

**ALMOST P-ARY PERFECT SEQUENCES AND THEIR  
APPLICATIONS TO CRYPTOGRAPHY**

**NEREDEYSE P-ARY MÜKEMMEL DİZİLER VE  
ONLARIN KRİPTOGRAFIYE UYGULANMASI**

**BÜŞRA ÖZDEN**

**ASSOC. PROF. DR. OĞUZ YAYLA**

**Supervisor**

Submitted to  
Graduate School of Science and Engineering of Hacettepe University  
as a Partial Fulfillment to the Requirements  
for the Award of the Degree of Master of Science  
in Mathematics

2019

This work named "**Almost  $p$ -ary Perfect Sequences and Their Applications to Cryptography**" by **Büşra ÖZDEN** has been approved as a thesis for the Degree of **MASTER OF SCIENCE IN MATHEMATICS** by the below mentioned Examining Committee Members.

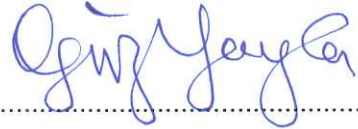
Prof. Dr. Evrim AKALAN

Head



Assoc. Prof. Dr. Oğuz YAYLA

Supervisor



Assoc. Prof. Dr. Oktay ÖLMEZ

Member



Assoc. Prof. Dr. Zülfükar SAYGI

Member



Assoc. Prof. Dr. Mesut ŞAHİN

Member



This thesis has been approved as a thesis for the Degree of **MASTER OF SCIENCE IN MATHEMATICS** by Board of Directors of the Institute for Graduate School of Science and Engineering.

Prof. Dr. Menemşe GÜMÜŞDERELİOĞLU

Director of the Institute of  
Graduate School of Science and Engineering

*To my brother*

## ETHICS

In this thesis study, prepared in accordance with the spelling rules of Institute of Graduate Studies in Science of Hacettepe University.

I declare that

- all the information and documents have been obtained in the base of the academic rules
- all audio-visual and written information and results have been presented according to the rules of scientific ethics
- in case of using other Works, related studies have been cited in accordance with the scientific standards
- all cited studies have been fully referenced
- I did not do any distortion in the data set
- and any part of this thesis has not been presented as another thesis study at this or any other university.

27/06/2019



Büşra ÖZDEN

## YAYINLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezimin/raporumun tamamını veya herhangi bir kısmını, basılı (kağıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanması zorunlu metinlerin yazılı izin alarak kullanıldığını ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim Kurulu tarafından yayınlanan “**Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge**” kapsamında tezim aşağıda belirtilen koşullar haricince YÖK Ulusal Tez Merkezi / H. Ü. Kütüphaneleri Açık Erişim Sisteminde erişime açılır.

- Enstitü / Fakülte yönetim kurulu kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren 2 yıl ertelenmiştir.
- Enstitü / Fakülte yönetim kurulu gerekçeli kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren .... ay ertelenmiştir.
- Tezim ile ilgili gizlilik kararı verilmiştir.

27/06/2019

Büşra ÖZDEN

This thesis was supported by TÜBİTAK (The Scientific and Technological Research Council of Turkey) under Project No: 116R026.

# ABSTRACT

## ALMOST P-ARY PERFECT SEQUENCES AND THEIR APPLICATIONS TO CRYPTOGRAPHY

Büşra ÖZDEN

Master of Science, Department of Mathematics

Supervisor: Assoc. Prof. Dr. Oğuz YAYLA

June 2019, 47 pages

In this thesis we study almost  $p$ -ary sequences and their autocorrelation coefficients. We first study the number  $\ell$  of distinct out-of-phase autocorrelation coefficients for an almost  $p$ -ary sequence of period  $n + s$  with  $s$  consecutive zero-symbols. We prove an upper bound and a lower bound on  $\ell$ . It is shown that  $\ell$  can not be less than  $\min\{s, p, n\}$ . In particular, it is shown that a nearly perfect sequence with at least two consecutive zero symbols does not exist. Next we define a new difference set, partial direct product difference set (PDPDS), and we prove the connection between an almost  $p$ -ary nearly perfect sequence of type  $(\gamma_1, \gamma_2)$  and period  $n + 2$  with two consecutive zero-symbols and a cyclic  $(n + 2, p, n, \frac{n-\gamma_2-2}{p} + \gamma_2, 0, \frac{n-\gamma_1-1}{p} + \gamma_1, \frac{n-\gamma_2-2}{p}, \frac{n-\gamma_1-1}{p})$  PDPDS for arbitrary integers  $\gamma_1$  and  $\gamma_2$ . We show that the almost  $p$ -ary sequences of type  $(\gamma_1, \gamma_2)$  and period  $n + 2$  with two consecutive zero-symbols are symmetric sequences except for zero entries. Then we prove a necessary condition on  $\gamma_2$  for the existence of such sequences. In particular, we show that they don't exist for  $\gamma_2 \leq -3$ .

Perfect sequences are very important for achieving non-linearity in a cryptosystem, and they are important in Code Division Multiple Access (CDMA) to ensure a proper communication. In this thesis, we show a method for obtaining cryptographic functions from almost  $p$ -ary nearly perfect sequences (NPS) of type  $(\gamma_1, \gamma_2)$ . In fact, most of the cases we obtain functions with the highest non-linearity, i.e. generalized bent functions. We use almost  $p$ -ary NPS of type  $(\gamma_1, \gamma_2)$  in CDMA communication. We simulate the bit-error-rate (BER) performance of CDMA with these sequences.

**Keywords:** Almost  $p$ -ary sequence, Nearly perfect sequence, Partial direct product difference set, cryptographic functions, generalized bent function, CDMA, bit-error-rate.

## ÖZET

### NEREDEYSE P-ARY DİZİLER VE ONLARIN KRİPTOGRAFIYE UYGULANMASI

**Büşra Özden**

**Yüksek Lisans, Matematik Bölümü**

**Tez Danışmanı: Doç. Dr. Oğuz Yayla**

**Haziran 2019, 47 sayfa**

Bu tezde, neredeyse  $p$ -ary diziler ve onların kriptografiye ve iletişime uygulamaları çalışılmıştır. Tezin ilk bölümünde neredeyse  $p$ -ary diziler ve onların otokorelasyon katsayıları çalışılmıştır. İlk olarak,  $n+s$  periyotlu ardışık  $s$  sıfır sembolü neredeyse  $p$ -ary dizinin tepe dışındaki otokorelasyon katsayılarının sayısı çalışılmıştır ve bu sayı  $\ell$  ile gösterilmektedir.  $\ell$  sayısı için bir üst sınır ve bir alt sınır bulunmuştur. Bu teoreme göre  $\ell$  sayısı  $\min\{s, p, n\}$  sayısından daha küçük olamaz. Bu durumda en az iki ardışık sıfır sembolü hemen hemen mükemmel bir dizi bulunmamaktadır. Yeni bir fark kümesi tanımlanmıştır ve bu küme *neredeyse direkt çarpım fark kümesi* (NDÇFK) olarak adlandırılıp  $n+2$  periyotlu ardışık 2 sıfır sembolü  $(\gamma_1, \gamma_2)$  tipindeki neredeyse  $p$ -ary dizisi ile bağlantı bulunmuştur.  $\gamma_1$  ve  $\gamma_2$  tamsayı olmak üzere,  $n+2$  periyotlu ardışık 2 sıfır sembolü  $(\gamma_1, \gamma_2)$  tipindeki neredeyse  $p$ -ary dizisi vardır ancak ve ancak  $R$  kümesi  $\mathbb{Z}_{n+s} \times \mathbb{Z}_p$ 'de,  $\left(n+2, p, n, \frac{n-\gamma_2-2}{p} + \gamma_2, 0, \frac{n-\gamma_1-1}{p} + \gamma_1, \frac{n-\gamma_2-2}{p}, \frac{n-\gamma_1-1}{p}\right)$ -NDÇK'dır. Bu dizilerin simetrik olduğu gösterilmiştir. Daha sonra, bir  $n+2$  periyotlu ardışık 2 sıfır sembolü  $(\gamma_1, \gamma_2)$  tipindeki neredeyse  $p$ -ary dizinin var olabilmesini sağlayan  $\gamma_2$  değeri için bir koşul ispatlanmıştır. Bu koşula göre  $\gamma_2 \leq -3$  için  $n+2$  periyotlu ardışık 2 sıfır sembolü  $(\gamma_1, \gamma_2)$  tipindeki neredeyse  $p$ -ary dizisi yoktur.

Tezin ikinci bölümünde, ilk bölümde çalışılmış olan dizilerin uygulamaları çalışılmıştır. Bu tezde, kriptografik fonksiyonları  $n+2$  periyotlu ardışık 2 sıfır sembolü  $(\gamma_1, \gamma_2)$  tipindeki neredeyse  $p$ -ary dizisinden elde etmek için bir yöntem verilmiştir. Bu yönteme göre çoğu durumda, dizilerden doğrusal olmama durumu fazla olan fonksiyonlar elde ederiz; genelleştirilmiş bent fonksiyonları. Son olarak, ilk bölümde çalışılmış olan dizileri KBÇE'de kullanılmıştır ve bu dizilerin bit-hata-oranı (BHO) performansı simüle edilmiştir.

**Anahtar Kelimeler:** neredeyse  $p$ -ary diziler, neredeyse mükemmel diziler, konferans matrisleri, kriptografik fonksiyonlar, kod bölmeli çoklu erişim



## ACKNOWLEDGEMENT

First of all, I would like to express my sincere gratitude to my supervisor Assoc. Prof. Dr. Oğuz Yayla for his invaluable suggestions, motivation, patience, and continuously support not only in this thesis but also in my life. His guidance helped me in all the time of research and writing of this thesis.

Besides my supervisor, I would like to thank the rest of my thesis committee: Prof. Dr. Evrim Akalan, Assoc. Prof. Dr. Oktay Ölmez, Assoc. Prof. Dr. Zülfükar Saygı, and Assoc. Prof. Dr. Mesut Şahin, for their encouragement, insightful comments.

I would like to my special thank to my dear friend Nihal Öztürk for always believing me and giving me strength.

I would like to express thanks to Damla Acar, Yağmur Çakıroğlu, and Sibel Kurt for supports during this thesis.

I acknowledge financial support from TÜBİTAK-3501 program during my graduate academic life.

Finally, I must express my very profound gratitude to my parents for providing me with unfailing support throughout all of my life. This accomplishment would not have been possible without them. And I would like to express thanks to my sister, who always keeps my information fresh. Thank you.

Büşra ÖZDEN

June 2019, Ankara

# Contents

	<u>Page</u>
ABSTRACT . . . . .	vii
ÖZET . . . . .	viii
ACKNOWLEDGEMENT . . . . .	ix
TABLE OF CONTENTS . . . . .	x
NOTATIONS . . . . .	xiii
1 INTRODUCTION . . . . .	1
2 ALMOST P-ARY SEQUENCES . . . . .	7
2.1 Preliminaries . . . . .	7
2.2 Autocorrelation Coefficients . . . . .	9
2.3 Partial Direct Product Difference Sets . . . . .	12
2.4 Conclusion . . . . .	22
3 APPLICATIONS . . . . .	23
3.1 Cryptographic Application . . . . .	23
3.1.1 Butson-Hadamard Matrices . . . . .	23
3.1.2 Generalized Bent Functions . . . . .	25
3.2 Communication Application . . . . .	29
3.3 Conclusion . . . . .	32
4 CONCLUSION AND FUTURE WORK . . . . .	33
4.1 Conclusion . . . . .	33
4.2 Future Work . . . . .	33
REFERENCES . . . . .	35
APPENDICES . . . . .	37
CURRICULUM VITAE . . . . .	46

## List of Figures

Figure 3.1. Structure of CDMA . . . . .	29
Figure 3.2. BER performance of CDMA with $a_1$ and 2, 3, 4 users respectively . . . .	30
Figure 3.3. BER performance of CDMA with $a_2$ and 2, 3, 4 users respectively . . . .	30
Figure 3.4. BER performance of CDMA with $a_3$ and 2, 3, 4 users respectively . . . .	30
Figure 3.5. BER performance of CDMA with $a_4$ and 2, 3, 4 users respectively . . . .	31

## List of Tables

Table 2.1. Difference table of the set $R_1$ . . . . .	8
Table 2.2. Difference Table of set $R_2$ . . . . .	13
Table 2.3. Non-existence results on NPS by Theorem 2.30 for $n=15$ . . . . .	21
Table 3.1. Examples of Walsh spectrum of some NPSs of type $(\gamma_1, \gamma_2)$ . . . . .	28

## NOTATIONS AND ACRONYMS

### Notations

$\mathbb{Z}$	Integers
$\mathbb{C}$	Complex numbers
$\bar{a}$	complex conjugate of $a$
$\zeta_p$	Primitive $p$ -th root of unity
$\langle, \rangle$	Dot product
$a_{ij}$	Entry of matrix
$C_{\underline{a}}(\cdot)$	Autocorrelation function of $\underline{a}$
$\hat{F}(\cdot)$	Walsh transform

### Acronyms

PS	Perfect sequence
NPS	Nearly perfect sequence
DS	Difference set
RDS	Relative difference set
DPDS	Direct product difference set
PDPDS	Partial direct product difference set
BH matrix	Butson-Hadamard matrix
CDMA	Code division multiple access
BER	bit-error-rate
AWGN	Additive white Gaussian noise
GBF	Generalized bent function

# 1 INTRODUCTION

Sequences have many applications in satellite telecommunication, cryptographic function design, wireless networks, signal processing, radar systems, and modern cell phones (see [1, 2, 3, 4, 5]). Sequences play an important role in the orthogonal signal design, for instance, spread spectrum communication and radar systems. In radar systems, correlation of the received signals and the transmitted signal must be zero to obtain the true echoes. In Code Division Multiple Access (CDMA), sequences with ideal correlation are important because a signal should not be affected by other signals in order to provide high-quality communication. In cryptography, privacy is provided by "good" Boolean functions and they are related to sequences having ideal correlation. For these reasons, sequences with the ideal correlation have been studied by many authors [6, 7, 8, 5]. Initially, binary sequences were widely studied, but complex sequences were started to be studied over time due to the lack of binary sequences with the ideal correlation.

We first give the definition of  $p$ -ary sequences and then we will present examples for illustrating their importance in cryptography and communication. Let  $p$  be a prime number. A  $p$ -ary sequence is a sequence whose entries are the power of primitive  $p$ -th root of unity. An almost  $p$ -ary sequence with  $s$  zero-symbols is a sequence with the power of primitive  $p$ -th root of unity of entries except for the  $s$  entries. It is widely used that a sequence with one zero-symbol is called an almost  $p$ -ary sequence.

**Example 1.1.** Let  $\zeta_5, \zeta_{11}$  be the primitive 5-th and 11-th roots of unity. Then,  $\underline{a} = (\zeta_5, \zeta_5^2, \zeta_5^4, 1, \zeta_5^2, \zeta_5^3, \dots)$  is a 5-ary sequence of period 6 and  $\underline{a} = (0, 0, \zeta_{11}, \zeta_{11}^4, \zeta_{11}^5, 0, \zeta_{11}^7, \dots)$  is an almost 11-ary sequence with 3 zero-symbols of period 7.

We now give an example to show the relationship between a sequence and a "good" cryptographic function.

**Example 1.2.** We choose a sequence  $\underline{a} = (0, 0, \zeta_7, 1, \zeta_7^2, 1, \zeta_7, \dots)$ , where  $\zeta_7 = e^{\frac{2i\pi}{7}}$ . We then construct a function  $f : \mathbb{Z}_7 \rightarrow \mathbb{Z}_7$  as follows  $f(5) = 1, f(4) = 0, f(3) = 2, f(2) = 0, f(1) = 1$  as  $\underline{a} = (0^{f(0)}, 0^{f(6)}, \zeta_7^{f(5)}, \zeta_7^{f(4)}, \zeta_7^{f(3)}, \zeta_7^{f(2)}, \zeta_7^{f(1)}, \dots)$ . By interpolating the function  $f$  of degree 2, we get a "good" cryptographic function  $f = 5x^2 + 5x + 5$ .

One of the aim of this thesis is to get "good" cryptographic functions via designing "good" sequences.

In the example below we show how a binary sequence is used in a signal design method, namely in CDMA.

**Example 1.3.** We consider that user<sub>1</sub> sends data<sub>1</sub> = 10 to the receiver<sub>1</sub> using the spreading\_code<sub>1</sub> = 1010. Here, data<sub>1</sub> is XORed by bit-bit with spreading\_code<sub>1</sub> and hence, the spreading\_message<sub>1</sub> is obtained.

$$\begin{array}{rcl}
 \text{data}_1 & = & 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \\
 \text{spreading\_code}_1 & = & 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \\
 \oplus \text{-----} & & \\
 \text{spreading\_message}_1 & = & 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0
 \end{array}$$

Similarly, we consider that user<sub>2</sub> sends data<sub>2</sub> = 11 to the receiver<sub>2</sub> using the spreading\_code<sub>2</sub> = 0000. Here, data<sub>2</sub> is XORed by bit-bit with spreading\_code<sub>2</sub> and hence, the spreading\_message<sub>2</sub> is obtained.

$$\begin{array}{rcl}
 \text{data}_2 & = & 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \\
 \text{spreading\_code}_2 & = & 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \\
 \oplus \text{-----} & & \\
 \text{spreading\_message}_2 & = & 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1
 \end{array}$$

Then, we are converting these messages into signals, separately. This is accomplished by 1 = -1 and 0 = 1 conversion. Hence, spreading\_message<sub>1</sub> is 1 -1 1 -1 -1 1 -1 1 and spreading\_message<sub>2</sub> is -1 -1 -1 -1 -1 -1 -1 -1. It is clear that spreading\_code<sub>1</sub> and spreading\_code<sub>2</sub> are orthogonal. Spreading\_message<sub>1</sub> is added to spreading\_message<sub>2</sub> so that the transmitted\_message is obtained.

$$\begin{array}{rcl}
 \text{spreading\_message}_1 & = & 1 \ -1 \ 1 \ -1 \ -1 \ 1 \ -1 \ 1 \\
 \text{spreading\_message}_2 & = & -1 \ -1 \ -1 \ -1 \ -1 \ -1 \ -1 \ -1 \\
 \oplus \text{-----} & & \\
 \text{transmitted\_message} & = & 0 \ -2 \ 0 \ -2 \ -2 \ 0 \ -2 \ 0
 \end{array}$$

In the receiver<sub>1</sub> side, firstly, to obtain data<sub>1</sub>, the transmitted\_message and the spreading\_code<sub>1</sub> are multiplied. Secondly, the transmitted message is divided into two. The elements of these pieces are added together and divided into four.

$$\begin{array}{rcl}
transmitted\_message & = & 0 \quad -2 \quad 0 \quad -2 \quad -2 \quad 0 \quad -2 \quad 0 \\
spreading\_code_1 & = & -1 \quad 1 \quad -1 \quad 1 \quad -1 \quad 1 \quad -1 \quad 1 \\
\hline
\otimes & & \\
signal_1 & = & 0 \quad -2 \quad 0 \quad -2 \quad 2 \quad 0 \quad 2 \quad 0 \\
& & \underbrace{\hspace{10em}} & \underbrace{\hspace{10em}} \\
& & \frac{0-2+0-2}{4} = -1 & \frac{2+0+2+0}{4} = 1 \\
& = & -11
\end{array}$$

Finally, we convert the  $signal_1$ , this is  $-11$ , into  $data_1$ . This is accomplished by  $-1=1$  and  $1=0$  conversion so that  $signal -11$  is  $10 = data_1$ . Similarly,  $data_2$  can be obtained. It means that this communication is successful.

Another aim of this thesis is to look for "good" spreading codes enabling noiseless communication as illustrated in the example above.

For a sequence  $\underline{a} = (a_0, a_1, \dots, a_n, \dots)$  of period  $n$ , its *autocorrelation function*  $C_{\underline{a}}(t)$  is defined as

$$C_{\underline{a}}(t) = \sum_{i=0}^{n-1} a_i \overline{a_{i+t}},$$

for  $0 \leq t \leq n-1$ . The values  $C_{\underline{a}}(t)$  at  $1 \leq t \leq n-1$  are called *the out-of-phase autocorrelation coefficients* of  $\underline{a}$ . Note that the autocorrelation function of  $\underline{a}$  is periodic with  $n$ .

We call an almost  $p$ -ary sequence  $\underline{a}$  of period  $n$  a *nearly perfect sequence* (NPS) of type  $(\gamma_1, \gamma_2)$  if all out-of-phase autocorrelation coefficients of  $\underline{a}$  are either  $\gamma_1$  or  $\gamma_2$ . We write *NPS of type  $\gamma$*  to denote an NPS of type  $(\gamma, \gamma)$ . Moreover, a sequence is called *perfect sequence* (PS) if it is an NPS of type  $(0, 0)$ . We also note that there is another notion of *almost perfect sequences* which is a  $p$ -ary sequence  $\underline{a}$  of period  $n$  having  $C_{\underline{a}}(t) = 0$  for all  $1 \leq t \leq n-1$  -with exactly one exception [9].

**Example 1.4.** We calculate the out-of-phase autocorrelation coefficients of the sequence  $\underline{a} = (1, \zeta_3, \zeta_3, \zeta_3, \dots)$ .

$$C_{\underline{a}}(1) = \sum_{i=0}^{n-1} a_i \overline{a_{i+1}} = 1 \cdot \zeta_3^2 + \zeta_3 \cdot \zeta_3^2 + \zeta_3 \cdot \zeta_3^2 + \zeta_3 \cdot 1 = \zeta_3^2 + 1 + 1 + \zeta_3 = 1$$

$$C_{\underline{a}}(2) = \sum_{i=0}^{n-1} a_i \overline{a_{i+2}} = 1 \cdot \zeta_3^2 + \zeta_3 \cdot \zeta_3^2 + \zeta_3 \cdot 1 + \zeta_3 \cdot \zeta_3^2 = \zeta_3^2 + 1 + \zeta_3 + 1 = 1$$



$$C_{\underline{a}}(3) = \sum_{i=0}^{n-1} a_i \overline{a_{i+1}} = 1 \cdot \zeta_3^2 + \zeta_3 \cdot 1 + \zeta_3 \cdot \zeta_3^2 + \zeta_3 \cdot \zeta_3^2 = \zeta_3^2 + \zeta_3 + 1 + 1 = 1$$

It is seen that the autocorrelation coefficients are equal to 1 for  $1 \leq t \leq 3$ . That is,  $\underline{a}$  is an 3-ary NPS of type (1,1) and period 4. Similarly,  $(\zeta_3, 0, 0, \zeta_3, 0, \zeta_3, \zeta_3, \dots)$  is an almost 3-ary NPS of type (2,2) and period 7 with 3 zero-symbols.  $(1, \zeta_3, \zeta_3, \dots)$  is a 3-ary NPS of type (0,0) and period 3, in fact this is a perfect sequence.

In this thesis, almost  $p$ -ary sequence with  $s$  zero-symbols is studied and their applications are investigated. Lately, NPSs have been worked by numerous authors. Jungnickel and Pott [9] worked a 2-ary NPS of type  $|\gamma| \leq 2$ . Ma and Ng [10] obtained a relation between a  $p$ -ary NPS of type  $|\gamma| \leq 1$  and a direct product difference set (DPDS) and obtained nonexistence on some  $p$ -ary NPS of type  $|\gamma| \leq 1$  by using character theory. Later Chee et al. [6] extended the methods due to Ma and Ng [10] to almost  $p$ -ary NPS of types  $\gamma = 0$  and  $\gamma = -1$  with one zero-symbol. Then, Özbudak et al. [11] proved the nonexistence of almost  $p$ -ary NPS with one zero-symbol at certain values. Liu and Feng [8] obtained new nonexistence results on  $p$ -ary PS and related difference sets (RDS) by using some results on cyclotomic fields and their sub-fields. They also considered almost  $p$ -ary PS with one zero-symbol. Chang Lv [12] obtained nonexistence of almost  $p$ -ary PS with  $s \leq 1$  zero-symbol for  $p \equiv 5 \pmod{8}$  (resp.  $p \equiv 3 \pmod{4}$ ) and period  $p^a q n'$  (resp.  $p^a q^l n'$ ) by considering equations cyclotomic fields satisfied by perfect sequences. Niu et al. [13] studied a binary sequence of the periodical with a 2-level autocorrelation value, this solves three open problems given by Jungnickel and Pott [9]. In [14], Çeşmelioglu and Ölmez studied the partial geometric difference sets, or  $1\frac{1}{2}$  difference sets, also their applications to cryptographic function, i.e. s-plateaued functions. In addition, they are shown that the relationship between three-valued cross-correlation of m-sequences and vectorial s-plateaued functions, and they are proved that the formed sets by using these sequences are partial geometric difference sets. Moreover, Yayla [15] proved an equality between a  $p$ -ary NPS of type  $\gamma$  and a DPDS for an arbitrary integer  $\gamma$ . In addition, he extended this result for an almost  $p$ -ary NPS with one zero-symbol, and proved its nonexistence cases by self-conjugacy condition.

The objective of this thesis is to analyze almost  $p$ -ary sequences with 2 zero-symbols and then apply them to telecommunication and cryptography. Very briefly, the existence of almost  $p$ -ary sequences with 2 zero-symbols with the aid of the results of [15] is studied in Chapter 2. Then, these sequences are used in the Code Division Multiple Access (CDMA) to bit-error-

rate (BER) analysis and cryptographic bent functions in Chapter 3.

In Chapter 2, we study almost  $p$ -ary sequences and their some properties. We first prove some bounds on the number of distinct out-of-phase autocorrelation coefficients of an almost  $p$ -ary sequence of period  $n + s$  with  $s$  consecutive zero-symbols (see Theorem 2.10). In particular, we prove that the number of distinct out-of-phase autocorrelation coefficients can not be less than  $\min\{s, p, n\}$ . It is known that there is an equivalence between perfect  $p$ -ary sequences and some difference sets. Therefore, in this thesis we define a new difference set called *partial direct product difference set* (PDPDS) (see Definition 2.14) and prove that a  $p$ -ary NPS of type  $(\gamma_1, \gamma_2)$  is equivalent to a PDPDS (see Theorem 2.18). And, we show that they exist only if  $p$  divides  $n - \gamma_2 - 2$  and  $n - \gamma_1 - 1$ . We show that the almost  $p$ -ary sequences of type  $(\gamma_1, \gamma_2)$  and period  $n+2$  with two consecutive zero-symbols are symmetric sequences except for zero entries (see Theorem 2.21). Finally, we show a bound on  $\gamma_2$  for the existence of an almost  $p$ -ary sequence of type  $(\gamma_1, \gamma_2)$  with two consecutive zero-symbols (see Theorem 2.30). As a consequence of this result we show that such sequences don't exist if  $\gamma_2 \leq -3$  (see Corollary 2.31).

In Chapter 3, the relationship between an almost  $p$ -ary sequences of period  $n + s$  with  $s$  consecutive zero-symbols and cryptographic function and CDMA is studied. In cryptography, privacy is provided by nonlinear *Boolean functions*. Non-linearity is satisfied by substitution boxes (s-boxes) in cryptography because they confuse a message into ciphertext. And, maximum non-linearity is obtained by so-called *Bent functions* used in the s-boxes. It is well known that one can get a generalized bent function from a PS (see [4] or Theorem 3.7 below). By extending this connection, we convert a NPS of type  $(\gamma_1, \gamma_2)$  to a generalized bent function in Section 3.1.2 and also we tabulate the examples of Walsh spectrum of functions obtained from NPSs of type  $(\gamma_1, \gamma_2)$  (see Table 3.1). It is seen that generalized bent functions can be obtained from nearly perfect sequences, and we obtain a larger set of cryptographic functions with the similar properties of generalized bent functions. The MAGMA codes used are given in the Appendix of the thesis.

While designing mobile communication technologies, it is aimed to provide the communication of the most possible users with the resources at hand. Different multiple access techniques have been developed for this purpose. The first two of them are Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA) used in GSM. In *TDMA*, users send and receive data over channels divided into a single frequency but

small time intervals. In *FDMA*, users are given different frequency ranges for data communication. With the rapid increase in the number of users in the developing world, CDMA technology has been developed to serve more users and higher data rates in 1957. In *CDMA*, instead of distributing time and frequency sources to users, users are given unique codes to transmit data at the same frequency and time. For high-quality communication, these codes must be orthogonal. These are orthogonal sequences, referred to herein as codes. In CDMA technology, we examined the working performance of  $p$ -ary sequences with  $s$  consecutive zero-symbols of type  $(\gamma_1, \gamma_2)$  studied in Chapter 3 and tabulated the results (see Section 3.2). The SAGE codes used are given in the Appendix of the thesis.

The rest of this thesis is organized as follows. In Chapter 2, almost  $p$ -ary sequences with  $s$  zero-symbols and their properties are presented. In Chapter 3, firstly, we show a method for obtaining cryptographic functions from almost  $p$ -ary nearly perfect sequences (NPS) of type  $(\gamma_1, \gamma_2)$ . Secondly, we present the BER analysis of almost  $p$ -ary nearly perfect sequences (NPS) of type  $(\gamma_1, \gamma_2)$  used in CDMA. Finally, the conclusion of this thesis and future works are given in Chapter 4.

The contribution of this thesis as follows:

- In Chapter 2; Theorem 2.10, Theorem 2.18, Corollary 2.22, Proposition 2.26, Theorem 2.30, Table 2.3, and Corollary 2.31,
- In Section 3.1 of Chapter 3; Table 3.1,
- In Section 3.2 of Chapter 3; Figure 3.2-3.5.

## 2 ALMOST P-ARY SEQUENCES

Let  $\zeta_p \in \mathbb{C}$  be a primitive  $p$ -th root of unity for some prime number  $p$ . A sequence  $\underline{a} = (a_0, a_1, \dots, a_{n-1}, \dots)$  of period  $n$  with  $a_i = \zeta_p^{b_i}$  for some integer  $b_i$ ,  $i = 0, 1, \dots, n-1$  is called a  $p$ -ary sequence. If  $a_{i_j} = 0$  for all  $j = 1, 2, \dots, s$  where  $\{i_1, i_2, \dots, i_s\} \subset \{0, 1, \dots, n-1\}$  and  $a_i = \zeta_p^{b_i}$  for some integer  $b_i$ ,  $i \in \{0, 1, \dots, n-1\} \setminus \{i_1, i_2, \dots, i_s\}$ , then we call  $\underline{a}$  an *almost  $p$ -ary sequence with  $s$  zero-symbols*. For instance,  $\underline{a} = (\zeta_3^3, \zeta_3^2, \zeta_3^4, \zeta_3^2, 1, \dots)$  is a 3-ary sequence of period 5 and  $\underline{a} = (0, \zeta_7^3, 1, \zeta_7^3, 0, 0, \zeta_7^5, \zeta_7^6, \zeta_7^6, \zeta_7^5, \dots)$  is an almost 7-ary sequence with 3 zero-symbols of period 10. It is widely used that a sequence with one zero-symbol is called an almost  $p$ -ary sequence. But in this paper we use this notation for a  $p$ -ary sequence with  $s$  zero-symbols, for  $s \geq 0$ .

For a sequence  $\underline{a}$  of period  $n$ , its *autocorrelation function*  $C_{\underline{a}}(t)$  is defined as

$$C_{\underline{a}}(t) = \sum_{i=0}^{n-1} a_i \overline{a_{i+t}},$$

for  $0 \leq t \leq n-1$ . The value  $C_{\underline{a}}(0)$  is called *the peak autocorrelation coefficients* of  $\underline{a}$ . In fact, the values  $C_{\underline{a}}(t)$  for all  $1 \leq t \leq n-1$  are called *the out-of-phase autocorrelation coefficients* of  $\underline{a}$ . Note that the autocorrelation function of  $\underline{a}$  is periodic with  $n$ .

We call an almost  $p$ -ary sequence  $\underline{a}$  of period  $n$  a *nearly perfect sequence* (NPS) of type  $(\gamma_1, \gamma_2)$  if all out-of-phase autocorrelation coefficients of  $\underline{a}$  are either  $\gamma_1$  or  $\gamma_2$ . We write *NPS of type  $\gamma$*  to denote an NPS of type  $(\gamma, \gamma)$ . Moreover, a sequence is called *perfect sequence* (PS) if it is an NPS of type  $(0, 0)$ . We also note that there is another notion of *almost perfect sequences* which is a  $p$ -ary sequence  $\underline{a}$  of period  $n$  having  $C_{\underline{a}}(t) = 0$  for all  $1 \leq t \leq n-1$  -with exactly one exception [9].

This Chapter is organized as follows. In Section 2.1 some preliminary results are presented. Then we present some properties of the autocorrelation coefficients of an almost  $p$ -ary sequence in Section 2.2. Then, we study the relation between an almost  $p$ -ary NPS and a partial direct product difference set in Section 2.3.

### 2.1 Preliminaries

We first give the definition of a direct product difference set.

**Definition 2.1.** [10] Let  $G = H \times P$ , where the order of  $H$  and  $N$  are  $n$  and  $m$ . The  $R \subset G$  set such that  $|R| = k$ , is called an  $(n, m, k, \lambda_1, \lambda_2, \mu)$  *direct product difference set (DPDS)*

in  $G$  relative to  $H$  and  $P$  if differences  $r_1 r_2^{-1}$ ,  $r_1, r_2 \in R$  with  $r_1 \neq r_2$  represent

- all non identity elements of  $H$  exactly  $\lambda_1$  times,
- all non identity elements of  $P$  exactly  $\lambda_2$  times,
- all non identity elements of  $G \setminus H \cup P$  exactly  $\mu$  times.

We can also define the DPDSs by using the group-ring algebra notation. Let  $\sum_{g \in R} g$  be an element of the group ring  $\mathbb{Z}[G]$ . If  $R$  is an  $(n, m, k, \lambda_1, \lambda_2, \mu)$ -DPDS in  $G$  relative to  $H$  and  $P$  then

$$RR^{(-1)} = (k - \lambda_1 - \lambda_2 + \mu) + \lambda_1 H + \lambda_2 P + \mu G \setminus (H \cup P) \quad (2.1)$$

holds in  $\mathbb{Z}[G]$ .

Now, we are given an example of DPDS.

**Example 2.2.**  $R_1$  set is written as  $R_1 = \{(0, 2), (1, 2), (2, 2), (3, 2), (4, 0)\} \subseteq \mathbb{Z}_5 \times \mathbb{Z}_3$  for almost 3-ary sequence  $\underline{a} = (\zeta_3^2, \zeta_3^2, \zeta_3^2, \zeta_3^2, 1, \dots)$ . Next, we are created of the difference table for this  $R_1$  set.

Table 2.1: Difference table of the set  $R_1$

	(0,2)	(1,2)	(2,2)	(3,2)	(4,0)
(0,2)	(0,0)	(4,0)	(3,0)	(2,0)	(1,2)
(1,2)	(1,0)	(0,0)	(4,0)	(3,0)	(2,2)
(2,2)	(2,0)	(1,0)	(0,0)	(4,0)	(3,2)
(3,2)	(3,0)	(2,0)	(1,0)	(0,0)	(4,2)
(4,0)	(4,1)	(3,1)	(2,1)	(1,1)	(0,0)

According to this difference table, we get  $\lambda_1 = 3$  as blue marked,  $\lambda_2 = 0$ ,  $\mu = 1$  as red marked, and  $R_1$  is a  $(5, 3, 5, 3, 0, 1)$ -DPDS in  $\mathbb{Z}_5 \times \mathbb{Z}_3$ . Here, we can see that the equation (2.1) is satisfied.

$$R_1 R_1^{(-1)} = (5 - 3 - 0 + 1) + 3H + 1G \setminus (H \cup N)$$

where  $H = \mathbb{Z}_5$ ,  $N = \mathbb{Z}_3$  and  $G = H \times N$ .

The following result on vanishing sums of roots of unity due to Lam and Leung [16], see also [17, Proposition 2.1].

**Lemma 2.3.** [16] *Let  $m$  be an integer with prime factorization  $m = p_1^{a_1} p_2^{a_2} \dots p_\ell^{a_\ell}$ . If there are  $m$ -th roots of unity  $\xi_1, \xi_2, \dots, \xi_v$  with  $\xi_1 + \xi_2 + \dots + \xi_v = 0$ , then  $v = p_1 t_1 + p_2 t_2 + \dots + p_\ell t_\ell$  with non-negative integers  $t_1, t_2, \dots, t_\ell$ .*

We now give the relation between an NPS and a DPDS. Let  $p$  be a prime,  $n \geq 2$  be an integer, and  $\underline{a} = (a_0, a_1, \dots, a_n, \dots)$  be an almost  $p$ -ary sequence of period  $n + s$  with  $s$  zero-symbol such that  $a_{i_j} = 0$  for all  $j = 1, 2, \dots, s$  where  $\{i_1, i_2, \dots, i_s\} \subset \{0, 1, \dots, n + s - 1\}$ . Let  $H = \langle h \rangle$  and  $P = \langle g \rangle$  be the (multiplicatively written) cyclic groups of order  $n + s$  and  $p$ . Let  $G$  be the group defined as  $G = H \times P$ . We choose a primitive  $p$ -th root of 1,  $\zeta_p \in \mathbb{C}$ . For  $i \in \{0, 1, \dots, n + s - 1\} \setminus \{i_1, i_2, \dots, i_s\}$  let  $b_i$  be the integer in  $\{0, 1, 2, \dots, p - 1\}$  such that  $a_i = \zeta_p^{b_i}$ . The  $R_a \subset G$  set defined as

$$R_a = \{(g^{b_i} h^i) \in G : i \in \{0, 1, \dots, n + s - 1\} \setminus \{i_1, i_2, \dots, i_s\}\}. \quad (2.2)$$

In the following we present a known result between an almost  $p$ -ary sequence of type  $\gamma$  with one zero-symbol and a DPDS such that  $\gamma \in \mathbb{Z}$ .

**Theorem 2.4.** [15]  *$\underline{a}$  is an almost  $p$ -ary NPS of period  $n + 1$  and type  $\gamma$  with one zero-symbol if and only if  $R_a$  defined as in (2.2) is an  $(n + 1, p, n, \frac{n-\gamma-1}{p} + \gamma, 0, \frac{n-\gamma-1}{p})$ -DPDS in  $G$  relative to  $H$  and  $P$ . In particular,  $p|(n - \gamma - 1)$ .*

**Example 2.5.**  $\underline{a} = (0, \zeta_3^2, \zeta_3^2, \zeta_3^2, 1, \zeta_3^2, \zeta_3, \zeta_3, \zeta_3^2, 1, \zeta_3^2, \zeta_3^2, \zeta_3^2, \dots)$  is an almost 3-ary NPS of period 13 and type 2 with one zero-symbol. If  $R_a$  is defined as in (2.2), then we are obtained

$$\begin{aligned} R_a &= \{(1^{b_i} 1^i) \in \mathbb{Z}_{13} \times \mathbb{Z}_3 : i \in \{0, 1, \dots, 12\} \setminus \{i_1\}\} \\ &= \{(i, b_i) \in \mathbb{Z}_{13} \times \mathbb{Z}_3 : i \in \{0, 1, \dots, 12\} \setminus \{i_1\}\} \\ &= \{(1, 2), (2, 2), (3, 2), (4, 0), (5, 2), (6, 1), (7, 1), (8, 2), (9, 0), (10, 2), (11, 2), (12, 2)\}. \end{aligned}$$

According to Theorem 2.4,  $R_a$  is an  $(13, 3, 12, \frac{12-2-1}{3} + 2, 0, \frac{12-2-1}{3}) = (13, 3, 12, 5, 0, 3)$ -DPDS in  $\mathbb{Z}_{13} \times \mathbb{Z}_3$ .

## 2.2 Autocorrelation Coefficients

In this section we use the notation of the previous section. We first give an extension of a well known divisibility result on difference sets whose proof follows by counting the number of elements in the difference table.

**Proposition 2.6.** *Let  $\underline{a}$  is a  $p$ -ary sequence of period  $n + s$  with  $s$  zero-symbol. Let  $R_a$  be a  $(n + s, p, n, \lambda_1, \lambda_2, \mu)$ -DPDS. Then  $(n + s - 1)(\lambda_1 + \mu(p - 1)) = n^2 - n$ .*

*Proof.* We know that there are  $n^2 - n$  nonidentity elements in the difference table of  $R_a$ . They correspond to  $\lambda_1$  times nonidentity elements of  $\mathbb{Z}_{n+s} \times \{0\}$  and  $\mu$  times nonidentity elements of  $\mathbb{Z}_{n+s} \times \mathbb{Z}_p \setminus (\mathbb{Z}_{n+s} \times \{0\} \cup \{0\} \times \mathbb{Z}_p)$ . Hence the result follows.  $\square$

It is now clear that  $R_a$  is not a DPDS if  $(n + s - 1) \nmid n^2 - n$ . If the zero-symbols are consecutive we have more than the divisibility condition. The proof of the following result follows similarly.

**Proposition 2.7.** *Let  $\underline{a}$  is a  $p$ -ary sequence of period  $n + s$  with  $s \geq 1$  consecutive zero-symbol. Let  $R_a$  be a  $(n + s, p, n, \lambda_1, \lambda_2, \mu)$ -DPDS. Then  $n - i = \lambda_1 + \mu(p - 1)$  for  $i = 1, 2, \dots, s$ , and so  $s = 1$ . In addition, if  $s = 0$  then  $n = \lambda_1 + \mu(p - 1)$  holds.*

*Proof.* If  $R$  is a  $(n + s, p, n, \lambda_1, \lambda_2, \mu)$ -DPDS, then by checking the sub-diagonal entries in difference table we have  $n - i = \lambda_1 + \mu(p - 1)$  for  $i=1,2,\dots,s$ . Thus, right hand side of this equation is fixed and so this can only hold for one index  $i$ , i.e.  $s = 1$ . The later statement of the theorem holds similarly.  $\square$

**Example 2.8.** *Let  $\underline{a} = (0, \zeta_3^2, \zeta_3^2, \zeta_3^2, 1, \zeta_3^2, \zeta_3, \zeta_3, \zeta_3^2, 1, \zeta_3^2, \zeta_3^2, \zeta_3^2, \dots)$  be a 3-ary NPS of period 13 and  $s = 1$ . Here we have  $\lambda_1 = 5$  and  $\mu = 3$ , then Proposition 2.7 is satisfied. Similarly, let  $\underline{a} = (\zeta_3^2, \zeta_3^2, \zeta_3^2, \zeta_3^2, 1, \dots)$  be a 3-ary NPS of period 5 and  $s = 0$ . In this case we have  $\lambda_1 = 3$  and  $\mu = 1$ , then Proposition 2.7 is also satisfied.*

Now we show that if  $s \geq 2$  there does not exist a nearly perfect sequence with only one out-of-phase autocorrelation coefficient. Before that we give the following lemma.

**Lemma 2.9.** *The number of congruence classes in a set  $\{1, 2, \dots, s\}$  modulo some prime  $p \leq s$  is equivalent to  $p$ .*

**Theorem 2.10.** *Let  $\underline{a}$  be an almost  $p$ -ary sequence of period  $n + s$  with  $s$  consecutive zero-symbols. Let  $\ell$  be the number of distinct elements in the set  $\{C_{\underline{a}}(1), C_{\underline{a}}(2), \dots, C_{\underline{a}}(n+s-1)\}$ . Then,*

$$\min\{s, p, n\} \leq \ell \leq n - 1 + \min\{n, s\}.$$

*Proof.* We first consider the case  $n > s$ . Let  $B = \{C_{\underline{a}}(1), C_{\underline{a}}(2), \dots, C_{\underline{a}}(s), \dots, C_{\underline{a}}(n), \dots, C_{\underline{a}}(n+s-2), C_{\underline{a}}(n+s-1)\}$ . Then we have

$$\begin{aligned}
B = & \{a_s \bar{a}_{s+1} + a_{s+1} \bar{a}_{s+2} + \dots + a_{n+s-2} \bar{a}_{n+s-1}, \\
& a_s \bar{a}_{s+2} + a_{s+1} \bar{a}_{s+3} + \dots + a_{n+s-3} \bar{a}_{n+s-1}, \\
& \dots \\
& a_s \bar{a}_{2s} + a_{s+1} \bar{a}_{2s+1} + \dots + a_{n-1} \bar{a}_{n+1}, \\
& \dots \\
& a_{2s} \bar{a}_s + a_{2s+1} \bar{a}_{s+1} + \dots + a_{n+1} \bar{a}_{n-1}, \\
& \dots \\
& a_{s+2} \bar{a}_s + a_{s+3} \bar{a}_{s+1} + \dots + a_{n+s-1} \bar{a}_{n+s-3}, \\
& a_{s+1} \bar{a}_s + a_{s+2} \bar{a}_{s+1} + \dots + a_{n+s-1} \bar{a}_{n+s-2}\}.
\end{aligned}$$

And let  $\ell$  be the number of distinct elements in  $B$ . If all the elements in  $B$  are distinct, then maximum value of  $\ell$  is  $\ell_{max} = \#B = n + s - 1$ . On the other hand,  $C_{\underline{a}}(i)$  is the sum of  $n - i$  elements for  $i = 1, 2, \dots, s$ ;  $C_{\underline{a}}(i)$  is the sum of  $n - s$  elements for  $i = s + 1, s + 2, \dots, n$  and  $C_{\underline{a}}(i)$  is the sum of  $i - s$  elements for  $i = n + 1, n + 2, \dots, n + s - 1$ . We note that the number of summands in  $C_{\underline{a}}(i)$  equals to the number of summands in  $C_{\underline{a}}(n + s - i)$  for  $i = 1, 2, \dots, s$  and the number of summands in  $C_{\underline{a}}(i)$  equals to the number of summands in  $C_{\underline{a}}(s)$  for  $i = s + 1, s + 2, \dots, n$ . Thus, we can decide the maximum value of  $\ell$  by checking the equality of  $C_{\underline{a}}(t)$  values for  $t \in \{1, 2, \dots, s\}$ . If  $C_{\underline{a}}(1) = C_{\underline{a}}(2)$  then  $C_{\underline{a}}(1) - C_{\underline{a}}(2) = 0$ , that is

$$a_s \bar{a}_{s+1} + a_{s+1} \bar{a}_{s+2} + \dots + a_{n+s-2} \bar{a}_{n+s-1} - (a_s \bar{a}_{s+2} + \dots + a_{n+s-3} \bar{a}_{n+s-1}) = 0.$$

Then we have,

$$\zeta_p^{b_s - b_{s+1}} + \zeta_p^{b_{s+1} - b_{s+2}} + \dots + \zeta_p^{b_{n+s-2} - b_{n+s-1}} - (\zeta_p^{b_s - b_{s+2}} + \dots + \zeta_p^{b_{n+s-3} - b_{n+s-1}}) = 0$$

where  $a_i = \zeta_p^{b_i}$  for some integer  $b_i$ , so

$$\begin{aligned}
& \zeta_p^{b_s - b_{s+1}} + \zeta_p^{b_{s+1} - b_{s+2}} + \dots + \zeta_p^{b_{n+s-2} - b_{n+s-1}} + \\
& (\zeta_p^{p-1} + \zeta_p^{p-2} + \dots + \zeta_p)(\zeta_p^{b_s - b_{s+2}} + \dots + \zeta_p^{b_{n+s-3} - b_{n+s-1}}) = 0.
\end{aligned}$$

Hence we get that  $n - 1 + (p - 1)(n - 2) = p(n - 2) + 1$  number of  $p$ -th root of unities sum up to zero. Similarly, the number of  $p$ -th root of unities in difference

$$C_{\underline{a}}(i) - C_{\underline{a}}(j)$$



is  $p(n - j) + j - i$  for  $j > i$ . By Lemma 2.3, the above equation vanishes only if  $p|j - i$ , that is  $i \equiv j \pmod{p}$ . If  $s > p$  then we have at least  $p$  distinct equivalence classes in the set  $\{1, 2, \dots, s\}$  modulo  $p$  by Lemma 2.9, and so  $\ell_{\min} = p$ . If  $p \geq s$  then  $p \nmid j - i$  for distinct  $i, j \in \{1, 2, \dots, s\}$ , and so we get  $\ell_{\min} = s$ .

Similarly, in the case of  $s \geq n$ ,  $\ell_{\max} = n - 1 + 1 + n - 1 = 2n - 1$ ,  $\ell_{\min} = p$  for  $n > p$  and  $\ell_{\min} = n$  for  $p \geq n$ .  $\square$

**Example 2.11.** For almost 3-ary sequences  $\underline{a}_1 = (0, 0, \zeta_3, \zeta_3, \zeta_3, \zeta_3, \dots)$ ,  $\underline{a}_2 = (0, 0, \zeta_3^2, \zeta_3, \zeta_3, \zeta_3^2, \dots)$ ,  $\underline{a}_3 = (0, 0, \zeta_3, 1, \zeta_3, \zeta_3, \dots)$  and  $\underline{a}_4 = (0, 0, \zeta_3^2, \zeta_3^2, 1, 1, \dots)$ , the number of distinct autocorrelation coefficients satisfies  $\ell = 2, 3, 4, 5$  respectively. Here we have  $s = 2$ ,  $n = 4$ ,  $p = 3$ . So Theorem 2.10 is satisfied, i.e.  $\min\{2, 4, 3\} \leq \ell \leq 4 - 1 + \min\{2, 4\}$ .

**Example 2.12.** Almost 3-ary sequences  $\underline{a}_1 = (1, 0, 0, 1, 0, 1, 1, \dots)$ ,  $\underline{a}_2 = (\zeta_3, 0, 0, \zeta_3, 0, \zeta_3, \dots)$  and  $\underline{a}_3 = (\zeta_3^2, 0, 0, \zeta_3^2, 0, \zeta_3^2, \dots)$  are NPS of type (2,2) and period 7 with 3 zero-symbols. Hence, Theorem 2.10 does not hold for almost  $p$ -ary sequences with non consecutive zero-symbols.

Now we give a direct consequence of Theorem 2.10, which says that one can not get an NPS of type  $\gamma$  by adding extra zero-symbols at consecutive positions.

**Corollary 2.13.** For  $n \in \mathbb{Z}^+$ , a prime number  $p$ ,  $s \geq 2$  and  $\gamma \in \mathbb{Z}$ , there does not exist an almost  $p$ -ary NPS of type  $\gamma$  and period  $n + s$  with  $s$  consecutive zero-symbols.

## 2.3 Partial Direct Product Difference Sets

Here we give a new difference set definition, called *partial direct product difference set (PDPDS)*.

**Definition 2.14.** Let  $G = H \times P$  be a group such that  $H = \langle h \rangle$  and  $P = \langle g \rangle$  are cyclic groups with  $|H| = n$  and  $|P| = m$ . The  $R \subset G$  set,  $|R| = k$ , is called an  $(n, m, k, \lambda_1, \lambda_2, \lambda_3, \mu_1, \mu_2)$  partial direct product difference set (PDPDS) in  $G$  relative to  $H$  and  $P$  if differences  $r_1 r_2^{-1}, r_1, r_2 \in R$  with  $r_1 \neq r_2$  represent

- all elements of  $\{h^2, h^3, \dots, h^n\}$  exactly  $\lambda_1$  times,
- all non identity elements of  $P$  exactly  $\lambda_2$  times,
- all elements of  $\{h, h^{n-1}\}$  exactly  $\lambda_3$  times,

- all elements of  $\{h^2, h^3, \dots, h^n\} \times \{g, g^2, \dots, g^{p-1}\}$  exactly  $\mu_1$  times,
- all non identity elements of  $\{h, h^{n-1}\} \times \{g, g^2, \dots, g^{p-1}\}$  exactly  $\mu_2$  times.

In the group-ring algebra notation, if  $R$  is an  $(n, m, k, \lambda_1, \lambda_2, \lambda_3, \mu_1, \mu_2)$ -PDPDS in  $G$  relative to  $H$  and  $P$  then

$$RR^{(-1)} = (k - \lambda_1 - \lambda_2 + \mu_1) + (\lambda_1 - \mu_1)H + (\lambda_2 - \mu_1)P + \mu_1G + (\lambda_3 - \lambda_1)\{h, h^{n-1}\} + (\mu_2 - \mu_1)(\{h, h^{n-1}\} \times \{g, g^2, \dots, g^{p-1}\}) \quad (2.3)$$

holds in  $\mathbb{Z}[G]$ .

Now, we are given an example of PDPDS.

**Example 2.15.**  $R_2$  set is written as  $R_2 = \{(2, 2), (3, 1), (4, 0), (5, 1), (6, 2)\} \subseteq \mathbb{Z}_7 \times \mathbb{Z}_3$  for almost 3-ary sequence  $\underline{a} = (0, 0, \zeta_3^2, \zeta_3, 1, \zeta_3, \zeta_3^2, \dots)$ . Next, we are created of the difference table for this  $R_2$  set.

Table 2.2: Difference Table of set  $R_2$

	(2,2)	(3,1)	(4,0)	(5,1)	(6,2)
(2,2)	(0,0)	(6,1)	(5,2)	(4,1)	(3,0)
(3,1)	(1,2)	(0,0)	(6,1)	(5,0)	(4,2)
(4,0)	(2,1)	(1,2)	(0,0)	(6,2)	(5,1)
(5,1)	(3,2)	(2,0)	(1,1)	(0,0)	(6,2)
(6,2)	(4,0)	(3,1)	(2,2)	(1,1)	(0,0)

According to this difference table, we get  $\lambda_1 = 1$  as green marked,  $\lambda_2 = 0$ ,  $\lambda_3 = 0$ ,  $\mu_1 = 1$  as blue marked,  $\mu_2 = 2$  as red marked and  $R_2$  is a  $(7, 3, 5, 1, 0, 0, 1, 2)$ -DPDS in  $\mathbb{Z}_7 \times \mathbb{Z}_3$ . Here, we can see that the (2.3) equation is satisfied.

$$R_2R_2^{(-1)} = (5 - 1 - 0 + 1) + (1 - 1)(H \times \{0\}) + (0 - 1)(\{0\} \times P) + 1G + (0 - 1)\{1, 6\} + (2 - 1)(\{1, 6\} \times \{1, 2\})$$

where  $H = \mathbb{Z}_7$ ,  $P = \mathbb{Z}_3$  and  $G = H \times P$ .

**Remark 2.16.** Let  $G = H \times P$  be a group such that  $H$  and  $P$  are cyclic groups with  $|H| = n$  and  $|P| = m$ . An  $(n, m, k, \lambda_1, \lambda_2, \lambda_1, \mu, \mu)$ -PDPDS in  $G$  relative to  $H$  and  $P$  is an  $(n, m, k, \lambda_1, \lambda_2, \mu)$ -DPDS in  $G$  relative to  $H$  and  $P$ . Moreover, an  $(n, m, k, \lambda, 0, \lambda, \lambda, \lambda)$ -PDPDS in  $G$  relative to  $H$  and  $P$  is an  $(n, m, k, \lambda)$ -RDS in  $G$  relative to  $P$ . Finally, an  $(n, m, k, \lambda, \lambda, \lambda, \lambda, \lambda)$ -PDPDS in  $G$  relative to  $H$  and  $P$  is an  $(nm, k, \lambda)$ -DS in  $G$ .

We extend Proposition 2.6 for DPDS to PDPDS below.

**Proposition 2.17.** *Let  $\underline{a} = (a_0, a_1, \dots, a_{n+1}, \dots)$  be an almost  $p$ -ary sequence of period  $n + 2$  such that  $a_0 = 0$  and  $a_1 = 0$ . Let  $R$  be  $(n + 2, m, k, \lambda_1, \lambda_2, \lambda_3, \mu_1, \mu_2)$ -PDPDS. Then  $(n - 1)(\lambda_1 + (p - 1)\mu_1) + 2(\lambda_3 + (p - 1)\mu_2) = n^2 - n$ .*

*Proof.* We know that there are  $n^2 - n$  non-identity elements in the difference table of  $R$  and we know that  $\lambda_1$  times  $\{h^2, h^3, \dots, h^n\} \times \{0\}$ ,  $\lambda_3$  times  $\{h, h^{n+1}\} \times \{0\}$ ,  $\mu_1$  times  $\{h^2, h^3, \dots, h^n\} \times \{g, g^2, \dots, g^{p-1}\}$  and  $\mu_2$  times  $\{h, h^{n+1}\} \times \{g, g^2, \dots, g^{p-1}\}$  from the definition of PDPDS. So,  $(n - 1)\lambda_1 + 2\lambda_3 + (n - 1)(p - 1)\mu_1 + 2(p - 1)\mu_2 = n^2 - n$ . Hence the result follows.  $\square$

Now we present a relation between a PDPDS and an NPS with two distinct out-of-phase autocorrelation coefficients. Before that, we give some definitions. A character  $\chi$  of a group  $G$  is group homomorphism from  $G$  to multiplicative group of a field. If  $\chi(g) = 1$  for all  $g \in G$ , then character  $\chi$  is called *principal character*. Others are called *nonprincipal character*.

**Theorem 2.18.** *Let  $p$  be a prime,  $n \in \mathbb{Z}^+$  such that  $n \geq 2$ , and  $\underline{a} = (0, 0, \dots, a_{n+1}, \dots)$  be an almost  $p$ -ary sequence of period  $n + 2$  with consecutive 2 zero-symbols. Let  $H = \langle h \rangle$  and  $P = \langle g \rangle$  be the (multiplicatively written) cyclic groups and  $|H| = n + 2$ ,  $|P| = p$ . Let  $G$  be the group defined as  $G = H \times P$ . For  $2 \leq i \leq n + 1$ , let  $b_i \in \mathbb{Z}_p$  such that  $a_i = \zeta_p^{b_i}$ . Then,  $\underline{a}$  is an almost  $p$ -ary NPS of type  $(\gamma_1, \gamma_2)$  if and only if  $R$  defined as in (2.2) is an*

$$\left( n + 2, p, n, \frac{n - \gamma_2 - 2}{p} + \gamma_2, 0, \frac{n - \gamma_1 - 1}{p} + \gamma_1, \frac{n - \gamma_2 - 2}{p}, \frac{n - \gamma_1 - 1}{p} \right)$$

-PDPDS in  $G$  relative to  $H$  and  $N$ .

*Proof.* Let  $A = \sum_{i=0}^{n-1} a_i h^i \in \mathbb{C}[H]$ . Then we have

$$A\bar{A}^{(-1)} = \sum_{t=0}^{n-1} C_a(t) h^t.$$

Let  $\chi$  be a character on  $P$ . We extend  $\chi$  to  $G$  such that  $\chi(h) = h$ . Let  $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_p) \setminus \mathbb{Q})$  such that  $\sigma(\zeta_p) = \chi(\zeta_p)$ . If  $\chi$  is a nonprincipal character on  $P$ , then we have  $\chi(R) = A^\sigma$ , and so

$$\chi(RR^{(-1)}) = (A\bar{A}^{(-1)})^\sigma.$$

Conversely, if  $\chi$  is a principal character on  $P$ , then we have

$$\chi(R) = H - \{1, h\}$$

and also

$$\chi(R^{(-1)}) = H - \{1, h^{n+1}\}.$$

Then

$$\chi(RR^{(-1)}) = \begin{cases} (H - \{1, h\})(H - \{1, h^{n+1}\}) & \text{if } \chi \text{ is principal on } P, \\ \sum_{t=0}^{n-1} C_a(t) \sigma h^t & \text{if } \chi \text{ is nonprincipal on } P. \end{cases}$$

So

$$\chi(RR^{(-1)}) = \begin{cases} (n-2)H + 2 + \{h, h^{n+1}\} & \text{if } \chi \text{ is pr. on } P, \\ \sum_{t=0}^{n-1} C_a(t) \sigma h^t & \text{if } \chi \text{ is nonpr. on } P. \end{cases}$$

If  $\underline{a}$  is an NPS of type  $(\gamma_1, \gamma_2)$ , then

$$\chi(RR^{(-1)}) = \begin{cases} (n-2)H + 2 + \{h, h^{n+1}\} & \text{if } \chi \text{ is pr. on } P, \\ n - \gamma_2 + (\gamma_1 - \gamma_2)\{h, h^{n+1}\} + \gamma_2 H & \text{if } \chi \text{ is nonpr. on } P. \end{cases} \quad (2.4)$$

By extending  $\chi$  to  $H$  we obtain

$$\chi(RR^{(-1)}) = \begin{cases} n^2 & \text{if } \chi \text{ is pr. on } P \text{ and } H, \\ 2 + h + h^{-1} & \text{if } \chi \text{ is pr. on } P \text{ and nonpr. on } H, \\ n + \gamma_2(n-1) + 2\gamma_1 & \text{if } \chi \text{ is nonpr. on } P \text{ and pr. on } H, \\ n - \gamma_2 + h + h^{-1} & \text{if } \chi \text{ is nonpr. on } P \text{ and nonpr. on } H. \end{cases} \quad (2.5)$$

First, we can consider

$$RR^{(-1)} = n - x + xH - zP + zG + x'\{h, h^{n+1}\} + z'(\{h, h^{n+1}\} \times \{g, g^2, \dots, g^{p-1}\}) \quad (2.6)$$

for some integers  $x, x', z, z'$ . We get the following equations by (2.5) and (2.6)

$$2 + h + h^{-1} = n - x + zp + x'(h + h^{-1}) \quad (2.7)$$

$$n - \gamma_2 + (h + h^{-1})(\gamma_1 - \gamma_2) = n - x + x'(h + h^{-1}) - z'(h + h^{-1}) \quad (2.8)$$

If we solve (2.7) and (2.8) together, then we get  $x = \gamma_2$ ,  $z = \frac{n-\gamma_2-2}{p}$ ,  $z' = \frac{\gamma_2-\gamma_1+1}{p}$ ,  $x' = \gamma_1 - \gamma_2 + \frac{\gamma_2-\gamma_1+1}{p}$ . Now we can easily get that  $R$  is an  $(n+2, p, n, \frac{n-\gamma_2-2}{p} + \gamma_2, 0, \frac{n-\gamma_1-1}{p} + \gamma_1, \frac{n-\gamma_2-2}{p}, \frac{n-\gamma_1-1}{p})$ -PDPDS by using (2.3) and (2.6).

On the other hand,  $(n+2, p, n, \frac{n-\gamma_2-2}{p} + \gamma_2, 0, \frac{n-\gamma_1-1}{p} + \gamma_1, \frac{n-\gamma_2-2}{p}, \frac{n-\gamma_1-1}{p})$ -PDPDS satisfies the diagram (2.4) for any character  $\chi$  on  $G$ . So we get that  $\underline{a} = (a_0, a_1, \dots, a_{n+1}, \dots)$  is an NPS of type  $(\gamma_1, \gamma_2)$ .  $\square$

Theorem 2.18 gives a necessary condition on the existence of a NPS with two distinct out-of-phase autocorrelation coefficients. Moreover this theorem gives bound on  $\gamma_1, \gamma_2$ . We state this condition in Corollary 2.19. After that we give an example of Theorem 2.18.

**Corollary 2.19.** *If  $\underline{a}$  is an almost  $p$ -ary NPS of type  $(\gamma_1, \gamma_2)$  and length  $n + 2$ , then  $p$  divides  $n - \gamma_2 - 2$  and  $n - \gamma_1 - 1$ . And there exists an almost  $p$ -ary sequence of type  $(\gamma_1, \gamma_2)$  and period  $n + 2$  with two consecutive zero-symbols for  $-\mu_1 \leq \gamma_2 \leq n - 2$  and  $-\mu_2 \leq \gamma_1 \leq n - 1$ .*

**Example 2.20.** *Sequence  $\underline{a} = (0, 0, \zeta_3, \zeta_3, \zeta_3, \dots)$  is an almost 3-ary NPS of type  $(2, 1)$  and  $R$  is an  $(3 + 2, 3, 3, \frac{3-1-2}{3} + 1, 0, \frac{3-2-1}{3} + 2, \frac{3-1-2}{3}, \frac{3-2-1}{3}) = (5, 3, 3, 1, 0, 2, 0, 0)$  PDPDS in  $\mathbb{Z}_5 \times \mathbb{Z}_3$ . Similarly,  $\underline{a} = (0, 0, \zeta_3^2, \zeta_3, 1, \zeta_3, \zeta_3^2, \dots)$  is an almost 3-ary NPS of type  $(-2, 0)$  and  $R$  is an  $(7, 3, 5, 1, 0, 0, 1, 2)$  PDPDS in  $\mathbb{Z}_7 \times \mathbb{Z}_3$ .*

**Theorem 2.21.** *Let  $R, G, H, N, n, p, b_i$  for  $i = 2, 3, \dots, n + 1$  be defined as in Definition 2.14 such that  $p \neq 2$ . If  $R$  is a PDPDS in  $G$  relative to  $H$  and  $N$ , then  $b_2 = b_{n+1}, b_3 = b_n, \dots, b_{\lfloor \frac{n+2}{2} \rfloor} = b_{\lceil \frac{n+2}{2} \rceil + 1}$ .*

*Proof.* Assume that  $R = \{(2, b_2), (3, b_3), \dots, (n+1, b_{n+1})\}$  is PDPDS and  $p \neq 2$ . If we consider to difference table of  $R$ , then we get  $\{(1, b_3 - b_2), (1, b_4 - b_3), \dots, (1, b_{n+1} - b_n), (2, b_4 - b_3), (2, b_5 - b_3), \dots, (2, b_{n+1} - b_{n-1}), \dots, (n+1, b_2 - b_3), (n+1, b_3 - b_4), \dots, (n+1, b_n - b_{n+1})\}$  without identity. Firstly,  $(b_3 - b_2) + (b_4 - b_3) + \dots + (b_{n+1} - b_n)$  and  $(b_4 - b_3 + (b_5 - b_3) + \dots + (b_{n+1} - b_{n-1}))$  and  $(b_2 - b_3) + (b_3 - b_4) + \dots + (b_n - b_{n+1})$  equations must be zero in  $\mathbb{Z}_p$  because  $R$  is PDPDS. Therefore, we get easily  $b_{n+1} = b_2, b_n = b_3$  and so on.  $\square$

We present an important property of an almost  $p$ -ary sequence of type  $(\gamma_1, \gamma_2)$  and period  $n + 2$  with two consecutive zero-symbols.

**Corollary 2.22.** *Let  $p$  be an odd prime number. If there exist an almost  $p$ -ary sequence of type  $(\gamma_1, \gamma_2)$  and period  $n + 2$  with two consecutive zero-symbols then this sequence is symmetric except for zero entries.*

**Example 2.23.**  $\underline{a}_1 = (0, 0, \zeta_3^2, 1, \zeta_3^2, \dots)$  and  $\underline{a}_2 = (0, 0, \zeta_3^2, \zeta_3, 1, \zeta_3, \zeta_3^2, \dots)$  sequences are almost 3-ary NPS of type  $(\gamma_1, \gamma_2)$  with 2 zero-symbols. These sequences are symmetric except for zero entries.

*Remark 2.24.* The converse of Corollary 2.22 is not correct. That is, a symmetric sequence of period  $n + 2$  with two consecutive zero-symbols do not necessarily have to be

an almost  $p$ -ary sequence of type  $(\gamma_1, \gamma_2)$  and period  $n + 2$  with two consecutive zero-symbols. For instance,  $\underline{a}_1 = (0, 0, \zeta_3, \zeta_3^2, \zeta_3, \zeta_3^2, \zeta_3, \dots)$ ,  $\underline{a}_2 = (0, 0, \zeta_3^2, \zeta_3^2, 1, \zeta_3^2, \zeta_3^2, \dots)$ , and  $\underline{a}_3 = (0, 0, \zeta_3^2, 1, \zeta_3^2, 1, \zeta_3^2, \dots)$  3-ary sequences of period 7 with two consecutive zero-symbols are symmetric except for zero entries, but these sequences are not almost 3-ary sequences of type  $(\gamma_1, \gamma_2)$  and period 7 with two consecutive zero-symbols.

We know that  $\lambda_1 + (p - 1)\mu_1 = n - 2$  and  $\lambda_3 + (p - 1)\mu_3 = n - 1$  from definition of PDPDS. If  $n$  is odd, then  $\lambda_1$  is odd and  $\lambda_3$  is even. If  $n$  is even,  $\lambda_1$  is even and  $\lambda_3$  is odd. On the other hand, we know that an almost  $p$ -ary sequence of type  $(\gamma_1, \gamma_2)$  and period  $n + 2$  with two consecutive zero-symbols is symmetric except for zero entries. Therefore, if  $n$  is odd, then  $\lambda_1 \geq 1$  because  $(2, 0), (3, 0), \dots, (n, 0)$  is one of diagonal of difference table of  $R$  and so if  $n$  is even, then  $\lambda_1 \geq 2$ ,  $\lambda_3 \geq 1$  because  $(3, 0), (5, 0), \dots, (n - 1, 0), (3, 0), (5, 0), \dots, (n - 1, 0), (1, 0), (n + 1, 0)$  is one of diagonal of difference table of  $R$ . For all these reasons, we get the following result.

**Proposition 2.25.** *Let  $\underline{a}$  is an almost  $p$ -ary sequence of type  $(\gamma_1, \gamma_2)$  and period  $n + 2$  with two consecutive zero-symbols. If  $n$  is odd, then  $\lambda_1 = 2k + 1$ ,  $k \in \mathbb{Z}^+ \cup \{0\}$  and if  $n$  is even, then  $\lambda_1 = 2k$ ,  $k \in \mathbb{Z}^+$ .*

Next we obtain a generalization of a well known theorem on difference sets, see [18, Lemma VI.5.4] or [11, Proposition 1].

**Proposition 2.26.** *Let  $R$  be a  $(n + 2, p, n, \frac{n - \gamma_2 - 2}{p} + \gamma_2, 0, \frac{n - \gamma_1 - 1}{p} + \gamma_1, \frac{n - \gamma_2 - 2}{p}, \frac{n - \gamma_1 - 1}{p})$ -PDPDS in  $G$  relative to  $H$  and  $N$ . Let  $s_i$  be the number of those whose elements are  $i$  in the second components of  $R$  for  $i \in \mathbb{Z}_p$ . Then*

$$\sum_{j=0}^{p-1} s_j^2 = \left( \frac{n - \gamma_2 - 2}{p} + \gamma_2 \right) (n - 1) + \left( \frac{n - \gamma_1 - 1}{p} + \gamma_1 \right) 2 + n \quad (2.9)$$

and

$$\sum_{j=0}^{p-1} s_j s_{j-i} = \left( \frac{n - \gamma_2 - 2}{p} \right) (n - 1) + \left( \frac{n - \gamma_1 - 1}{p} \right) 2 \quad (2.10)$$

for each  $i = 1, 2, \dots, \lceil \frac{p-1}{2} \rceil$ , here  $j - i$  is computed modulo  $p$ .

*Proof.* Let  $\psi$  the map from  $G = H \times N$  to  $N$  sending  $(a, i)$  to  $i$ . Let  $A$  be the set consisting of  $\psi(a, i)$  to all elements of the  $R \subset G$  set. By reordering on  $A$  we have

$$A = \{ * \underbrace{0, 0, \dots, 0}_{s_0}, \underbrace{1, 1, \dots, 1}_{s_1}, \underbrace{2, 2, \dots, 2}_{s_2}, \dots, \underbrace{p - 1, p - 1, \dots, p - 1}_{s_{p-1}} * \}.$$

So,

$$s_0 = |\{(b, i) \in R : i = 0\}|, \dots, s_{p-1} = |\{(b, i) \in R : i = p - 1\}|$$

and

$$s_0 + s_1 + s_2 + \dots + s_{p-1} = |R| = n. \quad (2.11)$$

Let  $\mathcal{T}_i$  be defined as

$$\mathcal{T}_i = \{(\beta_1, \beta_2) \in R \times R : \beta_1 \neq \beta_2 \text{ and } \psi(\beta_1 - \beta_2) = i\} \subset R \times R.$$

As  $R$  is a  $(n+2, p, n, \frac{n-\gamma_2-2}{p} + \gamma_2, 0, \frac{n-\gamma_1-1}{p} + \gamma_1, \frac{n-\gamma_2-2}{p}, \frac{n-\gamma_1-1}{p})$  PDPDS, for the cardinality  $|\mathcal{T}_i|$  of  $\mathcal{T}_i$ , using definition of PDPDS, we obtain that

$$|\mathcal{T}_i| = \begin{cases} \left(\frac{n-\gamma_2-2}{p} + \gamma_2\right)(n-1) + \left(\frac{n-\gamma_1-1}{p} + \gamma_1\right)2, & i = 0 \\ \left(\frac{n-\gamma_2-2}{p}\right)(n-1) + \left(\frac{n-\gamma_1-1}{p}\right)2, & 1 \leq i \leq p-1 \end{cases} \quad (2.12)$$

Let define as  $\mathcal{T}_{i,j} = \{(\beta_1, \beta_2) \in \mathcal{T}_i : \psi(\beta_1) = j\} \subset \mathcal{T}_i$  for  $0 \leq i, j \leq p-1$ . Then we have,

$$|\mathcal{T}_i| = \sum_{j=0}^{p-1} |\mathcal{T}_{i,j}|. \quad (2.13)$$

For  $1 \leq i \leq p-1$  and  $0 \leq j \leq p-1$ , we determine  $\mathcal{T}_{i,j}$ . We know that  $(\beta_1, \beta_2) \in \mathcal{T}_{i,j}$  if only if  $\beta_1 \in R$ ,  $\psi(\beta_1) = j$  and  $\beta_2 \in R$ ,  $\psi(\beta_2) = j - i$ . Therefore we get that,

$$|\{\beta_1 \in R : \psi(\beta_1) = j\}| = s_j \text{ and } |\{\beta_2 \in R : \psi(\beta_2) = j - i\}| = s_{j-i},$$

here  $j - i$  is computed modulo  $p$ . Hence we obtain that

$$\left(\frac{n-\gamma_2-2}{p}\right)(n-1) + \left(\frac{n-\gamma_1-1}{p}\right)2 = \sum_{j=0}^{p-1} s_j s_{j-i}. \quad (2.14)$$

with using (2.12) and (2.13). Remark that it is enough to consider the subset of equation in (2.14) corresponding to  $1 \leq i \leq \lceil \frac{p-1}{2} \rceil$  because each equation in (2.14) with  $\lceil \frac{p-1}{2} \rceil \leq i \leq p-1$  is the same as an equation in (2.14) with  $1 \leq i \leq \lceil \frac{p-1}{2} \rceil$ .

For  $0 \leq j \leq p-1$ , we determine  $\mathcal{T}_{0,j}$ . We know that  $(\beta_1, \beta_2) \in \mathcal{T}_{0,j}$  if only if  $\beta_1 \in R$ ,  $\psi(\beta_1) = j$  and  $\beta_2 \in R$ ,  $\psi(\beta_2) = j$  and  $\beta_1 \neq \beta_2$ . Therefore we get that  $|\mathcal{T}_{0,j}| = s_j(s_j - 1)$  for  $0 \leq j \leq p-1$ . Hence using (2.11), (2.12) and (2.13) we conclude that

$$\left(\frac{n-\gamma_2-2}{p} + \gamma_2\right)(n-1) + \left(\frac{n-\gamma_1-1}{p} + \gamma_1\right)2 = \sum_{j=0}^{p-1} s_j(s_j - 1) = \sum_{j=0}^{p-1} s_j^2 - n$$

and therefore

$$\sum_{j=0}^{p-1} s_j^2 = \left(\frac{n-\gamma_2-2}{p} + \gamma_2\right)(n-1) + \left(\frac{n-\gamma_1-1}{p} + \gamma_1\right)2 + n.$$

□

**Example 2.27.**  $R$  is a  $(7, 3, 5, 1, 0, 0, 1, 2)$  PDPDS in  $\mathbb{Z}_7 \times \mathbb{Z}_3$  for almost  $\underline{a} = (0, 0, \zeta_3^2, \zeta_3, 1, \zeta_3, \zeta_3^2, \dots)$  3-ary NPS of type  $(-2, 0)$ . Then,  $s_0 = 1, s_1 = 2, s_2 = 2$  and so we obtained that

$$s_0^2 + s_1^2 + s_2^2 = 1 + 2^2 + 2^2 = 9,$$

$$s_0s_1 + s_1s_0 + s_2s_0 = 1 * 2 + 2 * 1 + 2 * 2 = 8$$

where  $i = \lceil \frac{3-1}{2} \rceil = 1$ . On the other hand, we can get these results from the equation (2.9) and the equation (2.10).

$$\sum_{j=0}^{3-1} s_j^2 = \left( \frac{n-0-2}{3} + 0 \right) (5-1) + \left( \frac{5-(-2)-1}{3} + (-2) \right) 2 + 5 = 9$$

and

$$\sum_{j=0}^{3-1} s_j s_{j-i} = \left( \frac{5-0-2}{3} \right) (5-1) + \left( \frac{5-(-2)-1}{3} \right) 2 = 8.$$

Using Propositions 2.17 and 2.26, we get the following result.

**Corollary 2.28.** Let  $R$  be a  $(n+2, p, n, \lambda_1, \lambda_2, \lambda_3, \mu_1, \mu_2) = (n+2, p, n, \frac{n-\gamma_2-2}{p} + \gamma_2, 0, \frac{n-\gamma_1-1}{p} + \gamma_1, \frac{n-\gamma_2-2}{p}, \frac{n-\gamma_1-1}{p})$  PDPDS in  $G$  relative to  $H$  and  $N$ . Let  $s_i$  be the number of those whose elements are  $i$  in the second components of  $R$  for  $i \in \mathbb{Z}_p$ . Then

$$(p-1) \left( \sum_{j=0}^{p-1} s_j s_{j-i} \right) + \sum_{j=0}^{p-1} s_j^2 = n^2 \quad (2.15)$$

for each  $i = 1, 2, \dots, \lceil \frac{p-1}{2} \rceil$ , here  $j-i$  is computed modulo  $p$ .

*Proof.* We multiply (2.9) by  $p-1$  and add to (2.10), so we get

$$\begin{aligned} (p-1) \left( \sum_{j=0}^{p-1} s_j s_{j-i} \right) + \sum_{j=0}^{p-1} s_j^2 &= \left( \left( \frac{n-\gamma_2-2}{p} \right) (n-1) + \left( \frac{n-\gamma_1-1}{p} \right) 2 \right) (p-1) \\ &\quad + \left( \frac{n-\gamma_2-2}{p} + \gamma_2 \right) (n-1) + \left( \frac{n-\gamma_1-1}{p} + \gamma_1 \right) 2 + n. \end{aligned}$$

Equivalently, we have

$$\begin{aligned} (p-1) \left( \sum_{j=0}^{p-1} s_j s_{j-i} \right) + \sum_{j=0}^{p-1} s_j^2 &= (\mu_1(n-1) + \mu_2 2)(p-1) + \lambda_1(n-1) + \lambda_3 2 + n \\ &= (n-1)(\lambda_1 + (p-1)\mu_1) + 2(\lambda_3 + (p-1)\mu_2) + n. \end{aligned}$$

Finally, by Proposition 2.17, we get the result

$$(p-1) \left( \sum_{j=0}^{p-1} s_j s_{j-i} \right) + \sum_{j=0}^{p-1} s_j^2 = n^2 - n + n = n^2.$$

□



**Example 2.29.** We consider the sequence in Example 2.27,  $\underline{a} = (0, 0, \zeta_3^2, \zeta_3, 1, \zeta_3, \zeta_3^2, \dots)$ .

Hence, we get

$$(3-1)(s_0s_1 + s_1s_0 + s_2s_0) + s_0^2 + s_1^2 + s_2^2 = 8 * 2 + 9 = 5^2$$

On the other hand, we can get this result from the equation 2.15.

$$(3-1) \left( \sum_{j=0}^{3-1} s_j s_{j-i} \right) + \sum_{j=0}^{3-1} s_j^2 = 5^2.$$

Below we prove a bound on  $\gamma_2$  for the existence of a  $p$ -ary NPS of type  $(\gamma_1, \gamma_2)$  by using Proposition 2.6.

**Theorem 2.30.** Let  $p$  be an odd prime number,  $n \in \mathbb{Z}^+$ ,  $\gamma_1, \gamma_2 \in \mathbb{Z}$  such that  $n - \gamma_2 - 2 = k_1p$  and  $n - \gamma_1 - 1 = k_2p$  for some  $k_1, k_2 \in \mathbb{N}$ . Then, there does not exist an almost  $p$ -ary sequence of type  $(\gamma_1, \gamma_2)$  and period  $n + 2$  with two consecutive zero-symbols for  $\gamma_2 \leq \left\lfloor \frac{-pk_1 - 4 + \sqrt{p^2k_1^2 - 4pk_1 + 8pk_2}}{2} \right\rfloor$ .

*Proof.* Assume there exists an almost  $p$ -ary sequence of length  $n$  and type  $(\gamma_1, \gamma_2)$  such that  $\gamma_2 > \left\lfloor \frac{-pk_1 - 4 + \sqrt{p^2k_1^2 - 4pk_1 + 8pk_2}}{2} \right\rfloor$ . Set  $n - \gamma_2 - 2 = pk_1$  and  $n - \gamma_1 - 1 = pk_2$  in (2.9), and so we get

$$\sum_{j=0}^{p-1} s_j^2 = pk_1\gamma_2 + 3pk_1 + pk_1^2 + \gamma_2k_1 + k_1 + 2k_2 - 2pk_2 + (\gamma_2 + 2)^2. \quad (2.16)$$

On the other hand we know that  $s_0 + s_1 + \dots + s_{p-1} = n = pk_1 + \gamma_2 + 2$ , that is,

$$\sum_{j=0}^{p-1} s_j = pk_1 + \gamma_2 + 2. \quad (2.17)$$

Hence (2.17) gives that

$$\sum_{j=0}^{p-1} s_j^2 \geq \left( \frac{pk_1 + \gamma_2 + 2}{p} \right)^2 p = pk_1^2 + 2k_1(\gamma_2 + 2) + \frac{(\gamma_2 + 2)^2}{p}. \quad (2.18)$$

We consider (2.16) and (2.18) together. And we get

$$pk_1^2 + 2k_1(\gamma_2 + 2) + \frac{(\gamma_2 + 2)^2}{p} \leq pk_1\gamma_2 + 3pk_1 + pk_1^2 + \gamma_2k_1 + k_1 + 2k_2 - 2pk_2 + (\gamma_2 + 2)^2.$$

Equivalently, we have

$$(1-p)((\gamma_2 + 2)^2 + pk_1(\gamma_2 + 2) + pk_1 - 2pk_2) \leq 0 \quad (2.19)$$

Firstly, (2.19) holds if  $\gamma_2 \leq \frac{-pk_1 - \sqrt{p^2k_1^2 - 4pk_1 + 8pk_2}}{2} - 2 < -pk_1 - 1$ . But this contradicts to  $n - \gamma_2 - 2 = pk_1$ . Secondly, (2.19) holds if  $\gamma_2 \geq \frac{-pk_1 + \sqrt{p^2k_1^2 - 4pk_1 + 8pk_2}}{2} - 2$ , but this contradicts to the beginning assumption.  $\square$

Table 2.3: Non-existence results on NPS by Theorem 2.30 for  $n=15$

p=5				p=5				p=5				p=3			
$\gamma_1$	$\gamma_2$	B	Comments	$\gamma_1$	$\gamma_2$	B	Comments	$\gamma_1$	$\gamma_2$	B	Comments	$\gamma_1$	$\gamma_2$	B	Comments
-10	-8	-1	not exist	-4	1	-1		2	7	0		-6	-7	-2	not exist
-10	-5	-1	not exist	-4	4	0		2	10	1		-6	-2	-1	not exist
-10	-2	-1	not exist	-4	7	1		5	-8	-3	not exist	-6	3	0	
-10	1	0		-4	10	2		5	-5	-2	not exist	-6	8	1	
-10	4	1		-1	-8	-2	not exist	5	-2	-2	not exist	-1	-7	-2	not exist
-10	7	2		-1	-5	-2	not exist	5	1	-2		-1	-2	-2	not exist
-10	10	3		-1	-2	-2	not exist	5	4	-2		-1	3	-1	
-7	-8	-2	not exist	-1	1	-1		5	7	-1		-1	8	0	
-7	-5	-1	not exist	-1	4	-1		5	1	0		4	-7	-2	not exist
-7	-2	-1	not exist	-1	7	0		8	-8	-3	not exist	4	-2	-2	not exist
-7	1	0		-1	10	1		8	-5	-3	not exist	4	3	-2	
-7	7	1		2	-8	-2	not exist	8	-2	-3		4	8	0	
-7	10	2		2	-5	-2	not exist	8	1	-2		9	-7	-3	not exist
-4	-8	-2	not exist	2	-2	-2	not exist	8	4	-2		9	-2	-3	
-4	-5	-2	not exist	2	1	-2		8	7	-2		9	3	-2	
-4	-2	-1	not exist	2	4	-1		8	10	-1		9	8	-2	

We tabulate some nonexistence results obtained by Theorem 2.30 for  $n = 15$ ,  $-10 \leq \gamma_1, \gamma_2 \leq 10$ ,  $p = 3$  and  $p = 5$  respectively in Table 2.3, where  $B$  is the upper bound on  $\gamma_2$  given in Theorem 2.30. Pairs  $(\gamma_1, \gamma_2)$  not included in Table 2.3 are excluded by Corollary 2.19. The empty rows in the table are undecided cases. It is seen that the case  $\gamma_2 = -2$  and  $B = -3$  appears in the table, but Theorem 2.30 does not say anything about the status of its existence. Actually, it is easily seen that the upper bound on  $\gamma_2$  in Theorem 2.30 is at least  $-3$ . Hence we have the following corollary.

**Corollary 2.31.** *Let  $p$  be an odd prime number and  $n \in \mathbb{Z}^+$ . Then there does not exist an almost  $p$ -ary sequence of type  $(\gamma_1, \gamma_2)$  and period  $n + 2$  with two consecutive zero-symbols for  $\gamma_2 \leq -3$ .*

We now study the notion of multiplier of a PDPDS. Let  $M$  be a PDPDS in  $G$  relative to  $H$  and  $P$ . Define  $M^{(m)} = \{mr : r \in R\} \subset G$  for  $m \in \mathbb{Z}$ .  $m$  is called a multiplier of  $M$  if there exist  $g \in G$  such that  $M^{(t)} = M + g \subset G$  for some  $m \in \mathbb{Z}$  such that  $\gcd(m, |G|) = 1$ . The following result gives us a multiplier subset of a PDPDS.

**Proposition 2.32.** *Let  $R$  be a  $(n + 2, p, n, \frac{n-\gamma_2-2}{p} + \gamma_2, 0, \frac{n-\gamma_1-1}{p} + \gamma_1, \frac{n-\gamma_2-2}{p}, \frac{n-\gamma_1-1}{p})$  PDPDS in  $G$  relative to  $H$  and  $P$ . If  $m$  is a multiplier of  $R$ , then  $m \equiv \pm 1 \pmod{n + 2}$ .*

*Proof.* Let  $R = \{(2, a_1), (3, a_2), \dots, (n + 1, a_n)\}$  be a PDPDS in  $G$  relative to  $H$  and  $P$ . Let  $R_l$  denote the set of first components of elements in  $R$ , so  $R_l = \{2, 3, \dots, n + 1\}$ . Similarly  $R_l^{(m)}$ . We assume that  $t$  is a multiplier of  $R$ . For  $g \in \{1, 2, \dots, n\}$  we get  $R_l + g = 0$ . We know that  $\gcd(m, |G|) = 1$ , so  $\{0\}$  can never be found in  $R_l^{(m)}$ . Then  $g$  must be in  $\{0, n + 1\}$ .

Firstly if  $g = \{n + 1\}$ , then we get  $R_l + g = \{1, 2, \dots, n\}$ . We can use the group notion to find the relation between  $R$  and  $R^{(m)}$ . We know that  $R_l = \mathbb{Z}_{n+2} - \{0, 1\}$  so  $R_l^{(m)} = \mathbb{Z}_{n+2} - \{0, m\}$ . Then, we get

$$R_l^{(m)} = R_l - \{m\} + \{1\}. \quad (2.20)$$

by last two equations. We consider together to  $R_l$ ,  $R_l^{(m)}$  and (2.20), we get  $m \equiv n + 1 \equiv -1 \pmod{(n + 2)}$  one of the statement of result. Finally, we show the other statement of result. If  $g = \{0\}$ , then we get  $R_l + g = \{2, 3, \dots, n+1\}$ . It is now clear that  $m \equiv 1 \pmod{(n+2)}$ .  $\square$

## 2.4 Conclusion

In this chapter, we proved a lower and an upper bounds on the number of distinct out-of-phase autocorrelation coefficients of an almost  $p$ -ary sequence of period  $n + s$  with  $s$  consecutive zero-symbols. Theorem 2.10 shows that the number of distinct out-of-phase autocorrelation coefficients is between  $\min\{s, p, n\}$  and  $n - 1 + \min\{n, s\}$ . Therefore one can not get an NPS of type  $\gamma$  by adding extra zero-symbols at consecutive positions. We next prove in Theorem 2.18 that a  $p$ -ary NPS of type  $(\gamma_1, \gamma_2)$  is equivalent to a PDPDS. Then, we obtain that they only exist when  $p$  divides  $n - \gamma_2 - 2$  and  $n - \gamma_1 - 1$ . We give in Theorem 2.30 a necessary condition on  $\gamma_2$  for the existence of an almost  $p$ -ary NPS of type  $(\gamma_1, \gamma_2)$ . In particular we show that they don't exist for  $\gamma_2 \leq -3$ .

### 3 APPLICATIONS

There is also a close relationship between sequences and cryptography due to the relationship between Hadamard matrices. In particular, the functions called *bent functions* are used in block cipher cryptosystems, substitution boxes, and can be constructed with Butson-Hadamard matrices. Therefore, we start with the definition of a Butson-Hadamard matrix.

*Code Division Multiple Access (CDMA)* is the system that provides high-quality communication with orthogonal codes (sequences). Actually, CDMA system is used as third generation (3G) communication technology. In Code Division Multiple Access (CDMA), sequences with ideal autocorrelation are important because a signal should not be affected by other signals in order to provide high-quality communication. In CDMA, each user has his/her own code (sequence) and autocorrelation or crosscorrelation of this codes must be zero or nearly zero. But, there is not enough orthogonal code. Hence, in Section 3.2,  $p$ -ary sequences with  $s$  consecutive zero-symbols of type  $(\gamma_1, \gamma_2)$  application to the bit-error-rate (BER) on CDMA are presented. The simulation results on BER analysis of CDMA with almost  $p$ -ary NPS is given in Section 3.2. The *bit-error-rate* is the ratio of the number of different bits between the bits sent and the bits received, to the total number of bits sent. It is seen that although almost  $p$ -ary NPSs don't have better simulation results than perfect sequences, they serve a large set of sequences with almost ideal autocorrelation coefficients.

The rest of this chapter is organized as follows. In Section 3.1.1, we define  $(\gamma_1, \gamma_2)$ -near *Butson-Hadamard (resp. Conference)* matrix (see Definition 3.3). In Section 3.1.2, the equivalence between an almost  $p$ -ary NPS of type  $(\gamma_1, \gamma_2)$  and a  $(\gamma_1, \gamma_2)$ -near Conference matrix and a cryptographic function is studied and some examples of cryptographic function are presented (see Table 3.1). In Section 3.2, we study CDMA structure on the Rayleigh channel under additive white Gaussian noise (AWGN) as a communication application (see Figure 3.1), and we use the almost  $p$ -ary sequences in this scenario. On this structure, bit-error-rate is calculated and simulation results are given (see Figures 3.2-3.5).

## 3.1 Cryptographic Application

### 3.1.1 Butson-Hadamard Matrices

We first give the definition of a Butson-Hadamard matrix and a near Butson-Hadamard matrix.

A Hadamard matrix is an  $(v \times v)$  matrix with entries in  $\mathbb{Z}_2$  such that  $H\bar{H}^T = vI$ . A square matrix  $H = (h_{ij})$  of order  $v$  is called *circulant* if  $h_{i+1,j+1} = h_{i,j}$  for all  $0 \leq i, j < v$ .

$$A = \begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{bmatrix}$$

In the above examples, the matrix  $A$  is a Hadamard matrix of order 2 and the matrix  $B$  is a circulant matrix of order 5, where  $-$  represents  $-1$ . Let  $p$  be a prime and  $\mathcal{E}_p = \{1, \zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}\}$ . The identity matrix is denoted by  $I$  and all one matrix denoted by  $J_1$ . Moreover,  $J_2$  and  $J_3$  are defined as

$$J_2 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \dots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & \dots & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & \dots & 1 & 0 \end{bmatrix}, \quad J_3 = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & \dots & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & \dots & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & \dots & 1 & 1 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \dots & \ddots & \vdots \\ 1 & 1 & 1 & 0 & 0 & \dots & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & \dots & 0 & 0 \end{bmatrix}.$$

Then it is obtained that  $J_1 = J_2 + J_3 + I$ .

**Definition 3.1.** [19] Let  $H$  be a square matrix of order  $v$  with entries in  $\mathcal{E}_p$ . If  $H\bar{H}^T = vI$ , then  $H$  is called *Butson-Hadamard matrix* and it is denoted by  $BH(v, p)$ . In particular, if  $p = 2$ , then  $BH(v, p)$  is called *Hadamard matrix*. If  $H\bar{H}^T = (v - \gamma)I + \gamma J_1$  for  $\gamma \in \mathbb{R} \cap \mathbb{Z}[\zeta_p]$ , then  $H$  is called  $\gamma$  *near Butson-Hadamard matrix*. Similarly, it is denoted by  $BH_\gamma(v, p)$ .

The analysis of  $\gamma$  near Butson-Hadamard matrices is given in [19].

**Example 3.2.** [19, Example 5] The following matrix  $H$  is an  $BH_\gamma(5, 5)$  for  $\gamma = -\zeta_5^3 - \zeta_5^2 + 2$ , where  $\zeta_5$  is a 5-th root of unity,

$$H = \begin{bmatrix} 1 & 1 & -\zeta_5^2 & 1 & 1 \\ 1 & 1 & 1 & -\zeta_5^2 & 1 \\ 1 & 1 & 1 & 1 & -\zeta_5^2 \\ -\zeta_5^2 & 1 & 1 & 1 & 1 \\ 1 & -\zeta_5^2 & 1 & 1 & 1 \end{bmatrix}.$$

We extend Definition 3.3 given for  $\gamma$ -near Butson-Hadamard matrices to  $(\gamma_1, \gamma_2)$ -near Butson-Hadamard matrices and near Conference matrices in the following.

**Definition 3.3.** A  $(\gamma_1, \gamma_2)$ -near Butson-Hadamard matrix is a square matrix  $H$  of order  $n+2$  with entries in  $\mathcal{E}_p$  such that  $H\bar{H}^T = (n+2)I + \gamma_1 J_2 + \gamma_2 J_3$ , and denoted by  $BH_{(\gamma_1, \gamma_2)}(n+2, p)$ . Similarly, a  $(\gamma_1, \gamma_2)$  near Conference matrix is a square matrix  $C$  of order  $n+2$  with entries in  $\mathcal{E}_p \cup \{0\}$  such that  $C\bar{C}^T = nI + \gamma_1 J_2 + \gamma_2 J_3$ , and denoted by  $C_{(\gamma_1, \gamma_2)}(n+2, p)$ .

In this thesis, we study only circulant  $(\gamma_1, \gamma_2)$ -near Conference matrices with two leading zero entries. Please note that this kind of matrices are equivalent to nearly perfect sequences of type  $(\gamma_1, \gamma_2)$  by setting the first row of the matrix with the sequence itself.

**Example 3.4.** The following matrix

$$C = \begin{bmatrix} 0 & 0 & \zeta_5 & \zeta_5^2 & \zeta_5 \\ \zeta_5 & 0 & 0 & \zeta_5 & \zeta_5^2 \\ \zeta_5^2 & \zeta_5 & 0 & 0 & \zeta_5 \\ \zeta_5 & \zeta_5^2 & \zeta_5 & 0 & 0 \\ 0 & \zeta_5 & \zeta_5^2 & \zeta_5 & 0 \end{bmatrix}$$

is an  $C_{(\gamma_1, \gamma_2)}(5, 5)$  for  $\gamma_1 = \zeta_5^2 + \zeta_5^3$ ,  $\gamma_2 = 1$  with  $|\gamma_1| = 1.61$ ,  $|\gamma_2| = 1$ . Therefore, it satisfies

$$C\bar{C}^T = 3 \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} + (\zeta_5^2 + \zeta_5^3) \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} + 1 \begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

### 3.1.2 Generalized Bent Functions

In this section, we give a method for obtaining a generalized bent function from an almost  $p$ -ary NPS of type  $(\gamma_1, \gamma_2)$  and period  $n+2$  with two consecutive zero symbols. Before that we will give the definition of a Walsh transform, because the non-linearity of a function can be calculated by its Walsh spectrum. Then we will give the definition of generalized bent function. Let  $q$  be power of a prime number  $p$ .

For  $X, Y \in (\mathbb{Z}_p)^n$ , the dot product or scalar product of two vectors  $X = [x_1, x_2, \dots, x_n]$  and  $Y = [y_1, y_2, \dots, y_n]$  is defined by  $\sum_{i=1}^n x_i y_i \pmod p$  and denoted by  $\langle X, Y \rangle$ .

The nonlinearity of a Boolean function is the minimum of its distance from all affine functions.

$$nl(f) = \min\{d(f, A_n)\}$$

where  $A_n$  is the set of all affine functions in all Boolean functions of  $n$  variables. We take as  $F(x) = (-1)^{f(x)}$ .

$$\begin{aligned}\hat{F}(x) &= \sum_{y \in (\mathbb{Z}_2)^n} (-1)^{\langle x, y \rangle} (-1)^{f(x)} \\ &= \sum_{f(x) = \langle x, y \rangle} 1 - \sum_{f(x) \neq \langle x, y \rangle} 1 \\ &= 2^n - 2d(f, \langle x, y \rangle).\end{aligned}$$

So,  $d(f, \langle x, y \rangle) = 2^{n-1} - \frac{1}{2}\hat{F}(x)$  is obtained. Hence, the nonlinearity of a Boolean function  $f$  on  $\mathbb{Z}_2$  is  $nl(f) = 2^{n-1} - \frac{1}{2} \max\{|\hat{F}(x)| : x \in \mathbb{Z}_2^n\}$ .

**Definition 3.5.** [4] Let  $F$  be functions such that  $F : (\mathbb{Z}_q)^n \rightarrow \mathbb{C}$ . The Walsh transform  $\hat{F} : (\mathbb{Z}_q)^n \rightarrow \mathbb{C}$  of  $F$  is defined by

$$\hat{F}(x) = \sum_{y \in (\mathbb{Z}_q)^n} \zeta_q^{\langle x, y \rangle} F(y)$$

for all  $x \in (\mathbb{Z}_q)^n$ , where  $\langle, \rangle$  is dot product.

**Definition 3.6.** [4] Let  $f$  be function such that  $f : (\mathbb{Z}_q)^n \rightarrow \mathbb{Z}_q$ . The  $F : (\mathbb{Z}_q)^n \rightarrow \mathbb{C}$  function is defined by

$$F(x) = \zeta_q^{f(x)}$$

for all  $x \in (\mathbb{Z}_q)^n$ . If  $|\hat{F}(x)| = q^{n/2}$  for all  $x \in (\mathbb{Z}_q)^n$  then  $f$  is called a generalized bent function (GBF).

In Theorem 3.7, a well known connection between Butson-Hadamard matrices and generalized bent functions is given.

**Theorem 3.7.** [4] Let  $f$  and  $F$  be defined as in Definition 3.6. Define the matrix  $H_f = (h_{x,y})$  and  $h_{x,y} = F(x - y)$  for all  $x, y \in (\mathbb{Z}_q)^n$ .  $f$  is a GBF if and only if  $H_f$  is a BH( $q, q$ ) matrix.

Now we examine the functions corresponding to almost  $p$ -ary NPS of type  $(\gamma_1, \gamma_2)$ . Note that in Theorem 3.7, only the first row of a BH matrix is enough to obtain the truth-table of a function. Hence we can convert a sequence into a function's truth-table. However, since we work  $p$ -ary sequence of type  $(\gamma_1, \gamma_2)$  and period  $n + 2$  with two consecutive zero-symbols,

we can not directly obtain the truth-table values. Thus, we first interpolate the function  $f$  of largest degree from an almost  $p$ -ary NPS except two zero symbols. Then we get the truth-table, and so the Walsh transform of  $f$  is calculated by Definition 3.5.

**Example 3.8.** We choose a NPS  $\underline{a} = (0, 0, \zeta_5, \zeta_5^2, \zeta_5, \dots)$ . We look for a function  $f : \mathbb{Z}_5 \rightarrow \mathbb{Z}_5$ . We first set  $f(3) = 1$ ,  $f(2) = 2$  and  $f(1) = 1$  by using the direction of Theorem 3.7. By interpolating the function  $f$  of degree 2, we get  $f = 3x^2 + 3x$ , and so  $f(0) = f(4) = 0$ . Thus the truth-table is  $(0, 1, 2, 1, 0)$ , the Walsh spectrum is  $(\sqrt{5}, \sqrt{5}, \sqrt{5}, \sqrt{5}, \sqrt{5})$ . Therefore the spectrum is flat, it means that this function is a generalized bent function. The matrix  $C$  obtained from  $\underline{a}$  is given below, which is the same matrix illustrated in Example 3.4.

$$C = \begin{bmatrix} 0^{f(0-0)} & 0^{f(0-1)} & \zeta_p^{f(0-2)} & \zeta_p^{f(0-3)} & \zeta_p^{f(0-4)} \\ \zeta_p^{f(1)} & 0^{f(0)} & 0^{f(4)} & \zeta_p^{f(3)} & \zeta_p^{f(2)} \\ \zeta_p^{f(2)} & \zeta_p^{f(1)} & 0^{f(0)} & 0^{f(4)} & \zeta_p^{f(3)} \\ \zeta_p^{f(3)} & \zeta_p^{f(2)} & \zeta_p^{f(1)} & 0^{f(0)} & 0^{f(4)} \\ 0^{f(4)} & \zeta_p^{f(3)} & \zeta_p^{f(2)} & \zeta_p^{f(1)} & 0^{f(0)} \end{bmatrix}$$

We did an exhaustive search for almost  $p$ -ary sequences of type  $(\gamma_1, \gamma_2)$  and period  $n+2$  with two consecutive zero-symbols for  $p \in \{5, 7, 11\}$ . We tabulate our results in Table 3.1. The Boolean function  $f$  obtained from the corresponding sequence, its truth-table, Walsh spectrum and bentness are give in this table. It is seen that we generally obtain a bent function from a NPS. Moreover, we obtain some other functions with 3 distinct Walsh coefficients. These functions come from the same class of sequences, namely almost  $p$ -ary NPS with two distinct autocorrelation coefficients, but they are not bent. These examples were found in MAGMA programming language and Walsh transforms of the examples were again calculated with MAGMA programming language (see Appendix SEQUENCE SEARCH and WALSH TRASNFORM-MAGMA CODES).



Table 3.1: Examples of Walsh spectrum of some NPSs of type  $(\gamma_1, \gamma_2)$

Sequence	$q$	$\gamma_1, \gamma_2$	$f(x)$	Truth table	$ \hat{F} $	Generalized Bent Function
$(0, 0, \zeta_2^3, \zeta_3^3, \zeta_5^3)$	5	$\gamma_1 = -\zeta_5^3 - \zeta_3^3 - 1, \gamma_2 = 1$	$4x^2 + 4x + 4$	(4, 2, 3, 2, 4)	(2, 23, 2, 23, 2, 23, 2, 23)	$\checkmark$
$(0, 0, \zeta_2^2, \zeta_4^4, \zeta_5^2)$	5	$\gamma_1 = \zeta_3^3 + \zeta_5^3, \gamma_2 = 1$	$3x^2 + 3x + 1$	(1, 2, 4, 2, 1)	(2, 23, 2, 23, 2, 23, 2, 23)	$\checkmark$
$(0, 0, \zeta_2^3, \zeta_5^2, \zeta_3^3)$	5	$\gamma_1 = -\zeta_5^3 - \zeta_3^3 - 1, \gamma_2 = 1$	$x^2 + x + 1$	(1, 3, 2, 3, 1)	(2, 23, 2, 23, 2, 23, 2, 23)	$\checkmark$
$(0, 0, \zeta_3^3, 1, \zeta_5^3)$	5	$\gamma_1 = \zeta_3^3 + \zeta_5^3 - 1, \gamma_2 = 1$	$3x^2 + 3x + 2$	(2, 3, 0, 3, 2)	(2, 23, 2, 23, 2, 23, 2, 23)	$\checkmark$
$(0, 0, \zeta_4^4, 1, \zeta_5^4)$	5	$\gamma_1 = -\zeta_5^3 - \zeta_3^3 - 1, \gamma_2 = 1$	$4x^2 + 4x + 1$	(1, 4, 0, 4, 1)	(2, 23, 2, 23, 2, 23, 2, 23)	$\checkmark$
$(0, 0, \zeta_5^2, \zeta_3^3, \zeta_6)$	5	$\gamma_1 = \zeta_3^3 + \zeta_5^3, \gamma_2 = 1$	$3x^2 + 3x$	(0, 1, 2, 1, 0)	(2, 23, 2, 23, 2, 23, 2, 23)	$\checkmark$
$(0, 0, \zeta_4^4, 1, \zeta_5^4)$	5	$\gamma_1 = -\zeta_5^3 - \zeta_3^3 - 1, \gamma_2 = 1$	$4x^2 + 4x + 1$	(1, 4, 0, 4, 1)	(2, 23, 2, 23, 2, 23, 2, 23)	$\checkmark$
$(0, 0, 1, \zeta_5, 1)$	5	$\gamma_1 = -\zeta_5^3 - \zeta_3^3 - 1, \gamma_2 = 1$	$4x^2 + 4x + 2$	(2, 4, 0, 4, 2)	(2, 23, 2, 23, 2, 23, 2, 23)	$\checkmark$
$(0, 0, \zeta_5, 1, \zeta_5)$	5	$\gamma_1 = -\zeta_5^3 - \zeta_3^3 - 1, \gamma_2 = 1$	$x^2 + x + 4$	(4, 1, 0, 1, 4)	(2, 23, 2, 23, 2, 23, 2, 23)	$\checkmark$
$(0, 0, \zeta_2^3, \zeta_5^2, \zeta_3^3)$	5	$\gamma_1 = 2, \gamma_2 = 1$	2	(2, 2, 2, 2, 2)	(5, 0, 0, 0, 0)	$\checkmark$
$(0, 0, 1, \zeta_7^4, \zeta_7^3, 1)$	7	$\gamma_1 = \zeta_7^3 + \zeta_7^4 + \zeta_7^2 + \zeta_7^6, \gamma_2 = \zeta_7^2 + \zeta_7^4 + 1$	$4x^2 + 4x + 6$	(6, 0, 2, 5, 2, 0, 6)	(2, 64, 2, 64, 2, 64, 2, 64, 2, 64, 2, 64)	$\checkmark$
$(0, 0, 1, \zeta_7^3, \zeta_7^4, \zeta_7^3, 1)$	7	$\gamma_1 = -\zeta_7^3 - \zeta_7^4 - 1, \gamma_2 = \zeta_7^2 + \zeta_7^4 + \zeta_7^3 + 1$	$6x^2 + 6x + 2$	(2, 0, 3, 4, 3, 0, 2)	(2, 64, 2, 64, 2, 64, 2, 64, 2, 64, 2, 64)	$\checkmark$
$(0, 0, \zeta_7, 1, \zeta_7^2, 1, \zeta_7)$	7	$\gamma_1 = -\zeta_7^4 - \zeta_7^3 - 1, \gamma_2 = -\zeta_7^2 - \zeta_7^4 - \zeta_7^3 - \zeta_7^2$	$5x^2 + 5x + 5$	(5, 1, 0, 2, 0, 1, 5)	(2, 64, 2, 64, 2, 64, 2, 64, 2, 64, 2, 64)	$\checkmark$
$(0, 0, \zeta_7, \zeta_7^6, \zeta_7^3, \zeta_7^6, \zeta_7)$	7	$\gamma_1 = \zeta_7^3 + \zeta_7^4 + \zeta_7^2 + \zeta_7^6, \gamma_2 = \zeta_7^2 + \zeta_7^4 + 1$	$3x^2 + 3x + 2$	(2, 1, 6, 3, 6, 1, 2)	(2, 64, 2, 64, 2, 64, 2, 64, 2, 64, 2, 64)	$\checkmark$
$(0, 0, \zeta_7^2, \zeta_4^4, 1, \zeta_7^4, \zeta_7^2)$	7	$\gamma_1 = \zeta_7^3 + \zeta_7^4 + \zeta_7^2 + \zeta_7^6, \gamma_2 = \zeta_7^2 + \zeta_7^4 + 1$	$4x^2 + 4x + 1$	(1, 2, 4, 0, 4, 2, 1)	(2, 64, 2, 64, 2, 64, 2, 64, 2, 64, 2, 64)	$\checkmark$
$(0, 0, \zeta_7^2, \zeta_7^4, \zeta_7^4, \zeta_7^4, \zeta_7^2)$	7	$\gamma_1 = \zeta_7^3 + \zeta_7^2 + 2, \gamma_2 = \zeta_7^2 + \zeta_7^4 + 1$	$x^4 + 2x^3 + 4x^2 + 3x + 6$	(6, 2, 4, 4, 4, 2, 6)	(2, 1, 3, 04, 3, 04, 1, 91, 3, 04, 3, 04)	$\checkmark$
$(0, 0, \zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^2)$	7	$\gamma_1 = -\zeta_7^3 - \zeta_7^4 - \zeta_7^2 + 1, \gamma_2 = -\zeta_7^3 - \zeta_7^4 - \zeta_7^2 - \zeta_7^2$	$3x^4 + 6x^3 + 5x^2 + 2x + 1$	(1, 3, 2, 2, 2, 3, 1)	(5, 49, 1, 35, 2, 39, 1, 35, 2, 39, 1, 35)	$\checkmark$
$(0, 0, \zeta_7^4, \zeta_7^6, \zeta_7^2, \zeta_7^6, \zeta_7^4)$	7	$\gamma_1 = \zeta_7^3 + \zeta_7^4 + \zeta_7^2 + \zeta_7^6, \gamma_2 = \zeta_7^2 + \zeta_7^4 + 1$	$4x^2 + 4x + 3$	(3, 4, 6, 2, 6, 4, 3)	(2, 64, 2, 64, 2, 64, 2, 64, 2, 64, 2, 64)	$\checkmark$
$(0, 0, \zeta_7^4, \zeta_7, 1, \zeta_7, \zeta_7^4)$	7	$\gamma_1 = -\zeta_7^3 - \zeta_7^4 - 1, \gamma_2 = \zeta_7^2 + \zeta_7^4 + 1$	$x^2 + x + 2$	(2, 4, 1, 0, 1, 4, 2)	(2, 64, 2, 64, 2, 64, 2, 64, 2, 64, 2, 64)	$\checkmark$
$(0, 0, \zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^2)$	7	$\gamma_1 = \zeta_7^3 + \zeta_7^2 + 2, \gamma_2 = \zeta_7^2 + \zeta_7^4 + 1$	$2x^4 + 4x^3 + x^2 + 6x + 6$	(6, 5, 2, 2, 2, 5, 6)	(0, 60, 4, 31, 1, 69, 1, 69, 1, 69, 4, 31)	$\checkmark$
$(0, 0, \zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^2, \zeta_7^2)$	7	$\gamma_1 = -\zeta_7^3 - \zeta_7^4 - 1, \gamma_2 = \zeta_7^2 + \zeta_7^4 + 1$	$x^2 + x + 3$	(3, 5, 2, 1, 2, 5, 3)	(2, 64, 2, 64, 2, 64, 2, 64, 2, 64, 2, 64)	$\checkmark$
$(0, 0, \zeta_7^2, \zeta_7^3, \zeta_7^2, \zeta_7^2, \zeta_7^2)$	7	$\gamma_1 = -\zeta_7^4 - \zeta_7^3 - 1, \gamma_2 = -\zeta_7^3 - \zeta_7^4 - \zeta_7^3 - \zeta_7^2$	$6x^2 + 6x + 1$	(1, 6, 2, 3, 2, 6, 1)	(2, 64, 2, 64, 2, 64, 2, 64, 2, 64, 2, 64)	$\checkmark$
$(0, 0, \zeta_7^2, \zeta_7^4, \zeta_7^2, \zeta_7^4, \zeta_7^2)$	7	$\gamma_1 = \zeta_7^3 + \zeta_7^2 + \zeta_7^4 + \zeta_7^6, \gamma_2 = \zeta_7^2 + \zeta_7^4 + 1$	$2x^2 + 2x + 6$	(6, 3, 4, 2, 4, 3, 6)	(2, 64, 2, 64, 2, 64, 2, 64, 2, 64, 2, 64)	$\checkmark$
$(0, 0, \zeta_7^2, 1, 1, 1, \zeta_7^2)$	7	$\gamma_1 = \zeta_7^3, \gamma_2 = -\zeta_7^3 - \zeta_7^4 - \zeta_7^2$	$4x^4 + x^3 + 2x^2 + 5x + 1$	(1, 6, 0, 0, 0, 6, 1)	(5, 49, 1, 35, 2, 39, 1, 35, 2, 39, 1, 35)	$\checkmark$
$(0, 0, \zeta_{11}^{10}, \dots, \zeta_{11}^{10})$	11	$\gamma_1 = 8, \gamma_2 = 7$	10	(10, 10, ..., 10)	(11, 0, 0, ..., 0)	$\checkmark$

### 3.2 Communication Application

In this section, we explain how sequences are used in CDMA. First, we examine the CDMA structure (see Figure 3.1). At the transmitter side, we first choose data from set  $\mathbb{Z}_p$ , this is  $\{0, 1, \dots, p - 1\}$ , and convert the data to complex data obtained by taking corresponding power of  $\zeta_p$ . For example, when  $p = 3$  and the data is  $(0, 1, 2, 1, 1)$ , the complex data is  $(\zeta_3^0, \zeta_3^1, \zeta_3^2, \zeta_3^1, \zeta_3^1)$ . In the next step of CDMA, each term of the complex data is multiplied by the sequence given to the user and then the spread message is obtained, the spread messages of each user are add to each other to get the transmitted message. In the Rayleigh channel the signal is multiplied by the channel coefficient and AWGN is added. So, the received message is obtained. At the receiver side, the received message is multiplied by the user's sequence and  $cd'$  is obtained. In the decision process, for each component of  $cd'$ , the element closest to any of the set  $\mathcal{E}_p$  is chosen as the corresponding component of the  $d'$ . We give an example below.

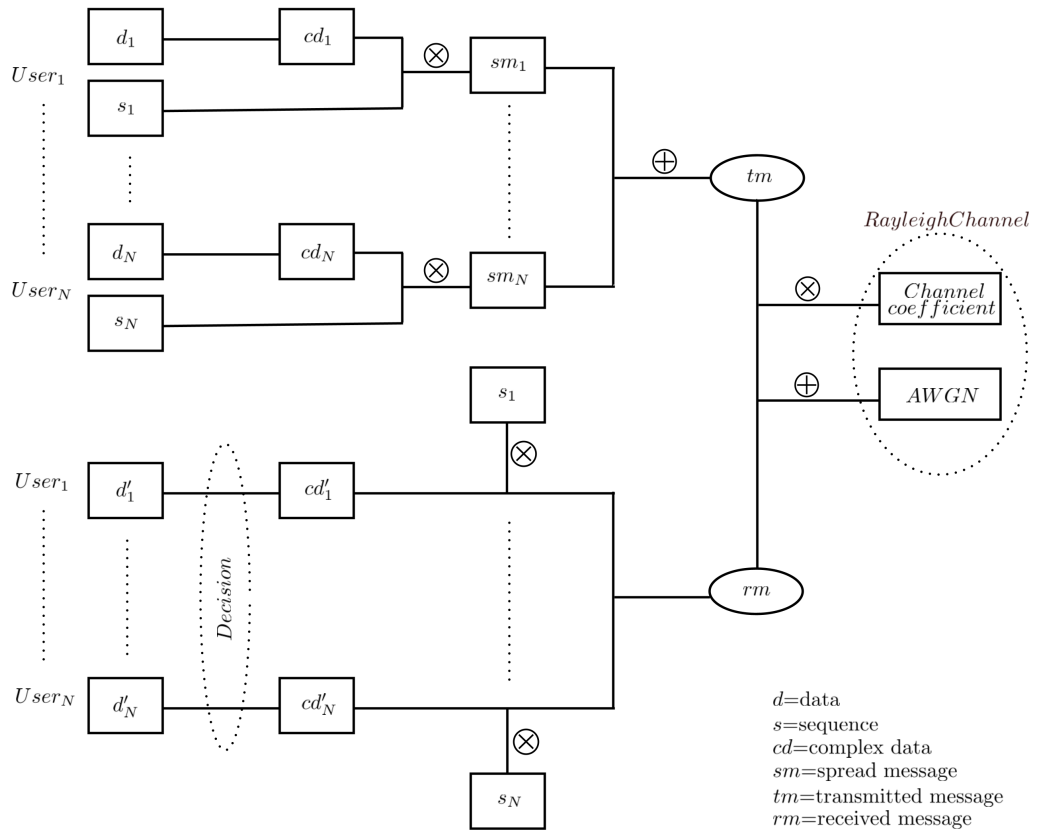


Figure 3.1: Structure of CDMA

**Example 3.9.** Let  $\mathcal{E}_3 = \{1, \zeta_3, \zeta_3^2\} \approx \{1, -0.49 + 0.86j, -0.5 - 0.86j\}$  and  $cd' = \{-2.5 - 0.81j, -1.3 - 0.69j\}$ . Now, we take the difference between  $(-2.5 - 0.81j)$  and each element in  $A$ , and calculate their norms.

$$\begin{aligned} \{| -2.5 - 0.81j - \mathcal{E}_{3_i} |\}_{i=1,2,3} &= \{|3.5 + 0.81j|, |2.01 + 1.67j|, |2 - 0.05j|\} \\ &= \{\sqrt{3.5^2 + 0.81^2}, \sqrt{2.01^2 + 1.67^2}, \sqrt{2^2 + (-0.05)^2}\} \\ &\approx \{3.6, 2.61, 2\} \end{aligned}$$

The minimum value is 2, obtained by the  $(-0.5 - 0.86j) \approx \zeta_3^2 \in A$ . Hence,  $d' = 2$  for  $cd' = (-2.5 - 0.81j)$ . Similarly, the  $d'$  for  $cd' = (1.3 - 0.69j)$  is 0. Therefore,  $cd' = \{-2.5 - 0.81j, -1.3 - 0.69j\}$  is easily converted to  $d' = \{2, 0\}$ .

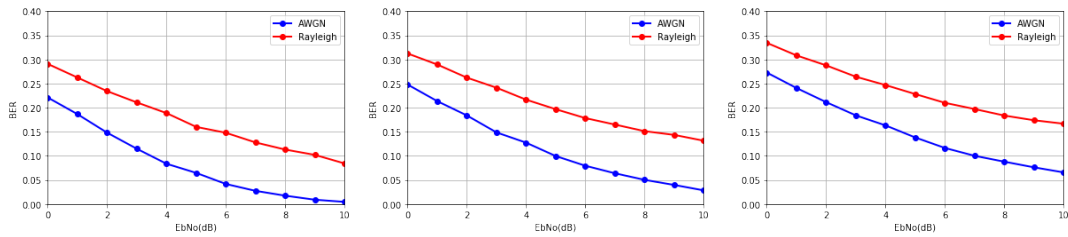


Figure 3.2: BER performance of CDMA with  $a_1$  and 2, 3, 4 users respectively

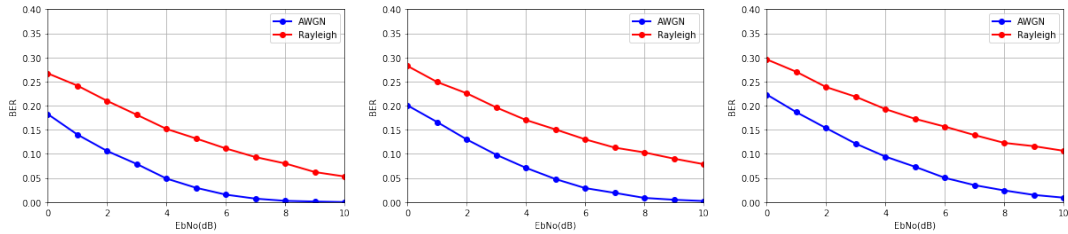


Figure 3.3: BER performance of CDMA with  $a_2$  and 2, 3, 4 users respectively

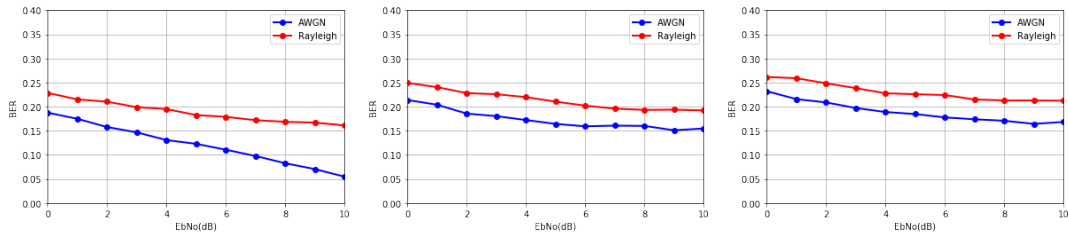


Figure 3.4: BER performance of CDMA with  $a_3$  and 2, 3, 4 users respectively

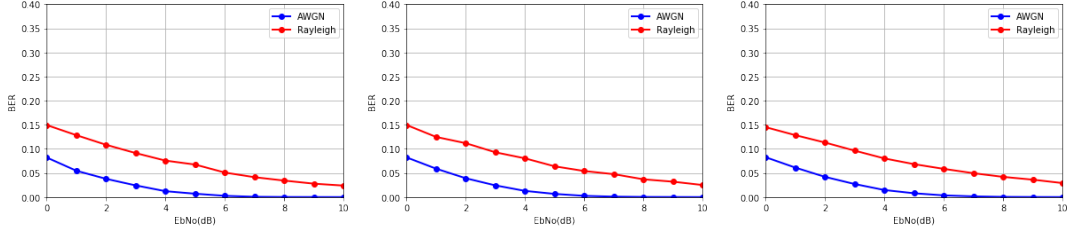


Figure 3.5: BER performance of CDMA with  $a_4$  and 2, 3, 4 users respectively

We simulated Figure 3.1 by using nearly perfect sequences  $a_1 = (0, 0, \zeta_3^2, 1, \zeta_3^2, \dots)$  of type  $(-1, 1)$ ,  $a_2 = (0, 0, \zeta_3^2, 1, \zeta_3^2, \zeta_3^2, \zeta_3^2, \zeta_3, \zeta_3^2, \zeta_3^2, \zeta_3^2, 1, \zeta_3^2, \dots)$  of type  $(1, 3)$ ,  $a_3 = (0, 0, 1, \zeta_2, 1, \dots)$  of type  $(-2, 1)$  and  $a_4 = (0, 0, 1, 1, 1, \zeta_2, \zeta_2, \zeta_2, 1, \zeta_2, \zeta_2, 1, \zeta_2, \dots)$  of type  $(0, -1)$ . We selected the number of users as 2, 3 and 4 in the simulations. We have simulated by using the code in Appendix BER ANALYSIS-SAGE CODES where the data length fixed to 10000 and each simulation repeated 11 times.

The simulation results are given in Figures 3.2, 3.3, 3.4, 3.5, where blue lines are for the simulation results when only AWGN is added to the transmitted message on the channel and red lines are for the simulation results when the transmitted message is first multiplied by channel coefficient and then AWGN is added. It is seen that the larger period of sequence is chosen, the better bit error rate (BER) is obtained when  $p$  and the number of users are fixed (see Figures 3.2 and 3.3 or Figures 3.4 and 3.5). On the other hand, the smaller  $p$  is chosen, the better BER is obtained when the period of sequence and the number of users are fixed (see Figures 3.2 and 3.4 or Figures 3.3 and 3.5). The BER performance is dependent on the number of users for any fixed sequence. It is seen that an increase in the number of users proportionally decreases the BER performance. We see the best simulation results is obtained by using  $a_4$  (see Figure 3.5). Note that the increase in the number of users for this sequence affects the BER performance very little. As a result, for a multiuser case, if  $p$  is small, choose the period of sequence as large as possible, so that the better BER performance is obtained.

In [20, Section 5.5], the BER performance of CDMA with  $M$ -sequence and orthogonal Gold sequence in AWGN or Rayleigh channel is given. In both channels, orthogonal Gold sequences have better results. The BER performance in our simulation is not as good as in [20, Section 5.5] because we used almost  $p$ -ary NPS of type  $(\gamma_1, \gamma_2)$ . However, for the  $a_4$  sequence we get approximately the same BER performance as in [20, Section 5.5, Fig.5.20]. For instance, in [20, Section 5.5, Fig.5.20], for  $dB = 8$ ,  $BER \approx 0.05$  where the number of

users is 7. In Figure 3.5, for  $dB = 8$ ,  $BER \approx 0.05$  where the number of users is 4. It would be a good future work to devise an efficient method for recovering the received message.

### 3.3 Conclusion

The main objective of this chapter is the application of almost  $p$ -ary sequences to cryptographic functions, e.g bent function, and BER analysis on CDMA wireless communication. Walsh spectrum of a function obtained from a sequence is calculated by using Butson-Hadamard matrix. In this way, some generalized bent functions are obtained. We obtained some generalized bent functions from an almost  $p$ -ary NPS except for that the same class of sequence. On the other hand, we simulated BER analysis on CDMA for some of almost  $p$ -ary NPS. According to these simulations, these sequences are not perfectly suitable for the CDMA, but we consider that with a few adjustments, better results can be obtained.

## 4 CONCLUSION AND FUTURE WORK

### 4.1 Conclusion

In this thesis, we studied almost  $p$ -ary sequences and their applications to cryptography and communication. Particularly, we studied the almost  $p$ -ary sequences with 2 zero-symbols and their relationship between the difference sets.

Primarily, we proved a lower and an upper bounds on the number of distinct out-of-phase autocorrelation coefficients of an almost  $p$ -ary sequence of period  $n + s$  with  $s$  consecutive zero-symbols. First main contribution of this thesis is that one can not get an NPS of type  $\gamma$  by adding extra zero-symbols at consecutive positions. Next, we presented a new type of difference set, partial direct product difference set (PDPDS). Then, we proved that a  $p$ -ary NPS of period  $n + 2$  of type  $(\gamma_1, \gamma_2)$  with 2 zero-symbols is equivalent to a PDPDS. We have presented an important property of an almost  $p$ -ary sequence of type  $(\gamma_1, \gamma_2)$  and period  $n + 2$  with 2 consecutive zero-symbols. If there exists such a sequence then this sequence is symmetric except for zero entries. Then, we obtained a necessary condition  $\gamma_2$  for the existence of an almost  $p$ -ary NPS of type  $(\gamma_1, \gamma_2)$ .

Next, we studied the application of the almost  $p$ -ary sequences of type  $(\gamma_1, \gamma_2)$  and period  $n + 2$  with 2 consecutive zero-symbols to cryptographic functions, e.g bent function, and BER analysis on CDMA for these sequences. We presented a new definition of Butson-Hadamard matrix for an almost  $p$ -ary sequence of type  $(\gamma_1, \gamma_2)$  and period  $n + 2$  with 2 consecutive zero-symbols, this is  $(\gamma_1, \gamma_2)$ -near Butson-Hadamard matrix. Walsh spectrum of cryptographic functions is calculated by using this Butson-Hadamard matrix. In this way, we obtained some generalized bent functions by using interpolation. Then, we simulated BER analysis on CDMA for some sequences of almost  $p$ -ary NPS. In these simulations, it was seen that the family of these sequences, although, is so large, they are not perfectly proper for the CDMA type communication.

### 4.2 Future Work

Based on the worked-out examples throughout this thesis, we conjecture that if an almost  $p$ -ary sequence of type  $(\gamma_1, \gamma_2)$  and period  $n + 2$  with 2 consecutive zero-symbols exists then it is a trivial sequence for prime  $p > 3$ . It would be nice future work to construct a class of almost ternary sequences of type  $(\gamma_1, \gamma_2)$  and period  $n + 2$  with 2 consecutive zero-symbols.

In Section 3.1.2 on Chapter 3, we have presented examples of Walsh spectrum of some NPSs of type  $(\gamma_1, \gamma_2)$  (see Table 3.1). Some NPS of type  $(\gamma_1, \gamma_2)$  in this Table 3.1 is not equivalent to generalized bent function. Hence, we will study these sequences, and the equivalent class of boolean functions. And we will try other methods than interpolation for bent functions to obtain from the sequences.

In Section 3.2 on Chapter 3, we have presented simulation results of some NPSs of type  $(\gamma_1, \gamma_2)$  (see Figure 3.2-3.5). But it is clear that these results are not good. this means that NPSs of type  $(\gamma_1, \gamma_2)$  are not suitable perfectly in CDMA under this modulation. Therefore, alternative modulation methods would be a another future work.

## References

- [1] Chih-Lin, I. & Gitlin, R. D. Multi-code cdma wireless personal communications networks. In *Proceedings IEEE International Conference on Communications ICC'95*, vol. 2, 1060–1064 (1995).
- [2] Golomb, S. W. & Gong, G. *Signal design for good correlation: for wireless communication, cryptography, and radar* (Cambridge University Press, 2005).
- [3] Hollon, J. R., Rangaswamy, M. & Setlur, P. New families of optimal high-energy ternary sequences having good correlation properties. *Journal of Algebraic Combinatorics* 1–38 (2018).
- [4] Kumar, P. V., Scholtz, R. A. & Welch, L. R. Generalized bent functions and their properties. *Journal of Combinatorial Theory, Series A* **40**, 90–107 (1985).
- [5] Schmidt, K.-U. Quaternary constant-amplitude codes for multicode cdma. *IEEE Trans. Information Theory* **55**, 1824–1832 (2009).
- [6] Chee, Y. M., Tan, Y. & Zhou, Y. Almost  $p$ -ary perfect sequences. In *International Conference on Sequences and Their Applications*, 399–415 (2010).
- [7] Helleseth, T. Sequences with low correlation. *Handbook of coding theory* (1998).
- [8] Liu, H. Y. & Feng, K. Q. New results on nonexistence of perfect  $p$ -ary sequences and almost  $p$ -ary sequences. *Acta Mathematica Sinica, English Series* **32**, 2–10 (2016).
- [9] Jungnickel, D. & Pott, A. Perfect and almost perfect sequences. *Discrete Applied Mathematics* **95**, 331–359 (1999).
- [10] Ma, S. L. & Ng, W. S. On non-existence of perfect and nearly perfect sequences. *International Journal of Information and Coding Theory* **1**, 15–38 (2009).
- [11] Özbudak, F., Yayla, O. & Yıldırım, C. C. Nonexistence of certain almost  $p$ -ary perfect sequences. In *International Conference on Sequences and Their Applications*, 13–24 (2012).
- [12] Lv, C. On the non-existence of certain classes of perfect  $p$ -ary sequences and perfect almost  $p$ -ary sequences. *IEEE Transactions on Information Theory* **63**, 5350–5359 (2017).



- [13] Niu, X., Cao, H. & Feng, K. Non-existence of perfect binary sequences. *arXiv preprint arXiv:1804.03808* (2018).
- [14] Çeşmelioglu, A. & Olmez, O. Graphs of vectorial plateaued functions as difference sets. *arXiv preprint arXiv:1807.11181* (2018).
- [15] Yayla, O. Nearly perfect sequences with arbitrary out-of-phase autocorrelation. *Advances in Mathematics of Communications* **10**, 401–411 (2016).
- [16] Lam, T. Y. & Leung, K. H. On vanishing sums of roots of unity. *Journal of algebra* **224**, 91–109 (2000).
- [17] Winterhof, A., Yayla, O. & Ziegler, V. Non-existence of some nearly perfect sequences, near butson-hadamard matrices, and near conference matrices. *Mathematics in Computer Science, to appear*, (2018).
- [18] Beth, T., Jungnickel, D. & Lenz, H. *Design Theory*:. No. 1. c. in *Encyclopedia of Mathematics and its Applications* (Cambridge University Press, 1999). URL <https://books.google.com.tr/books?id=z3RvAQAACAAJ>.
- [19] Kurt, S. & Yayla, O. Near butson-hadamard matrices and nonlinear boolean functions. In *International Conference on Number-Theoretic Methods in Cryptology*, 254–266 (2017).
- [20] Harada, H. & Prasad, R. *Simulation and software radio for mobile communications* (Artech House, 2002).

## Appendix: SEQUENCE SEARCH-MAGMA CODES

We present the used MAGMA source codes to find samples of NPSs of type  $(\gamma_1, \gamma_2)$ . We obtained all examples about NPSs of type  $(\gamma_1, \gamma_2)$  in this thesis with these codes.

```
correlation := function (a, n, t)
    sum := 0;
    for i in [1..n] do
        if (i+t) gt n then
            ipt := ((i+t) mod n);
        else
            ipt := i+t;
        end if;
        sum += (a[i]*ComplexConjugate(a[ipt]));
    end for;
    return sum;
end function;
```

```
is_symm := function (a)
    n := #a;
    for i in [1..(n div 2)] do
        if a[i] ne a[n+1-i] then
            return false;
        end if;
    end for;
    return true;
end function;
```

```
s := 2;
set_a := {};
for n in [15] do
    printf "n: %o\n", n;
    for p in [17] do
        ext_set := {};
```

```

ext_set_abs := { };
ext_set_im := { };
printf "\nn: %o p: %o\n", n, p;
pary := { };
unity := RootOfUnity(p);
for i in [0..(p-1)] do
    Include(~pary, unity^i);
end for;
seq_set := CartesianPower(pary, n);
n_seq_set := #seq_set;
p_n_seq_set := n_seq_set div (100);
counter := -1;
for a in seq_set do
    if not is_symm(a) then
        continue a;
    end if;
    counter += 1;
    b := [];
    for i in [1..s] do
        b[i] := unity - unity;
    end for;
    for i in [1..n] do
        b[i+s] := a[i];
    end for;
    set_gamma := { };
    for t in [1..n+s-1] do
        cor := correlation(b, n+s, t);
        Include(~set_gamma, cor);
    end for;
    nbr_set_gamma := #set_gamma;
    if nbr_set_gamma eq 2 then
        a_exponent := [];

```

```

for i in a do
  for j in [0..p-1] do
    if i eq unity^j then
      Append(~a_exponent , j);
    end if;
  end for;
end for;
printf "a:= %o\n", a_exponent;
printf "a:= %o\n", a;
printf "correlation:= %o\n",
      set_gamma;
Include(~set_a , a_exponent);
end if;
end for; ext_set;
end for;
end for;

```

## Appendix: WALSH TRANSFORM-MAGMA CODES

We present the used MAGMA source codes to calculate the Walsh transform of obtained bent functions from NPSs of type  $(\gamma_1, \gamma_2)$ . Results obtained using these codes, we are illustrated in Table 3.1.

```
innerproduct := function(x, y, n)
    product := x[1]*y[1];
    for i in [2..n] do
        product += x[i]*y[i];
    end for;
    return product;
end function;

lex := function(x, n, p)
    a := Integers()!x[n];
    for i in [2..n] do
        a += p^(i-1)*Integers()!x[n-i+1];
    end for;
    return a;
end function;

f := function(x, truth_table)
    a := lex(x);
    return truth_table[a];
end function;

/* FIND WALSH SPECTRUM */
walshspec := function(f, p, n)
    K := GF(p);
    w := RootOfUnity(p);
    carK := CartesianPower(K, n);
    WalshSpectrum := [];
    WalshSpectrumAbs := [];
```

```

for x in carK do
  value := 0;
  for y in carK do lex(y,n,p);
    value += (w)^(Integers()!innerproduct(x,y,n)
+f[lex(y,n,p)+1]);
  end for;
  Append(~WalshSpectrum , value );// ,
  Append(~WalshSpectrumAbs ,Abs(ComplexField()! value ));
end for;
printf "%o\n ", WalshSpectrumAbs;
return WalshSpectrum;
end function;

f:=[0,2,0,0,0];
walhspec(f,5,1);

```

## Appendix: BER ANALYSIS-SAGE CODES

We present the used SAGE source codes to BER analysis using NPSs of type  $(\gamma_1, \gamma_2)$  in CDMA. According to these codes, we are simulated some NPSs of type  $(\gamma_1, \gamma_2)$  (see Figure 3.2-3.5).

```
import numpy as np
from numpy import pi, exp, sqrt
from random import choice
import random
import matplotlib.pyplot as plt

def nthRootOfUnity(p): # linear space , parallelizable
    return exp(2j * pi / p )

def crosscorrelation(a1 ,a2):
    sum=0
    for i in range(len(a1)):
        sum+=a1[i]*conjugate(a2[i])
    return sum

def eq_func(a1 ,a2):
    sum=0
    for i in range(len(a1)):
        if (a1[i]==a2[i]):
            sum+=1
    return sum

def min_func(dsdata ,p):
    pth=[0]*p
    for l in range(p):
        pth[l]+=(zp^l)
    dmndsdata=[]
    a=[]
```

```

for i in range(len(dsdata)):
    for j in range(p):
        a.append(abs(pth[j]-dsdata[i]))
    dmdata.append(zp^(a.index(min(a))))
    del a[:]
return dmdata

```

```
seq=[]
```

```

def sequence(a,un):
    for t in range(un):
        seq.append(a[t:] + a[:t])
    return seq

```

```

def main(a,s,p,rpt,un,dl):    #a=sequence , rpt=repeat
    n=len(a)-s
    zp=nthRootOfUnity(p)
    seq=sequence(a,un)
    A=[0]*rpt
    corr=[]
    for i in seq:
        corrx=[]
        for t in range(un):
            corrx.append(crosscorrelation(seq[t],i))
        corr.append(corr)
    for K in range(rpt):
        data=[]
        mdata_noise=[]
        mdata_orj=[]
        dsdata=[]
        eq=[]
        EbNodB_range = range(rpt)
        EbNodB = EbNodB_range[K]

```



```

EbNo=10.0**(EbNodB/10.0)
noise_std = 1/sqrt(2*EbNo)
noise_mean = 0
for i in range(un):
    data.append(np.random.randint(p, size=dl))
for k in range(un):
    datax=[]
    dataxx=[]
for j in range(dl):
    dataxx.append(zp^data[k][j])
    noise=complex(random.gauss(noise_mean, noise_std),
random.gauss(noise_mean, noise_std))
    ch_coeff=sqrt(random.gauss(0,1)**2+
random.gauss(0,1)**2)/sqrt(2)
    datax.append((zp^data[k][j]*ch_coeff)+noise)
mdata_orj.append(np.array(dataxx))
mdata_noise.append(np.array(datax))
for i in range(un):
    dsdatax=[]
    for t in range(dl):
        dsdatax_sum=0
        for un2 in range(un):
            dsdatax_sum+=mdata_noise[un2][t]*corr[i][un2]
        dsdatax.append(dsdatax_sum/n)
    dsdata.append(dsdatax)
for i in range(un):
    eq.append(eq_func(mdata_orj[i], min_func(dsdata[i],
,p)))
    sayac=[]
for i in range(un):
    if (dl==eq[i]):
        sayac.append(0)

```

```

        else :
            sayac.append(float(dl-eq[i])/dl)
        A[K]+=(sum(sayac)/un)
    return A

p=3
s=2
dl=10000
un=4
rpt=11
zp=nthRootOfUnity(p)
a=[0,0,zp^2,1,zp^2]

plt.plot(range(11), main(a,s,p,rpt,un,dl), 'bo-')
plt.axis([0, 10, 1e-6, 1e-3])
plt.xscale('linear')
plt.xlabel('EbNo(dB)')
plt.ylabel('BER')
plt.grid(True)
plt.show()

```



**HACETTEPE UNIVERSITY  
GRADUATE SCHOOL OF SCIENCE AND ENGINEERING  
THESIS/DISSERTATION ORIGINALITY REPORT**

**HACETTEPE UNIVERSITY  
GRADUATE SCHOOL OF SCIENCE AND ENGINEERING  
TO THE DEPARTMENT OF MATHEMATICS**

Date:22/07/2019

Thesis Title / Topic: **Almost p-ary Sequences and Their Applications to Cryptography**

According to the originality report obtained by my thesis advisor by using the *Turnitin* plagiarism detection software and by applying the filtering options stated below on 22/07/2019 for the total of **55** pages including the a) Title Page, b) Introduction, c) Main Chapters, d) Conclusion sections of my thesis entitled as above, the similarity index of my thesis is 10%.

Filtering options applied:

1. Bibliography/Works Cited excluded
2. Quotes included
3. Match size up to 5 words excluded

I declare that I have carefully read Hacettepe University Graduate School of Science and Engineering Guidelines for Obtaining and Using Thesis Originality Reports; that according to the maximum similarity index values specified in the Guidelines, my thesis does not include any form of plagiarism; that in any future detection of possible infringement of the regulations I accept all legal responsibility; and that all the information I have provided is correct to the best of my knowledge.

I respectfully submit this for approval.

  
Date and Signature

**Name Surname:** Büşra Özden

**Student No:** N17120286


**Department:** Mathematics

**Program:** Mathematics

**Status:**  Masters  Ph.D.  Integrated  
Ph.D.

**ADVISOR APPROVAL**

APPROVED.

  
(Title, Name Surname,  
Signature)

Assoc. Prof. Dr. Oguz Yayla

# CURRICULUM VITAE

## Credentials

Name, Surname : Büşra Özden  
Place of Birth : TEKİRDAĞ, 1995  
Marital Status : single  
E-mail : busraozdenn@gmail.com  
Address : Hacettepe Üniversitesi, Beytepe Kampüsü, Beytepe,  
Çankaya, Ankara, TURKEY

## Education

High School : 2009-2013 Ankara High School (Anatolian)  
BSc. : 2013-2017 Hacettepe University, Faculty of Science, Department of  
Mathematics  
MSc. : 2017-2019 Hacettepe University, Institute of Graduate Studies in Science,  
Department of Mathematics

## Foreign Languages

English

## Work Experience

### Areas of Experience

## Publications

1. Özden, Büşra, and Oğuz Yayla. "Almost p-ary Sequences." arXiv preprint arXiv:1807.11412 (2018). (submitted to a journal)

## Projects and Budgets

2017-2019 TUBITAK-3501 - Career Development Program (Project No: 116R026)

## **Oral and Poster Presentations**

1. TOBB University, Ankara Mathematics Days 2018, "Research of Supersingular Isogeny Key Encapsulation Protocol" presentation speaker
2. Erzincan Binali Yıldırım University, National Mathematics Symposium 2018, "Almost  $p$ -ary Sequences" presentation speaker