt{\frac{N}{D \cdot i_D}} \log\left(\frac{N}{D \cdot i_D}\right) \right\}$$
$$\leq 4 \cdot i_D \leq 4 \cdot \frac{d}{p_1}.$$

Finally, for $1 \leq \omega(d) \leq r - 2$, because $(i, \frac{N}{D}) = i_D \leq d = (i, N)$, so equation (7.21) satisfies

$$\left| \sum_{n=0}^{M} \zeta n \cdot \chi_{N/D}(n + kd_3^{-1}) \cdot \chi_{N/D}(n + sd_2^{-1}) \right|$$

$$\leq 4 \cdot max \left\{ i_D, 2^r \sqrt{\frac{N}{d \cdot i_D}} \log\left(\frac{N}{D \cdot i_D}\right) \right\} \qquad \text{by Property 7.2.5}$$

$$\leq 4 \cdot max \left\{ d, 2^r \sqrt{\frac{N}{d}} \log\left(\frac{N}{d}\right) \right\}$$

Now for the first term of expression (7.14).

$$\sum_{\substack{n=0 \\ g_1 g_2 > 1}}^{M} v[\ (k + nd_3)d_1 d_2\ ] \cdot v[\ (s + nd_2)d_1 d_3\ ] \neq 0$$

It means that there exist another set of factors d_1', d_2' and d_3', with $d_1'd_2'd_3' \mid N$ such that

$$k'd_1'd_2' + i = s'd_1'd_3'$$

where $(k', \frac{N}{d_1'd_2'}) = (s', \frac{N}{d_1'd_3'}) = 1$. Then we can set up another series of equalities similar to (7.13) and obtain the same upper bound as before. Repeating the previous steps, we could come up with the following

$$|P_v(i)| \leq \sum_{1<d|N} |\sum_{n=0}^{M} \zeta_n \cdot \chi_{\frac{N}{d}}(n+k_d) \cdot \chi_{\frac{N}{d}}(n+s_d)|$$

where $\zeta_n = \{+1, -1\}$ depending on n values, k_d and s_d are some integers depending on the values of d with $(s_dk_d, \frac{N}{d}) = 1$ and $(s_d - k_d, \frac{N}{d}) = (i, \frac{N}{d})$.

Noting that

$$d(N) = \sum_{d|N} 1$$

is a finite number only depending on r value, by the discussion above, we have proved the lemma. □

Now we are ready to prove the following lemma:

Lemma 7.2.7. *Suppose $N = p_1p_2 \ldots p_r$, where $p_1 < p_2 < \cdots < p_r$'s are distinct odd primes and r is finite. Let z be the binary sequences of length N as defined in expression (7.2). Then*

$$\sum_{i=1}^{N-1} P_z^2(i) \leq C \times N^2/p_1 \,,$$

where C is a constant only depending on r.

Proof. Let the binary sequence V be as defined in form (6.24). Then $z_j = V_j + v_j$, where sequence v is as defined in definition 7.1.1. So from Property 3.2.13, we know

that

$$\sum_{i=1}^{N-1} P_z^2(i) = A + B + C + D + E + F \tag{7.22}$$

In expression (7.22), we have separated the summands into six groups. In the following, we will show that the absolute value of every sum from the same group has the same upper bound. To simplify the notation, it should be understood that all of the following statements are valid when p_1 and p_2's are **large enough**. For group A, from Lemma 7.2.2

$$\sum_{i=1}^{N-1} P_V^2(i) \leq C_1 \times N^2/p_1 \ ,$$

where C_1 is a constant only depending on r.

For group B, we denote $i_N = (i, N)$. From Lemma 7.2.6, we have

$$\sum_{i=1}^{N-1} P_v^2(i) = \sum_{i_N=1} P_v^2(i) + \sum_{\omega(i_N)=r-1} P_v^2(i) + \sum_{1\leq\omega(i_N)\leq r-2} P_v^2(i).$$

From Lemma 7.2.6,

$$\sum_{i_N=1} P_v^2(i) \leq C_{21} \times N \times \frac{N}{p_1 p_2} \log^2(\frac{N}{p_1 p_2}) \leq C_{21} \times \frac{N^2}{p_1}, \tag{7.23}$$

where C_{21} is a constant only depending on r.

$$\sum_{\omega(i_N)=r-1} P_v^2(i) = \sum_{j=1}^{r} \sum_{s=1}^{p_j-1} P_v^2(s\frac{N}{p_j}) \leq \sum_{j=1}^{r} \frac{N^2}{p_1^2 p_j} \leq r \times \frac{N^2}{p_1} \tag{7.24}$$

Note that

$$\sum_{\omega(i_N)\le r-2} P_v^2(i) = \sum_{\substack{d|N \\ \omega(d)\le r-2}} {\sum_{m=1}^{N/d}}' P_v^2(md)$$

$$\le \sum_{\substack{\omega(d)\le r-2 \\ d\ge\sqrt{N/d}\,\log(N/d)}} \frac{N}{d}\times d^2 + \sum_{\substack{\omega(d)\le r-2 \\ d<\sqrt{N/d}\,\log(N/d)}} \frac{N^2}{d^2}\times \log^2(N/d)$$

$$\le C_{22}\times\frac{N^2}{p_1}, \tag{7.25}$$

where C_{22} is a constant only depending on r.

Combine the results from equations (7.23), (7.24) and (7.25), we have

$$\sum_{i=1}^{N-1} P_v^2(i) \le C_2\times\frac{N^2}{p_1},$$

where $C_2 = max\{C_{21}, C_{22}, r\}$.

For groups C and D, every term in this group could be written as

$$\sum_{i=1}^{N-1} P_V(i) \sum_{m=0}^{N-1} v_m\xi_m, \quad \text{where} \quad \xi_m\in\{+1,-1\}.$$

Lemma 3.2.5, 3.2.8, 7.2.1 and Lemma 7.2.2 give

$$|\sum_{i=1}^{N-1} P_V(i) \sum_{m=0}^{N-1} v_m\zeta_m| \le rN/p_1\times\sum_{i=1}^{N-1}|P_V(i)|$$

$$= rN/p_1 \times [\sum_{i=1}^{N-1}{}' |P_V(i)| + \sum_{\substack{i=1 \\ (i,N)>1}}^{N-1} |P_V(i)| \ ]$$

$$< rN/p_1 \times [N + \sum_{d|N} \sum_{k=1}^{N/d}{}' |P_V(kd)|]$$

$$\leq rN/p_1 \times [N + \sum_{d|N} N/d \times d]$$

$$\leq C_3 \times N/p_1 \times N$$

$$= C_3 \times N^2/p_1 \ ,$$

where C_3 is a constant only depending on r. Again, the inequality second to the last follows from the fact that $d(N)$ is a finite number.

Now we consider the terms in group F.

$$\sum_{i=1}^{N-1} P^2_{V,v}(i) = \sum_{i=1}^{N-1} \sum_{j=0}^{N-1} \sum_{m=0}^{N-1} V_j v_{j+i} V_m v_{m+i}$$

$$= \sum_{i=1}^{N-1} \sum_{j=0}^{N-1} V_j v_{j+i} \sum_{m=0}^{N-1} V_{N-m} v_{N-m-i} \tag{7.26}$$

$$= \sum_{i=1}^{N-1} \sum_{j=0}^{N-1} \sum_{m=0}^{N-1} V_j v_{j+i} v_m V_{m+i} = \sum_{i=1}^{N-1} P_{V,v}(i) P_{v,V}(i)$$

The third equality follow from Lemma 6.3.2. Similarly we can prove that

$$\sum_{i=1}^{N-1} P^2_{v,V}(i) = \sum_{i=1}^{N-1} P_{V,v}(i) P_{v,V}(i)$$

Therefore for every term in group F, it is enough to estimate the upper bound of $\sum_{i=1}^{N-1} P_{V,v}(i)P_{v,V}(i)$.

$$\sum_{i=1}^{N-1} P_{V,v}(i)P_{v,V}(i) = \sum_{i=1}^{N-1}\sum_{j=0}^{N-1}\sum_{m=0}^{N-1} V_j v_{j+i} v_m V_{m+i}$$

$$= \sum_{i=1}^{N-1}\sum_{j=0}^{N-1}\sum_{m=0}^{N-1} v_j v_m V_{j-i} V_{m+i}$$

$$= \chi_N(-1) \sum_{j=0}^{N-1}\sum_{m=0}^{N-1} v_j v_m \Big(\sum_{i=1}^{N-1} V_{j-i} V_{-m-i}\Big)$$

$$= \chi_N(-1) \sum_{j=0}^{N-1}\sum_{m=0}^{N-1} v_j v_m P_V(m+j)$$

Also

$$\Big|\sum_{j=0}^{N-1}\sum_{m=0}^{N-1} v_j v_m P_V(m+j)\Big|$$

$$= \Big|\sum_{s=0}^{N-1}\sum_{j=0}^{N-1} v_j v_{s-j} P_V(s)\Big|$$

$$\leq \Big|\sum_{\substack{j=0\\ s=0}}^{N-1} v_j^2 P_V(0)\Big| + \Big|\sum_{\substack{s=1\\ (s,N)>1}}^{N-1} P_v(s)P_V(s)\Big| + \Big|{\sum_{s=1}^{N}}' P_v(s)(-1)^r\Big|$$

From Lemma 3.2.8,

$$|\sum_{j=0}^{N-1} v_j^2 P_V(0)| = N|\sum_{j=0}^{N-1} v_j^2| \leq rN \times N/p_1 \leq r \times N^2/p_1 \tag{7.27}$$

In the proof of Lemma 7.2.6, we know that when $(s, N) = 1$,

$$|P_v(s)| \leq 2^r \sqrt{\frac{N}{p_1 p_2}} \log(\frac{N}{p_1 p_2}) .$$

Then when $r \geq 2$,

$$|\sum_{s=1}^{N}{}' P_v(s)| \leq \sum_{s=1}^{N}{}' |P_v(s)| < N \times 2^r \sqrt{\frac{N}{p_1 p_2}} \log(\frac{N}{p_1 p_2}) \leq 2^r \times N^2/p_1 \tag{7.28}$$

We will have to be more careful in estimating $|\sum_{(s,N)>1}^{N-1} P_v(s)P_V(s)|$. We write

$$|\sum_{\substack{s=1 \\ (s,N)>1}}^{N-1} P_v(s)P_V(s)\ | \leq |\sum_{\omega((s,N))=r-1} P_v(s)P_V(s)\ | + |\sum_{\omega((s,N))\leq r-2} P_v(s)P_V(s)\ | \tag{7.29}$$

For the first item of equation (7.29),

$$|\sum_{\omega((s,N))=r-1} P_v(s)P_V(s)\ | = |\sum_{k=1}^{r}\sum_{m=1}^{p_k-1} P_v(mN/p_k)P_V(mN/p_k)\ | \tag{7.30}$$

$$\leq \sum_{k=1}^{r}\sum_{m=1}^{p_k-1} |P_v(mN/p_k)\ | \times |P_V(mN/p_k)\ | \leq \sum_{k=1}^{r}\sum_{m=1}^{p_k-1} \frac{N}{p_1 p_k} \times \frac{N}{p_k}$$

$$< \sum_{k=1}^{r} N^2/(p_1 p_k) < N^2/p_1$$

Now for the second item of equation (7.29),

$$
\begin{aligned}
&|\sum_{\omega((s,N))\le r-2} P_v(s)P_V(s)| \qquad (7.31)\\
&= |\sum_{\substack{d|N\\ \omega(d)\le r-2}} {\sum_{m=1}^{N/d}}' P_v(md)P_V(md)|\\
&\le \sum_{\substack{d|N\\ \omega(d)\le r-2}} {\sum_{m=1}^{N/d}}' |P_v(md)||P_V(md)|\\
&\le \sum_{d\ge\sqrt{N/d}\,\log(\frac{N}{d})} \frac{N}{d}\times d^2 + \sum_{d<\sqrt{N/d}\,\log(\frac{N}{d})} d\times\sqrt{\frac{N^3}{d^3}}\times\log(\frac{N}{d}) \le C_{31}\times\frac{N^2}{p_1},
\end{aligned}
$$

here C_{31} is a constant only depending on r .

$$d(N)=\sum_{d|N}1 \text{ is finite}$$

Now equations (7.27) and (7.28),(7.30) and (7.31) give us

$$|\sum_{i=1}^{N-1}\sum_{j=0}^{N-1}\sum_{m=0}^{N-1} V_jv_{j+i}v_mV_{m+i}| = |\sum_{j=0}^{N-1}\sum_{m=0}^{N-1} v_jv_mP_V(m+j)| \le C_3\times\frac{N^2}{p_1},$$

where C_3 is a constant only depending on r .

Finally, for the items in group E, we first consider

$$\sum_{i=1}^{N-1} P_v(i)P_{v,V}(i) = \sum_{i=1}^{N-1} P_v(i)\sum_{j=0}^{N-1} v_jV_{j+i}.$$

We will use a similar method to the proof for Lemma 7.2.6 to give an upper estimate

of $\sum_{j=0}^{N-1} v_j V_{j+i}$.

From Lemma 3.2.8 and 7.2.6, we have

$$v_j V_{j+i} \neq 0 \Leftrightarrow (j, N) = d > 1 \text{ and } (j+i, N) = 1$$

Write $j = kd$, $j + i = s$. So , $(k, N/d) = (s, N) = 1$.

Again, we can set up the following series of equalities, noting that all the values are taken modulo N.

$$\begin{aligned} kd + i &= s \\ (k+1)d + i &= s + d \\ &\cdot \\ &\cdot \\ (k + (M-1))d + i &= s + (M-1)d \end{aligned} \tag{7.32}$$

where $M = \frac{N}{d}$.

The equation series in (7.32) give the following partial sum of $\sum_{j=0}^{N-1} v_j V_{j+i}$

$$\begin{aligned} &\sum_{m=0}^{M-1} \zeta_m \cdot \chi_{\frac{N}{d}}(m) \cdot \chi_N(md+i) \\ =&\chi_d(i) \cdot \chi_{\frac{N}{d}}(d) \cdot \left(\sum_{m=0}^{M-1} \zeta_m \cdot \chi_{\frac{N}{d}}(m) \cdot \chi_{\frac{N}{d}}(m + id^{-1}) \right) , \end{aligned}$$

where $\zeta_m = +1$, or $(-1)^{m'}$ with $m' \equiv m \pmod{N/d}$, $dd^{-1} \equiv 1 \pmod{N/d}$. Note that $(d, N/d) = 1$, so that $(id^{-1}, \frac{N}{d}) = (i, \frac{N}{d})$. Then from Lemma 7.2.6, if $\zeta_m = 1$,

for all $0 \leq m \leq M-1$, then

$$|\sum_{m=0}^{M-1} \zeta_m \chi_{\frac{N}{d}}(m)\chi_{\frac{N}{d}}(m+id^{-1})| = |P_{\chi_{\frac{N}{d}}}(id^{-1})| = (i, \frac{N}{d}) \leq i_N \tag{7.33}$$

If $\zeta_m = (-1)^{m'}$, where $m' \equiv m \pmod{N/d}$, then just repeating the process in expression (7.19) and using Lemma 7.2.5, we can obtain

$$\left| \sum_{m=0}^{M-1} (-1)^{m'} \cdot \chi_{\frac{N}{d}}(m) \cdot \chi_{\frac{N}{d}}(m+id^{-1}) \right| \tag{7.34}$$

$$\leq max\{i_D, 2^r \sqrt{\frac{N}{d \cdot i_D}} \log\left(\frac{N}{d \cdot i_D}\right)\}$$

where $i_D = (i, N/d)$.

For the remaining items in $\sum_{j=0}^{N-1} v_j V_{j+i}$, we use a similar argument to before. Since $d(i_N)$ is a finite number, we have

$$|\sum_{j=0}^{N-1} v_j V_{j+i}| \leq max\{i_D, \sqrt{\frac{N}{i_D}} \log\left(\frac{N}{i_D}\right)\} \tag{7.35}$$

By Lemma 7.2.6 and expression (7.35), we have

$$|\sum_{i=1}^{N-1} P_v(i)(\sum_{j=0}^{N-1} v_j V_{j+i})| \leq \sum_{i=1}^{N-1} |P_v(i)| \times |\sum_{j=0}^{N-1} v_j V_{j+i}|$$

$$= \sum_{(i,N)=1} |P_v(i)| \times |\sum_{j=0}^{N-1} v_j V_{j+i}| + \sum_{d|N} {\sum_{s=1}^{N/d}}' |P_v(sd)| \times |\sum_{j=0}^{N-1} v_j V_{j+sd}|$$

$$= \sum_{(i,N)=1} |P_v(i)| \times |\sum_{j=0}^{N-1} v_j V_{j+i}|$$

$$+ \Big(\sum_{\substack{d|N \\ d \geq \sqrt{N/d}\,\log(N/d)}} + \sum_{\substack{d|N \\ d < \sqrt{N/d}\,\log(N/d)}} \Big) \sum_{s=1}^{N/d}{}' |P_v(sd)| \times |\sum_{j=0}^{N-1} v_j V_{j+sd}|$$

$$\leq C_{41} \times \left(\sum_{k=1}^{r-1} \sum_{\substack{d|N \\ d \geq \sqrt{N/d}\,\log(N/d)}} Nd + \sum_{\substack{d|N \\ d < \sqrt{N/d}\,\log(N/d)}} \frac{N^2}{d^2} \log^2\left(\frac{N}{d}\right) \right)$$

$$+ \quad C_{41} \times \left(\sum_{(i,N)=1} \frac{N}{\sqrt{p_1 p_2}} \log^2(N) \right) \leq C_4 \times \frac{N^2}{p_1};$$

where C_4 is a constant only depending on r.

Using the similar method to expression (7.26), it can be shown that $P_v(i)P_{v,V}(i) = P_v(i)P_{V,v}(i)$, for any $i = 1, \ldots, N-1$. Then all of the inequalities above will give us the desired result. □

Now we are ready to prove Theorem 7.1.3.

7.3 Proof of Theorem 7.1.3

Proof. (Theorem 6.3.3 part (1))
We denote $\xi_N^j = e^{\frac{2\pi j}{N} i}$. For any sequence x of length N, let $x[\,\xi_N^j]$ be the Discrete Fourier Transform of x as defined in Definition 3.1. Recall the interpolation formula

as in Property 3.2.9,

$$x[\ -\xi_N^j] = \frac{2}{N} \sum_{k=0}^{N-1} \frac{\xi_N^k}{\xi_N^k + \xi_N^j} x[\ \xi_N^k] \tag{7.36}$$

Then for the sequence z as defined in Definition 7.1.1, we have

$$z[\ \xi_N^j] = V[\ \xi_N^j] + v[\ \xi_N^j]$$

Note that from Gauss sum,

$$|V[\ \xi_N^j]| = \begin{cases} \sqrt{N}, & if\ (j,N) = 1; \\ 0, & otherwise \end{cases} \tag{7.37}$$

Therefore, using the interpolation formula (7.36), we have

$$\begin{aligned} |V[\ -\xi_N^j]| &= \left| \frac{2}{N} \sum_{k=0}^{N-1} \frac{\xi_N^k}{\xi_N^k + \xi_N^j} V[\ \xi_N^k] \right| \\ &\leq \frac{2}{\sqrt{N}} \sum_{k=0}^{N-1} \left| \frac{\xi_N^k}{\xi_N^k + \xi_N^j} \right| \leq \sqrt{N} \log N \end{aligned} \tag{7.38}$$

Now consider $v[\ \xi_N^j]$. By definition

$$v[\ \xi_N^j] = \sum_{\substack{d|N \\ d \equiv N (\bmod 4)}} \chi_d[\ \xi_d^j] + \sum_{\substack{d|N \\ d \not\equiv N (\bmod 4)}} \chi_d[\ -\xi_d^j]$$

Using the Gauss sum ([38], page 233),

$$| \sum_{\substack{d|N \\ d \equiv N (\bmod 4)}} \chi_d[\ \xi_d^j]| \leq \sum_{\substack{d|N \\ d \equiv N (\bmod 4)}} |\chi_d[\ \xi_d^j]| \leq \sqrt{\frac{N}{p_1}}$$

As in (7.38), we have

$$|\sum_{\substack{d|N \\ d\not\equiv N(\bmod 4)}} \chi_d[-\xi_d^j]| \le \sum_{\substack{d|N \\ d\not\equiv N(\bmod 4)}} |\chi_d[-\xi_d^j]| \le C \times \sqrt{\frac{N}{p_1}} \log\left(\frac{N}{p_1}\right),$$

where C is a constant only depending on r.

Then we have obtained

$$v[\xi_N^j] \le C \times \sqrt{\frac{N}{p_1}} \log\left(\frac{N}{p_1}\right) \tag{7.39}$$

Note that

$$v[-\xi_N^j] = \sum_{\substack{d|N \\ d\equiv N(\bmod 4)}} \chi_d[-\xi_d^j] + \sum_{\substack{d|N \\ d\not\equiv N(\bmod 4)}} \chi_d[\xi_d^j]$$

Then using exactly the same method, we have

$$v[-\xi_N^j] \le C \times \sqrt{\frac{N}{p_1}} \log(\frac{N}{p_1}) \tag{7.40}$$

Let F be the merit factor of sequence x, $\widetilde{F}$ the merit factor of V. From Property 3.2.10,

$$1/F = \frac{1}{2N^3} \sum_{j=0}^{N-1} \left[|z[\xi_N^j]|^4 + |z[-\xi_N^j]|^4\right] - 1$$

$$1/\widetilde{F} = \frac{1}{2N^3} \sum_{j=0}^{N-1} \left[|V[\xi_N^j]|^4 + |V[-\xi_N^j]|^4\right] - 1$$

Let $1/F - 1/\widetilde{F} = G/2N^3$, want to show that

$$G/2N^3 \to 0 \quad \text{as } N \to \infty.$$

Put $a_j = v[\ \xi_N^j]$ and $b_j = v[\ -\xi_N^j]$. Then from Property 3.2.11,

$$|G| \leq \sum_{j=0}^{N-1} [\ |a_j|^4 + 6|V[\ \xi_j]|^2|a_j|^2 + 4(\ |V[\ \xi_j]|^2 + |a_j|^2\ )|a_j||V[\ \xi_j]|\ ] \qquad (7.41)$$
$$+ \sum_{j=0}^{N-1} [\ |b_j|^4 + 6|V[-\xi_j]|^2|b_j|^2 + 4(\ |V[-\xi_j]|^2 + |b_j|^2\ )|b_j||V[-\xi_j]|\ ]$$

If we apply the results from (7.37), (7.38), (7.39), and (7.40) to (7.41), then we obtain

$$|G| \ll \frac{N^3}{\sqrt{p_1}} \log^4(N) \qquad (7.42)$$

Thus provided (7.3) is satisfied, we have

$$\lim_{N\to\infty} \frac{G}{2N^3} = 0$$

$$\lim_{N\to\infty} \frac{G}{2N^3} = 0$$

which finishes the proof for part (1) of Theorem 6.3.3. □

Now we are ready to prove part (2) of Theorem 7.1.3.

Proof. (Theorem 7.1.3 part (2))

For $N = p_1 p_2 \ldots p_r$ odd, Lemma 6.3.2 shows that sequence z is symmetric or antisymmetric depending the value of $N \pmod 4$. Let the sequence β of length $2N$ be as defined in (3.1.5). Then for

$$b = \{z\ ;\ z\} * \beta$$

$$\sum_{k=1}^{2N-1} A_b^2(k) = N + \sum_{k=1}^{N-1} A_z^2(k) + 2 \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_z(k) A_z(k) + \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_z(k)^2 .$$

By Lemma 4.0.17.

The proof for part (1) of Theorem 7.1.3 shows that

$$2\sum_{k=1}^{N-1} A_z^2(k) \sim \frac{2}{3}N^2 \tag{7.43}$$

if the condition (7.3) holds. Lemma 7.2.7 shows that

$$\sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_z(k)^2 \leq \sum_{k=1}^{N-1} P_z(k)^2 \leq C \ll \frac{N^2}{p_1}$$

Then given condition (7.3), by the Cauchy-Schwarz inequality

$$|\sum_{\substack{k=1 \\ k \text{ even}}}^{N-1} P_z(k)A_z(k)| \leq \sqrt{[\sum_{\substack{k=1 \\ k \text{ even}}}^{N-1} A_z^2(k)] \cdot [\sum_{\substack{k=1 \\ k \text{ even}}}^{N-1} P_z^2(k)]}$$

$$\leq \sqrt{[\sum_{k=1}^{N-1} A_z^2(k)] \cdot [\sum_{k=1}^{N-1} P_z^2(k)]} \ll \frac{N^2}{\sqrt{p_1}}$$

Therefore, provided condition (7.3) holds, the asymptotic merit factor of b is

$$\lim_{N\to\infty}(F_b) = \lim_{N\to\infty} \frac{(2N)^2}{2(\sum_{k=1}^{2N-1} A_b^2(k))}$$

$$= \lim_{N\to\infty} \frac{4N^2}{2\sum_{k=1}^{N-1} A_\alpha^2(k)} = 4 \times \frac{3}{2} = 6\,.$$

This finishes the proof of part (2) of Theorem 7.1.3. □

Conclusion. For a long time, being afraid of losing ideal properties of the real prim-

itive character sequences, people have been passive in changing the values of those j-th positions with $gcd(j, N) > 1$. This thesis has provided new modifications to character sequences on those j-th positions with $gcd(j, N) > 1$. Particularly, at length $N = p_1 p_2$, the author has shown that we could have more freedom in changing the values on those positions. The author was informed recently that Jedwab and Schmidt have obtained the same result independently under an improved condition ([40]).

All the known binary sequences obtaining high asymptotic merit factor 6.0 prior to this thesis are of odd length. This thesis also provides a general technique to construct binary sequences of even length, from which the high asymptotic merit factor 6.0 can be achieved as well.

BIBLIOGRAPHY

[1] R.H. Barker, "Group Synchronizing of Binary Digital Systems", *Communication Theory (W. Jackson, ed.)*, Academic Press, New York, 1953, Page 273-287.

[2] R. Fano, *Transimission of Information*, Cambridge, MIT Press, 1961.

[3] EC Farnett, GH Stevens, Radar handbook, 1990 - helitavia.com.

[4] G.R. Welti, "Quaternary Codes for Pulsed Radar", *IRE Trans. Inform. Theory* Vol. IT-6, 1960, Page 400-408.

[5] A.M. Boehmer, "Binary Pulse Compression Codes", *IEEE Trans. Inform. Theory* Vol.IT-13, 1967, Page 156-167.

[6] R.J. Turyn and J. Storer, "On Binary Sequences", *Proc. Amer. Math. Soc.*, Vol. 12, 1961, Page 394-399.

[7] R.J. Turyn, "Sequences with Small Correlation", *Error Correcting Codes (H.B. Mann, ed.)*, Wiley, New York, 1968, Page 195-228.

[8] J. Jedwab, "What Can Be Used Instead of a Barker Sequence?", *Contemporary Math.*, Vol 461, 2008, Page 153-178.

[9] M.J.E. Golay, "A Class of Finite Binary Sequences with Alternate Autocorrelation Values Equal to Zero", *IEEE Trans. Inform. Theory*, Vol. IT-18, 1972, Page 449-450.

[10] M.J.E. Golay, "Hybrid Low Autocorrelation Sequences", *IEEE Trans. Inform. Theory*, Vol. IT-21, 1975, Page 460-462.

[11] M.J.E. Golay, "Sieves for Low autocorrelation Binary Sequences", *IEEE Trans. Inform. Theory*, Vol. IT-23, 1977, Page 43-51. .

[12] M.J.E. Golay, "The Merit Factor of Long Low Autocorrelation Binary Sequences", *IEEE Trans. Inform. Theory*, Vol. IT-28, 1982, Page 543-549.

[13] M.J.E. Golay. "The merit Factor of Legendre Sequences", *IEEE Trans. Inform. Theory*, Vol. IT-29, 1983, Page 934-936.

[14] M.J.E. Golay and D.B. Harris. "A New Search for Skewsymmetric Binary Sequences with Optimal Merit Factors", *IEEE Trans. Inform. Theory*, Vol. 36, 1990, Page 1163-1166.

[15] P. Borwein, R. Ferguson, and J. Knauer, "The Merit Factor Problem", *2000 Mathematics Subject Classification*, Vol. 11B83, 11Y55, Page 52-70.

[16] J.E. Littlewood, "Some Problems in Real and Complex Analysis", *Heath Mathematical Monographs*, D.C. Heath and Company, Massachusetts, 1968.

[17] J.E. Littlewood, "On Polynomials $\sum^n \pm z^m$, $\sum^n e^{\alpha m i} z^m$, $z = e^{\theta i}$", *J. London Math. Soc.*, Vol. 41, 1966, Page 367-376.

[18] D.J.Newman and J.S.Byrnes, "The L^4 Norm of a Polynomial with Coefficients ± 1", *Amer. Math. Monthly*, , Vol. 97, 1990, Page 42-45.

[19] L. Lunelli, "Tabelli di Sequenze $(+1, -1)$ con Autocorrelazione Troncata non Maggiore di 2", *Politecnico di Milano*, 1965.

[20] S. Mertens, "Exhaustive Search for Low-Autocorrelation Binary Sequences", *J. Phys. A: Math. Gen.*, Vol. 29, 1996, Page L473-L481.

[21] S. Mertens and H. Bauke, "Ground States of the Bernasconi Model with Open Boundary Conditions", *Online available: <http://odysseus.nat. uni-magdeburg. de/ mertens/bernasconi/open.dat>*, November 2004.

[22] J. Jedwab, "A Survey of the Merit Factor Problem for Binary Sequences," in: T. Helleseth et al, eds., *Lecture Notes in Computer Science, Vol. 3486, Sequences and Their Applications—Proceedings of SETA 2004*, Springer-Verlag, 2005, Page 30-55.

[23] T. Høholdt, H.E. Jensen, "Determination of the Merit Factor of Legendre Sequences," *IEEE Transactions on Inform. Theory*, Vol. 34 No. 1, Jan. 1988, Page 161–164.

[24] J.M. Jensen, H.E. Jensen, T. Høholdt, "The Merit Factor of Binary Sequences Related to Difference Sets," *IEEE Transactions on Inform. Theory*, Vol. 37 No. 3, May 1991, Page 617–625.

[25] P. Borwein,K-K. S. Choi, "Merit Factors of Polynomials Formed by Jacobi Symbols", *canad. J. Math.* Vol. 53 (1), 2001, Page 33-50.

[26] C. de Groot, D. Würtz, and K.H. Hoffmann, "Low Autocorrelation Binary Sequences: Exact Enumeration and Optimization by Evolutionary Strategies", *Optimization*, Vol. 23, 1992, Page 369-384.

[27] P. Borwein, K-K. S. Choi, and J. Jedwab, "Binary Sequences with Merit Factor Greater Than 6.34", *IEEE Transactions on Inform. Theory*, Vol. 50, No. 12, Dec. 2004, Page 3234–3249.

[28] M.G. Parker, "Even Length Binary Sequence Families with Low Negaperiodic Autocorrelation", *Applied Algebra, Algebraic Algorithms and Error-Correctin Codes, AAECC-14 Proceedings, Springer-Verlag*, 2001, Page 200-210.

[29] N.Y. Yu and G. Gong, "The Perfect Binary Sequence of Period 4 for Low Periodic and Aperiodic Autocorrelations", *Sequences, Subsequences, and Consequences, Springer-Verlag, Berlin*, 2007, Page 37-49.

[30] K.U. Schmidt, J. Jedwab, and M.G. Parker, "Two Binary Sequence Families with Large Merit Factor ", *Advances in Mathematics of Communications*, Vol. 3, No.2, 2009, Page 135-156.

[31] D.H. Green and P.R. Green, "Modified Jacobi Sequences", *IEE Proc.-Comput. Digit. Tech.*, Vol. 147 No. 4, July 2000, Page 241-251.

[32] W. Zhang, " On a Problem of P. Gallagher ", *Acta math. Hungar.* Vol. 78, 1998, Page 345-357.

[33] H. N. Liu, " New Pseudorandom Sequences Constructed Using Multiplicative Inverses ", *Acta Arith.* Vol. 125, 2006, Page 11-19.

[34] A. Weil, "Sur les courbes algebriques et les varietes qui s'en deduisent", *Actualites math. sci.* No.1041, Paris, 1945, Deuxieme Partie, §IV.

[35] A. A. Karatsuba,"Sums of Characters With Prime Numbers and Their Applications", *Tatra Mt. Math. Publ.* Vol. 20, 2000, Page 155-162.

[36] W. M. Schmidt,"Equations over Finite Fields: an Elementary Approach", Springer, 1976

[37] C. Mauduit and A. Sárközy, "On Finite Psudorandom Binary Sequences I: Measure of Pseudorandomness, the Legendre Symbol, *Acta Arithmetica*, LXXXII.4, 1997.

[38] G. Everest, T. Ward, "An Introduction to Number Theory", Springer, 2005.

[39] T. Xiong and J.I.Hall, "Construction of Even Length Binary Sequences With Asymptotic Merit Factor 6," *IEEE Transactions on Information Theory* Vol. 54(2), 2008, Page 931-935.

[40] J. Jedwab, K. Schmidt, "The Merit Factor of Binary Sequences Derived from the Jacobi Symbol", Preprint, 2010.

[41] T. Xiong and J.I.Hall, "Modifications of Modified Jacobi Sequences," submitted.

[42] B. Conrey, A. Granville, B. Poonen, K. Soundararajan, "Zeros Of Fekete Polynomials ", *Annales de l'institut Fourier*, Vol. 50, No. 3, 2000, Page 865-889.