EXISTENCE PROBLEM OF ALMOST P-ARY PERFECT AND NEARLY PERFECT SEQUENCES

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

CEMAL CENGİZ YILDIRIM

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
CRYPTOGRAPHY

SEPTEMBER 2012

Approval of the thesis:

EXISTENCE PROBLEM OF ALMOST P-ARY PERFECT AND NEARLY PERFECT SEQUENCES

submitted by **CEMAL CENGİZ YILDIRIM** in partial fulfillment of the requirements for the degree of **Doctor of Philosopy in Department of Cryptography, Middle East Technical University** by,

Prof. Dr. Bülent Karasözen _____
Director, Graduate School of **Applied Mathematics**

Prof. Dr. Ferruh Özbudak _____
Head of Department, **Cryptography**

Prof. Dr. Ferruh Özbudak _____
Supervisor, **Department of Mathematics**

Dr. Oğuz Yayla _____
Co-supervisor, **Department of Cryptography**

Examining Committee Members:

Assoc. Prof. Dr. Ali Doğanaksoy _____
Department of Mathematics, METU

Prof. Dr. Ferruh Özbudak _____
Department of Mathematics, METU

Assist. Prof. Dr. Zülfükar Saygı _____
Department of Mathematics, TOBB ETU

Assist. Prof. Dr. Ömer Küçüksakallı _____
Department of Mathematics, METU

Dr. Hamdi Murat Yıldırım _____
Department of Computer Technology and Information Systems, Bilkent University

Date: _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: CEMAL CENGİZ YILDIRIM

Signature :

ABSTRACT

EXISTENCE PROBLEM OF ALMOST P-ARY PERFECT AND NEARLY PERFECT SEQUENCES

Yıldırım, Cemal Cengiz
Ph.D., Department of Cryptography
Supervisor : Prof. Dr. Ferruh Özbudak
Co-Supervisor : Dr. Oğuz Yayla

September 2012, 43 pages

Almost p-ary perfect and nearly perfect sequences are equivalent to certain relative difference sets and direct product difference sets, respectively. This feature enables Chee, Tan and Zhou to determine the existence status of those sequences by using the tools of Design Theory. In particular, they determined the existence status of almost p-ary perfect and nearly perfect sequences of period $n+1$ for $n \leq 100$, except some open cases in [6]. In this thesis, we obtained a set of Diophantine equations in integers while observing relative difference sets, and proved nonexistence of almost p-ary perfect sequences of period $n+1$ for $n \in \{50, 76, 94, 99, 100\}$. Also, we observed that it was possible to extend Diophantine equations that we used for relative difference sets to the direct product difference sets, thereby proved the nonexistence of almost p-ary nearly perfect sequences of type II of period $n+1$ for $p = 2$, $p = 3$ and $p = 5$ at certain values of n. As a result, we answered two questions posed by Chee, Tan and Zhou in [6].

Keywords: almost p-ary perfect sequence, almost p-ary nearly perfect sequence, relative

difference set, direct product difference set

ÖZ

YAKLAŞIK P-ARY MÜKEMMEL VE MÜKEMMELE YAKIN DİZİLERİN VAROLABİLİRLİK PROBLEMİ

Yıldırım, Cemal Cengiz
Doktora, Kriptografi Bölümü
Tez Yöneticisi : Prof. Dr. Ferruh Özbudak
Ortak Tez Yöneticisi : Dr. Oğuz Yayla

Eylül 2012, 43 sayfa

Yaklaşık p-ary mükemmel ve mükemmele yakın diziler ile sırasıyla nispi fark kümeleri ve doğrudan çarpım fark kümeleri arasında denklik vardır. Bu özellik, Chee, Tan ve Zou' nun söz konusu dizilerin varolabilirlik durumlarını Dizayn Teorisinin yöntemlerini kullanarak tespit etmelerine imkan vermiştir. Spesifik olarak onlar, [6]'da $n \leq 100$ için, periyodu $n+1$ olan yaklaşık p-ary mükemmel ve mükemmele yakın dizilerin var olup olmadığını bazı n değerleri hariç tespit etmişlerdir. Bu tezde, biz nispi fark kümelerini incelerken, tamsayılar üzerine bir grup Diophantine denklem elde ettik ve $n \in \{50, 76, 94, 99, 100\}$ için periyodu $n+1$ olan yaklaşık p-ary mükemmel dizilerin mevcut olmadığını ispatladık. Aynı zamanda, nispi fark kümeleri için kullandığımız Diophantine denklemlerini doğrudan çarpım fark kümeleri için de uyarlayarak kullanabileceğimizi gözlemledik ve bu yolla, $p = 2$, $p = 3$ ve $p = 5$ için, periyodu $n+1$ olan yaklaşık p-ary mükemmele yakın tip II dizilerin belirli n değerleri için mevcut olmadığını ispatladık. Sonuç olarak, Chee, Tan ve Zou tarafından [6]'da sorulan iki soruya cevap verdik.

Anahtar Kelimeler: yaklaşık p-ary mükemmel dizi, yaklaşık p-ary mükemmele yakın dizi, nispi fark kümesi, doğrudan çarpım fark kümesi

To my family

ACKNOWLEDGMENTS

I would like to express my deep gratitude to my supervisor Prof. Dr. Ferruh Özbudak for his supervision, guidance, suggestions and above all his encouragement throughout the development of this thesis. Especially, his guidance on how to approach to an open problem is invaluable. I am indebted to my co-supervisor Dr. Oğuz Yayla who helps me to organize my thesis, provides indispensable material for this thesis and corrects my errors. I want to express my sincere thanks to my instructors for their support and generosity while sharing their knowledge. Last but not least, I would like to thank my family for their continuous support.

TABLE OF CONTENTS

LIST OF TABLES

TABLES

CHAPTER 1

INTRODUCTION AND PRELIMINARIES

1.1 Introduction

Correlation property of a periodic sequence is of great importance when it comes into consideration for engineering applications. According to ([1]), ([2]) and references therein, periodic sequences having good correlation property are widely used in various areas such as telecommunications and radar applications. For instance, Golomb sets light to possible areas where such sequences are likely to be used in [3]. Also in [1], it is given a simplified practical application of perfect binary sequences.

This motivates the search for new methods to construct periodic sequences with good correlation property. By the term "good correlation", it is meant that the autocorrelation coefficients of a periodic sequence are two-valued. More precisely, let $\underline{a} = (a_0, a_1, \ldots, a_n)$ be an m-ary or an almost m-ary sequence of period $n+1$. For $0 \leq t \leq n$, the value of the autocorrelation function $C_{\underline{a}}(t)$ at t is defined by

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

where $\overline{a_{i+t}}$ is the complex conjugate of a_{i+t}. Note that $C_{\underline{a}}(t) \in \mathbb{C}$. The value $C_{\underline{a}}(t)$ is called *the autocorrelation coefficient of* $\underline{a}$ *at* t. For $t \in \mathbb{Z}$, let t_1 be the integer $0 \leq t_1 \leq n$ such that $t \equiv t_1 \bmod (n+1)$. Then, one can extends the autocorrelation function to the values on $\mathbb{Z}$ via $C_{\underline{a}}(t) = C_{\underline{a}}(t_1)$. The autocorrelation function of m-ary or an almost m-ary sequence $\underline{a}$ of period $n+1$ is *two-valued* if $C_{\underline{a}}(t)$ is equal to a constant γ for all $1 \leq t \leq n$, i.e. all coefficients except the coefficient at $t = 0$. $C_{\underline{a}}(t)$ is also called in-phase autocorrelation coefficient when $t \equiv 0 \bmod (n+1)$, and out-of-phase for the other values of t. Furthermore, if $\gamma = 0$, then the corresponding sequence is called perfect, and if $\gamma = |1|$, then it is called nearly perfect.

In this study, the sequences which we are dealing with are *m-ary* and *almost m-ary sequences*. So that, it might be useful to remember the definition of those sequences. Let $\underline{a} = (a_0, a_1, \ldots, a_n)$ be sequence of period $n+1$ with entries $a_0, a_1, \ldots, a_n \in \mathbb{C}$, the field of complex numbers. Let $m \geq 2$ be an integer and ζ_m be a primitive m-th root of 1 in $\mathbb{C}$. Let $\langle \zeta_m \rangle$ be the multiplicative subgroup of $\mathbb{C}^*$ generated by ζ_m. If the entries of $\underline{a}$ are in the subgroup of $\langle \zeta_m \rangle$, then $\underline{a}$ is called an *m-ary sequence*. If $a_0 = 0$ and the rest of the entries $a_1, a_2, \ldots, a_n$ of $\underline{a}$ are in the subgroup $\langle \zeta_m \rangle$, then $\underline{a}$ is called an *almost m-ary sequence*.

The existence problem of such sequences has gained more attention over the past twenty years. Therefore, significant number of existence and non-existence results has been found. The first article seems to initiate this term is due to Wolfmann ([4]) which contains results on existence of almost perfect autocorrelation sequences. Subsequently, Pott and Bradley ([5]) answered two open cases posed in ([4]) and showed that almost perfect autocorrelation sequences are equivalent to certain cyclic divisible difference sets. In particular, for $m = 2$, i.e., perfect and almost perfect binary periodic sequences, Jungnickel and Pott ([1]) summarized previous results and showed that perfect binary periodic sequences are equivalent to certain cyclic difference sets. For $m = p$ where p is an odd prime, i.e., p-ary perfect and nearly perfect sequences, Ma and Ng ([2]) obtained the existence and non-existence results, except some open cases. Recently, Chee-Tan-Zhou ([6]) studied almost p-ary perfect and nearly perfect sequences. They determined the existence status of almost p-ary perfect and nearly perfect sequences of period $n+1$ for $3 \leq n \leq 100$ and posed two questions. In this thesis, we tried to answer those questions. Both of the questions are quoted here respectively:

Question 1.1.1 (Question 1 in [6]) *Is there an almost p-ary perfect sequence of period* $n+1$ *for each case* $n = 50, 76, 77, 94, 99, 100$*, where p is an odd prime with* $p|(n-1)$*?*

Question 1.1.2 (Question 2 in [6]) *Do almost p-ary nearly perfect sequence of type II with period n+1 exist?*

In both ([2]) and ([6]), the authors showed that existence problem of (almost) p-ary perfect and nearly perfect sequences are equivalent to existence problem of certain relative difference sets and direct product difference sets, respectively. One of the methods used in ([6]) to find existence status of such sequences is an application of multiplier theorem which is regarded as a main instrument of Design Theory on constructing difference sets.

It is worth here to define difference sets and shortly explain how multiplier theorem is used to construct difference sets. Let G be a group of order v in which the identity element is $\{0\}$. Let k and λ be positive integers such that $2 \leq k < v$. Let D be a k-subset of G. If the multiset $[a - b : a, b \in D, a \neq b]$ contains every element in $G\backslash\{0\}$ exactly λ times, then D is called a (v,k,λ)-difference set. Let m be an integer such that

$$mD = \{ma : a \in D\} = D + g$$

for some $g \in G$, then m is a multiplier of D. The definition of multiplier hints the usage of multiplier theorem as a method while determining the existence status of difference sets. More precisely, since m is a multiplier of D, let Λ be the set of orbits of G under the action $x \to mx$. Then, $\exists \Upsilon \subseteq \Lambda$ such that

$$D + h = \bigsqcup_{A \in \Upsilon} A,$$

for some $h \in G$ according to definitions above. This means that $D + h$ is fixed by multiplier m, i.e., $m(D + h) = D + h$ (see [7]). Since D is a difference set, $D + h$ is also a difference set. Therefore, it is possible to decide whether there exists a difference set of any finite group G by checking possible subsets of orbit set formed by the multiplication of group elements with multiplier. The term "possible subsets" means the union of orbits whose cardinality is equal to the cardinality of difference set. The concept of multiplier theorem does not change when it is used to determine the existence status of relative difference sets. However, the problem arises, when the number of possible subsets gets larger. For instance, in remark 1 of ([6]), the authors gave an example in which the number of possible subsets is $\approx 2^{75}$ and concluded that it was not doable to check all those possible sets. Hence, they posed Question 1.1.1.

In this thesis, we initially gave some background on almost p-ary perfect and nearly perfect sequences and their relation with relative difference sets and direct product difference sets. In Chapter 2, we focused on Question 1.1.1. We obtained a set of Diophantine equations in integers and also reduced the number of possible combinations of orbits forming a candidate relative difference set. In some cases we immediately proved the nonexistence as a consequence of the inconsistency of the obtained Diophantine equations. In the other cases we drastically reduced the number of possible combinations of orbits forming a candidate relative difference set so that the reduced size enabled us to check them via a computer. As a consequence, nonexistence of almost p-ary perfect sequences (PS) of period $n + 1$ for $n \in \{50, 76, 94, 99, 100\}$ was proved.

In Chapter 3, we directed our attention to the second question (Question 1.1.2) which is related with almost p-ary nearly perfect sequences (NPS) of type II. We observed that it was possible to extend Diophantine equations that we used for relative difference sets to the direct product difference sets. Thus, we obtained a set of Diophantine equations in integers, and we proved the nonexistence of almost p-ary nearly perfect sequences of type II of period $n+1$ as a consequence of the inconsistency of the obtained Diophantine equations for $p = 2$, $p = 3$ and $p = 5$ at certain values of n.

1.2 Preliminaries

In this section, we will briefly introduce relative difference sets and direct product difference sets. We will also show that they are equivalent to p-ary perfect and nearly perfect sequences respectively.

1.2.1 Relative Difference Sets

Let G be an abelian group of size mn. Let N be a subgroup of G with $|N| = n$. A subset R of G is called an (m, n, k, λ) relative difference set (RDS) in G relative to N if both of the followings hold:

(i.) $|R| = k$,

(ii.) all elements of G not in N can be represented exactly λ times in the form $r_1 - r_2$, where $r_1, r_2 \in R$ with $r_1 \neq r_2$.

A systematic treatment of relative difference sets are due to Elliott and Butson [8]. There are good references like [1, 9, 10] for further background and applications of relative difference sets. The following known result is crucial (see [6, Theorem 1]). Let $\mathbb{Z}_m$ denote the (additively written) cyclic group of order m.

Theorem 1.2.1 *Let p be a prime, $n \geq 2$ be an integer, and $\underline{a} = (a_0, a_1, \ldots, a_n)$ be an almost p-ary sequence of period $n+1$. Let G and N be the groups*

$$G = \mathbb{Z}_{n+1} \times Z_p \text{ and } N = \{0\} \times \mathbb{Z}_p.$$

For a primitive p-th root of 1, $\zeta_p \in \mathbb{C}$, let b_i be the integer in $\{0, 1, 2, \ldots, p-1\}$ such that $a_i = \zeta_p^{b_i}$ for $1 \leq i \leq n$. Let $1 \leq h \leq n+1$ and $1 \leq g \leq p-1$ be integers with $gcd(h, n+1) = 1$ and $gcd(g, p) = 1$. Let R be the subset of G defined as

$$R = \{(ih, b_i g) \in \mathbb{Z}_{n+1} \times \mathbb{Z}_p : 1 \leq i \leq n\}.$$

Then $\underline{a}$ is an almost p-ary perfect sequence of period $n+1$ if and only if R is an $(n+1, p, n, \frac{n-1}{p})$-RDS in G relative to N. In particular, p should divide $n-1$.

1.2.2 Direct Product Difference Sets

Let $G = H \times N$, where the order of H and N are m and n. A subset R of G is called an $(m, n, k, \lambda_1, \lambda_2, \mu)$ direct product difference set (DPDS) in G relative to H and N if both of the following statements hold:

(i.) $|R| = k$,

(ii.) Differences $r_1 - r_2$, $r_1, r_2 \in R$ with $r_1 \neq r_2$ represent

- all non identity elements of $H \times \{0_N\}$ exactly λ_1 times,
- all non identity elements of $\{0_H\} \times N$ exactly λ_2 times,
- all non identity elements of $H \backslash \{0_H\} \times N \backslash \{0_N\}$ exactly μ times.

Direct Product Difference Sets were first defined in [11], but studied only the case $\lambda_1 = 0, \lambda_2 = 0$. General definition of direct product difference sets was given in [2]. The following known result is crucial (see [6, Theorem 6]).

Theorem 1.2.2 *Let p be a prime, $n \geq 2$ be an integer, and $\underline{a} = (a_0, a_1, \ldots, a_n)$ be an almost p-ary sequence of period $n+1$. Let $H = \mathbb{Z}_{n+1}$ and $N = \mathbb{Z}_p$ be the (additively written) cyclic groups of order $n+1$ and p. Let G be the group defined as $G = \mathbb{Z}_{n+1} \times Z_p$. We choose a primitive p-th root of 1, $\zeta_p \in \mathbb{C}$. For $1 \leq i \leq n$ let b_i be the integer in $\{0, 1, 2, \ldots, p-1\}$ such that $a_i = \zeta_p^{b_i}$. Let $1 \leq h \leq n+1$ and $1 \leq g \leq p-1$ be integers with $gcd(h, n+1) = 1$ and $gcd(g, p) = 1$. Let R be the subset of G defined as*

$$R = \{(ih, b_i g) \in \mathbb{Z}_{n+1} \times \mathbb{Z}_p : 1 \leq i \leq n\}.$$

Then

(i.) $\underline{a}$ *is an almost p-ary NPS of type I if and only if R is an* $(n+1, p, n, \frac{n}{p}-1, 0, \frac{n}{p})$*-DPDS in G relative to H and N. In particular, p should divide n.*

(ii.) $\underline{a}$ *is an almost p-ary NPS of type II if and only if R is an* $(n+1, p, n, \frac{n-2}{p}+1, 0, \frac{n-2}{p})$*-DPDS in G relative to H and N. In particular, p should divide* $n-2$*.*

From 1.2.2, one can see that there exists two types of almost p-ary nearly perfect sequence (NPS), namely *almost p-ary NPS of type I* and *almost p-ary NPS of type II*. According to definitions given at the beginning of this chapter, out-of-phase autocorrelation coefficients of almost p-ary NPS are all either 1 or -1. So that almost p-ary NPS is *type I* if all out-of-phase autocorrelation coefficients are -1, and *type II* otherwise.

CHAPTER 2

NONEXISTENCE OF CERTAIN ALMOST p-ARY PERFECT SEQUENCES

In this chapter, we give an answer to Question 1.1.1 for $n = 50, 76, 94, 99, 100$. Our method is based on the approach of [6] in using relative difference sets.

2.1 Background

An important method for the existence and the nonexistence of certain relative difference sets in G relative to N uses the notion of multiplier. For an integer t, let $R^{(t)}$ denote the subset $R^{(t)} = \{tr : r \in R\} \subset G$. Assume that $gcd(t, |G|) = 1$. We call that t is a *multiplier* of R if there exists $g \in G$ such that

$$R^{(t)} = R + g = \{r + g : r \in R\} \subset G.$$

In fact if $k^2 \neq \lambda mn$, then we have a nice situation (see [9], see also [6] page 406, Result 6).

Theorem 2.1.1 *Let R be an (m, n, k, λ)-RDS with $k^2 \neq \lambda mn$. Let t be a multiplier of R. Then there exists at least one translate $(R + g)$ of R such that $(R + g)^{(t)} = R + g$.*

Theorem 2.1.1 gives a nice method for the existence and nonexistence of certain relative difference sets that we recall here (see [6] page 406). Assume that R is an (m, n, k, λ)-RDS in G relative to N, $k^2 \neq \lambda mn$ and t is a multiplier of R. Let Ω be the set of orbits of G under the action $x \to tx$. As $R^{(t)} = R$ without loss of generality (see Theorem 2.1.1), we see that there exists a collection Φ of orbits (i.e. a subset $\Phi \subseteq \Omega$) such that

$$R = \bigsqcup_{A \in \Phi} A,$$

where A is an orbit in Φ. This gives strict conditions on the existence and nonexistence of relative difference sets (see Example 2.3.1 and, for example, Proposition 2.3.2 below).

Here we note that relative difference sets in Theorem 1.2.1 have parameters $(n+1, p, n, \frac{n-1}{p})$ and hence the condition $k^2 \neq \lambda mn$ in Theorem 2.1.1 becomes $n^2 \neq \frac{n-1}{p}(n+1)p = n^2 - 1$, which is satisfied trivially.

Finally we also recall a useful method for finding multipliers for the class relative difference sets that we consider (see [6, Theorem 4]).

Theorem 2.1.2 *Let p be a prime and $n \geq 2$ be an integer. Let G and N be the groups in Theorem 1.2.1. Assume that there exists an $(n+1, p, n, \frac{n-1}{p})$-RDS in G relative to N. Let $n = p_1^{u_1} p_2^{u_2} \dots p_l^{u_l}$ be the prime factorization of n in $\mathbb{Z}$. Let ξ be the primitive $(n+1)p$-th root of 1 in $\mathbb{C}$. For $1 \leq i \leq l$, let $\sigma_i \in Gal(\mathbb{Q}(\xi)/\mathbb{Q})$ defined as $\sigma_i(\xi) = \xi^{p_i}$. Assume also that $\varphi \in (\cap_{i=1}^{l} \langle \sigma_i \rangle) \setminus \{1\}$. Let α be an integer such that $\varphi(\xi) = \xi^{\alpha}$. Then α is a multiplier of R.*

2.2 The Method

In this section we give some tools that we use in Section 2.3. We begin with the next proposition.

Proposition 2.2.1 *Let R be an $(n+1, p, n, \frac{n-1}{p})$-RDS in $G = \mathbb{Z}_{n+1} \times \mathbb{Z}_p$ relative to $N = \{0\} \times \mathbb{Z}_p$. Let R have s_i many elements having i in the second component for $i = 0, 1, 2, \dots, p-1$. Then $\sum_{j=0}^{p-1} s_j^2 = \frac{n(n+p-1)}{p}$ and $\sum_{j=0}^{p-1} s_j s_{j-i} = \frac{n(n-1)}{p}$ for each $i = 1, 2, \dots, \lceil (p-1)/2 \rceil$, where subscripts are computed modulo p.*

Proof. Let φ be the map from $G = \mathbb{Z}_{n+1} \times \mathbb{Z}_p$ to $\mathbb{Z}_p$ sending (a, i) to i. Let V be the multiset consisting of the images (counting multiplicities) of φ restricted to R. By reordering on V we have

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

In other words,

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

Then it is clear that

$$s_0 + s_1 \ldots + s_{p-1} = |R| = n. \tag{2.1}$$

For $0 \leq i \leq p-1$, let T_i be the subset of $G\backslash N$ defined as $T_i = \{(a,e) \in G\backslash N : e = i\}$. It is clear that $T_i = \{(a,i) : a \in Z_{n+1}\backslash\{0\}\}$ and hence

$$|T_i| = n + 1 - 1 = n. \tag{2.2}$$

Moreover, let $\mathcal{T}_i$ be the subset of $R \times R$ defined as

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

As R is an $(n+1, p, n, \frac{n-1}{p})$-RDS, for the cardinality $|\mathcal{T}_i|$ of $\mathcal{T}_i$, using (2.2), we obtain that

$$|\mathcal{T}_i| = \frac{n-1}{p}|T_i| = \frac{(n-1)n}{p}. \tag{2.3}$$

For $0 \leq i \leq p-1$ and $0 \leq j \leq p-1$, let $\mathcal{T}_{i,j}$ be the subset of $\mathcal{T}_i$ defined as

$$\mathcal{T}_{i,j} = \{(\beta_1, \beta_2) \in \mathcal{T}_i : \varphi(\beta_1) = j\}.$$

Then we have

$$|\mathcal{T}_i| = \sum_{j=0}^{p-1} |\mathcal{T}_{i,j}|. \tag{2.4}$$

Next we determine $\mathcal{T}_{i,j}$ for $0 \leq i, j \leq p-1$ and $i \neq 0$. Note that $(\beta_1, \beta_2) \in \mathcal{T}_{i,j}$ if and only if $\beta_1 \in R$, $\varphi(\beta_1) = j$ and $\beta_2 \in R$, $\varphi(\beta_2) = j - i$. Here, $\beta_1 \neq \beta_2$ automatically as $i \neq 0$. Recall that

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

where we define the subscript $j - i$ modulo p. Therefore using (2.3) and (2.4) we conclude that

$$\frac{(n-1)n}{p} = \sum_{j=0}^{p-1} s_j s_{j-i}. \tag{2.5}$$

Note that it is enough to consider the subset of equations in (2.5) corresponding to $1 \leq i \leq \left\lceil \frac{p-1}{2} \right\rceil$ since each equation in (2.5) with $\left\lceil \frac{p-1}{2} \right\rceil < i \leq p-1$ is the same as an equation in (2.5) with $1 \leq i \leq \left\lceil \frac{p-1}{2} \right\rceil$.

Finally, we determine $\mathcal{T}_{0,j}$ for $0 \leq j \leq p-1$. Note that $(\beta_1, \beta_2) \in \mathcal{T}_{0,j}$ if and only if $\beta_1 \in R$, $\varphi(\beta_1) = j$ and $\beta_2 \in R$, $\varphi(\beta_2) = j$ and $\beta_1 \neq \beta_2$. Hence, we get that $|\mathcal{T}_{0,j}| = s_j(s_j - 1)$ for $0 \leq j \leq p-1$. Then using (2.1), (2.3) and (2.4) we conclude that

$$\frac{(n-1)n}{p} = \sum_{j=0}^{p-1} s_j(s_j - 1) = \sum_{j=0}^{p-1} (s_j^2 - s_j) = \sum_{j=0}^{p-1} s_j^2 - \sum_{j=0}^{p-1} s_j = \sum_{j=0}^{p-1} s_j^2 - n,$$

and hence

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

□

The following simple observation is also useful in our proofs in Section 2.3.

Proposition 2.2.2 *Let R be an $(n+1, p, n, n-1/p)$-RDS in $G = \mathbb{Z}_{n+1} \times \mathbb{Z}_p$ relative to $N = \{0\} \times \mathbb{Z}_p$. Assume that t is a multiplier of R such that $R^{(t)} = R$. Let Ω be the set of orbits of the action $x \to tx$ given by the multiplier t. Let Φ be a collection of orbits forming R, that is Φ subset of Ω and*

$$R = \bigsqcup_{A \in \Phi} A.$$

If B is an orbit in Ω such that there exist two distinct elements (b, i_1) in B and (b, i_2) in B with the same first components, then B is not in Φ.

Proof. Assume the contrary. Then $(b, i_1) - (b, i_2) = (0, i_1 - i_2) \in G \backslash N$, which is a contradiction. □

2.3 Results

We start with a simple example illustrating the method.

Example 2.3.1 *There exists (5,3,4,1)-RDS in $G = \mathbb{Z}_5 \times \mathbb{Z}_3$ relative to $\{0\} \times \mathbb{Z}_3$.*

Proof. By Theorem 2.1.2, $t = 2$ is a multiplier. The orbits of G under the action $x \to 2x$ are $\{(0,0)\}$, $\{(0,1),(0,2)\}$, $\{(1,0),(2,0),(4,0),(3,0)\}$, $\{(1,1),(2,2),(4,1),(3,2)\}$, $\{(1,2),(2,1),(4,2),(3,1)\}$. Let s_0, s_1 and s_2 denote the number of elements in R whose second components are 0, 1 and 2, respectively. Using Proposition 2.2.1 we have

$$s_0^2 + s_1^2 + s_2^2 = 8 \text{ and } s_0 s_1 + s_0 s_2 + s_1 s_2 = 4. \tag{2.6}$$

We also have $s_0 + s_1 + s_2 = 4$. We look for a collection Φ of orbits of G satisfying (2.6). The only candidates are the three orbits of length 4. The orbit $\{(1,0),(2,0),(4,0),(3,0)\}$ does not

satisfy (2.6). Both of the remaining two orbits of length 4 satisfy (2.6) as $s_0 = 0$, $s_1 = s_2 = 2$. In fact by checking the differences we observe that both of the remaining two orbits of length 4 are (5,3,4,1)-RDS in G relative to $\{0\} \times \mathbb{Z}_3$. □

In the remaining of this section we present results that fill unknown entries of Table 2 in [6]. We first prove the next proposition in detail.

Proposition 2.3.2 *There does not exist almost 3-ary PS with period 101.*

Proof. We prove by contradiction. Assume that there exists such an almost 3-ary PS with period 101. Using Theorem 1.2.1 we obtain an $(101, 3, 100, 99/3)$-RDS R in $\mathbb{Z}_{101} \times \mathbb{Z}_3$ relative to $\{0\} \times \mathbb{Z}_3$. By Theorem 2.1.2 we obtain that $t = 16$ is a multiplier of R. Indeed let ζ be a primitive 303-th root of 1 in $\mathbb{C}$. We have $100 = 2^2 5^2$ and $\zeta^{16} = (\zeta^2)^8$ and $\zeta^{16} = (\zeta^5)^{185}$. We tabulate the orbits of the action $x \to 16x$ in G in Table A.1 in Appendix. There are three orbits of length 1 and 12 orbits of length 25 in Table A.1. Moreover, using Theorem 2.1.1, we assume without loss of generality that there exists a subset Φ of the orbits in Table A.1 satisfying

$$R = \bigsqcup_{A \in \Phi} A.$$

As $|R| = 100$, it is clear from the lengths and the numbers of the orbits in Table A.1 that Φ consists of 4 distinct orbits of length 25.

As in Proposition 2.2.1, let s_0, s_1 and s_2 denote the number of elements in R with the second component 0,1 and 2 respectively. Using Proposition 2.2.1 we obtain that

$$s_0^2 + s_1^2 + s_2^2 = 100(100 + 3 - 1)/3 = 3400. \tag{2.7}$$

Moreover in each orbit B of Ω, the second component is the same, which follows from the fact that $16 \equiv 1 \bmod 3$. As Φ consists of orbits of length 25 we conclude that s_0, s_1 and s_2 are divisible by 25. Let $s_0 = 25s_0'$, $s_1 = 25s_1'$, $s_2 = 25s_2'$. Then, by (2.7) we obtain that $(s_0')^2 + (s_1')^2 + (s_2')^2 = 3400/625$, which is not an integer. This completes the proof. □

Proposition 2.3.3 *There does not exist almost 7-ary PS with period 51.*

Proof. Similar to Proposition 2.3.2, we prove by contradiction. Assume that there exists such an almost 7-ary PS with period 51. Using Theorem 1.2.1 we obtain an

$(51, 7, 50, 49/7)$-RDS R in $\mathbb{Z}_{51} \times \mathbb{Z}_7$ relative to $\{0\} \times \mathbb{Z}_7$. By Theorem 2.1.2 we obtain that $t = 4$ is a multiplier of R. We tabulate the orbits of the action $x \to 4x$ in G in Table A.2 in Appendix. There are 3 orbits of length 1, 6 orbits of length 3, 12 orbits of length 4 and 24 orbits of length 12. As in Proposition 2.3.2, R is formed by a certain collection Φ of these orbits. By Proposition 2.2.2, since the orbits of length 3 and 12 consist of elements whose first component are same, so these orbits can not be included in Φ. Then we are left by orbits whose elements have 0 in the second component. Now by Proposition 2.2.1, we have $s_0^2 = 400$ and $s_0 = 50$, which is inconsistent. Therefore, there does not exist any (51,7,50,7)-RDS in G relative to $\{0\} \times \mathbb{Z}_7$. □

Proposition 2.3.4 *There does not exist almost 31-ary PS with period 95.*

Proof. Assume that there exists such an almost 31-ary PS with period 95. Using Theorem 1.2.1 we obtain an $(95, 31, 94, 93/31)$-RDS R in $\mathbb{Z}_{95} \times \mathbb{Z}_{31}$ relative to $\{0\} \times \mathbb{Z}_{31}$. By Theorem 2.1.2 we obtain that $t = 4$ is a multiplier of R. We tabulate the orbits of the action $x \to 4x$ in G in Table A.3 in Appendix. There are one orbit of length 1, 2 orbits of length 2, 6 orbits of length 5, 2 orbits of length 9, 12 orbits of length 10, 4 orbits of length 18, 12 orbits of length 45 and 24 orbits of length 90. Let R be formed by the collection Φ of these orbits. By Proposition 2.2.2, since orbits of length 5, 10, 45 and 90 consist of elements whose first component is same, so they are not in Φ. Then we are left by orbits whose elements have 0 in the second component. Now by Proposition 2.2.1, we obtain $s_0^2 = 376$ and $s_0 = 94$, which is inconsistent. This completes the proof. □

Proposition 2.3.5 *There does not exist almost 7-ary PS with period 100.*

Proof. Assume that there exists such an almost 7-ary PS with period 100. Using Theorem 1.2.1 we obtain an $(100, 7, 99, 98/7)$-RDS R in $\mathbb{Z}_{100} \times \mathbb{Z}_7$ relative to $\{0\} \times \mathbb{Z}_7$. By Theorem 2.1.2 we obtain that $t = 81$ is a multiplier of R. We tabulate the orbits of the action $x \to 81x$ in G in Table A.4 in Appendix. There are 20 orbits of length 1, 40 orbits of length 3, 32 orbits of length 15 and 16 orbits of length 5. Let R be formed by the collection Φ of these orbits. By Proposition 2.2.2, since orbits of length 3 and 15 consist of elements whose first component are same, so they are not in Φ. Then we are left by orbits whose elements have 0 in the second component. Now by Proposition 2.2.1, we get $s_0^2 = 1485$ and $s_0 = 99$, which is inconsistent. This completes the proof. □

Proposition 2.3.6 *There does not exist almost 3-ary PS with period 77.*

Proof. By Theorem 1.2.1, it is equivalent to prove that there does not exist (77,3,76,25)-RDS in $G = \mathbb{Z}_{77} \times \mathbb{Z}_3$ relative to $\{0\} \times \mathbb{Z}_3$. Assume there exists a (77,3,76,25)-RDS in G, say R. It can be checked that 4 is a multiplier of R by Theorem 2.1.2. We compute 27 orbits of G under the group automorphism $x \to 4x$. There are 3 orbits of length 1, 6 orbits of length 3, 6 orbits of length 5 and 12 orbits of length 15. We know that R is a subset in the set of the orbits, Ω. We have $|R| = 76$. According to Table A.5, there are some possible subsets of Ω of total cardinality 76. However, by Proposition 2.2.2, one can not include two orbits having same first components. Therefore, a subset of cardinality 76 can only consist of orbits having length 15,15,15,15,5,5,3,3. For such a combination, we have 3^8 distinct subsets.

Let s_0, s_1 and s_2 be numbers as defined in Proposition 2.2.1, then we have two new constraints on the set R:

$$s_0^2 + s_1^2 + s_2^2 = 1976,$$
$$s_1 s_0 + s_2 s_1 + s_0 s_2 = 1900.$$

The solution set of the above system is $\{(20, 26, 30), (20, 30, 26), (26, 20, 30), (26, 30, 20), (30, 20, 26), (30, 26, 20)\}$. Now, we calculate the number of possible subsets of Ω having number of 0s,1s, and 2s as given in the solution set. For instance, let us calculate number of possible subsets having $(s_0, s_1, s_2) = (20, 26, 30)$. We have already observed that in our case possible orbit combination can only consist of orbits of length 15,15,15,15,5,5,3,3 with each of them has distinct first components. Now, under this observations, one can choose 20 many 0s by selecting orbits of length 15 and 5, which can be done in 8 different ways. Next, one can choose 26 many 1s by selecting orbits of length 15,5,3,3 from the remaining sets, which can be done in 3 different ways. And finally, 30 many 2s can be chosen uniquely. Therefore, one can choose 24 distinct possible sets of R satisfying $(s_0, s_1, s_2) = (20, 26, 30)$. Similarly, 24 distinct possible sets can be selected for the other solutions. Thus, we have totally 144 different possible sets satisfying the constraints. Finally, we checked by computer that none of 144 possible sets of R is an RDS. This completes the proof. □

Proposition 2.3.7 *There does not exist almost 11-ary PS with period 101.*

Proof. We will show that there does not exist (101,11,100,9)-RDS in $G = \mathbb{Z}_{101} \times \mathbb{Z}_{11}$ relative to $\mathbb{Z}_{11}$ as in the previous propositions. Assume there exists a (101,11,100,9)-RDS in G, say R. It can be checked that 5 is a multiplier of R by Theorem 2.1.2. We compute 47 orbits of G under the group automorphism $x \to 5x$. There are 1 orbit of length 1, 44 orbits of length 25 and 2 orbits of length 5. We know that R is a subset of the set of the orbits, hence there are 2^{47} distinct subsets. We have $|R| = 100$. Therefore, a subset of length 100 can only consist of orbits having length 25. However, by Proposition 2.2.2, one can not include two orbits having same first components. And, as $\mathbb{Z}_{101}\backslash\{0\}$ has 100 elements, set of orbits of length 25 can be divided in to 4 subsets which have first components from the same set, denote these subsets as $\Omega_1, \Omega_2, \Omega_3$ and Ω_4. This is also seen in Table A.6. This reduces the number of possible subsets to the $11^4 \approx 2^{14}$. Furthermore, each Ω_i can be divided in to 3 subsets, say $\Phi_{i1}, \Phi_{i2}, \Phi_{i3}$, $i = 1, 2, 3, 4$. These subsets are formed as Φ_{i1} consists of elements having 0 as a second component, Φ_{i2} consists of elements having $\{2, 6, 10, 7, 8\}$ as second component, and Φ_{i3} consists of elements having $\{1, 5, 4, 9, 3\}$ as second component. Let k_1, k_2, k_3 be the number of orbits in R from the sets $\{\Phi_{11}, \Phi_{21}, \Phi_{31}, \Phi_{41}\}, \{\Phi_{12}, \Phi_{22}, \Phi_{32}, \Phi_{42}\}, \{\Phi_{13}, \Phi_{23}, \Phi_{33}, \Phi_{43}\}$, respectively. Then,

$$k_1 + k_2 + k_3 = 4. \tag{2.8}$$

By Proposition 2.2.1, we have the following equality

$$s_0^2 + s_1^2 + \ldots + s_{10}^2 = 1000,$$

where s_i is defined as in Proposition 2.2.1, $i = 0, 1, \ldots, 10$. In this case, second components of elements in the sets $\Phi_{12}, \Phi_{22}, \Phi_{32}, \Phi_{42}, \Phi_{13}, \Phi_{23}, \Phi_{33}$ and Φ_{43} repeats five times, and we have 25 times 0s as a second component in each element of $\Phi_{11}, \Phi_{21}, \Phi_{31}$ and Φ_{41}. Then, we have

$$(25k_1)^2 + 5(5k_2)^2 + 5(5k_3)^2 = 1000$$

which reduces to

$$5k_1^2 + k_2^2 + k_3^2 = 40. \tag{2.9}$$

Equations (2.8) and (2.9) has a unique solution $\{(0, 2, 2)\}$.

Subsets of orbits satisfying $(k_1, k_2, k_3) = (0, 2, 2)$ can be chosen as follows. $k_1 = 2$ sets can be chosen among sets $\Omega_1, \Omega_2, \Omega_3$ and Ω_4 as $\begin{pmatrix} 4 \\ 2 \end{pmatrix}$. And, $k_2 = 2$ sets can be chosen among the

remaining sets uniquely. Then, for a chosen $k_i = 2$ sets as $\Omega_{i_1}, \Omega_{i_2}$, we have 5 distinct possible sets in each $\Phi_{i_l i}$ for each $k_i, i = 1, 2$ and $l = 1, 2$. Therefore, number of subsets becomes

$$\begin{pmatrix} 4 \\ 2 \end{pmatrix} \cdot 5 \cdot 5 \cdot 5 \cdot 5 = 6 \cdot 5^4 = 3750.$$

Finally, we checked by computer that none of the possible 3750 subsets of the orbits is an RDS. This completes the proof. □

CHAPTER 3

NONEXISTENCE OF ALMOST p-ARY NEARLY PERFECT SEQUENCES OF TYPE II

In this chapter we give an answer to Question 1.1.2 for $p = 2$, $p = 3$ and $p = 5$ at certain values of n. In other words, we prove non-existence of NPS of type II for $p = 2$, $p = 3$ and $p = 5$ with period $n + 1$ for certain values of n. Our method is based on the approach of [6] in using direct product difference sets (see Theorem 1.2.2). We use extra arguments that we obtain by extending Proposition 2.2.1 to the direct product difference sets, which is stated as Proposition 3.1.1 of Section 3.1 below. We combine Theorem 1.2.2 and Proposition 3.1.1 in Corollary 3.1.2. Using this corollary we obtain a set of Diophantine equations in integers, and we prove the nonexistence as a consequence of the inconsistency of the obtained Diophantine equations for $p = 2$, $p = 3$ and $p = 5$ at certain values of n (see Theorem 3.2.1, Theorem 3.3.1, Theorem 3.3.4, Theorem 3.4.1, and Theorem 3.4.4).

We prove our results answering Question 1.1.2 for $p = 2$, $p = 3$ and $p = 5$ in Section 3.2, Section 3.3 and Section 3.4, respectively. Theorem 1.2.2 gives a way showing existence and nonexistence of nearly perfect sequences in terms of direct product difference sets. We will use this method in Section 3.2, Section 3.3 and Section 3.4 to show nonexistence of NPS of type II for some values of n when $p = 2$, $p = 3$ and $p = 5$, respectively.

3.1 Direct Product Difference Sets

In this section we obtain a system of equations for direct product difference sets. We state this property in the next proposition.

Proposition 3.1.1 *Let R be an $(m_1, m_2, k, \lambda_1, \lambda_2, \mu)$-DPDS in $G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ relative to $H = \mathbb{Z}_{m_1}$ and $N = \mathbb{Z}_{m_2}$. Let R have s_j many elements having j in the second component for $j = 0, 1, 2, \ldots, m_2 - 1$. Then $\sum_{j=0}^{m_2-1} s_j^2 = (m_1 - 1)\lambda_1 + k$ and $\sum_{j=0}^{m_2-1} s_j s_{j-i} = (m_1 - 1)\mu + \lambda_2$ for each $i = 1, 2, \ldots, \lceil (m_2 - 1)/2 \rceil$, where subscripts are computed modulo m_2.*

Proof. Let φ be the map from $G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ to $\mathbb{Z}_{m_2}$ sending (a, i) to i. Let V be the multiset consisting of the images (counting multiplicities) of φ restricted to R. By reordering on V we have

$$V = \{* \underbrace{0, 0, \ldots, 0}_{s_0}, \underbrace{1, 1, \ldots, 1}_{s_1}, \underbrace{2, 2, \ldots, 2}_{s_2}, \ldots, \underbrace{m_2 - 1, m_2 - 1, \ldots, m_2 - 1}_{s_{m_2-1}} *\}.$$

In other words,

$$s_0 = |\{(b, i) \in R : i = 0\}|, \ldots, s_{m_2-1} = |\{(b, i) \in R : i = m_2 - 1\}|.$$

Then it is clear that

$$s_0 + s_1 \ldots + s_{m_2-1} = |R| = k. \tag{3.1}$$

For $1 \leq i \leq m_2 - 1$, let T_i be the subset of $G \backslash (H \cup N)$ defined as $T_i = \{(a, e) \in G \backslash (H \cup N) : e = i\}$. And, we define an other set V_i as $V_i = \{(0, i) \in N\}$. It is clear that $T_i = \{(a, i) : a \in Z_{m_1} \backslash \{0\}\}$ and hence

$$|T_i| = m_1 - 1. \tag{3.2}$$

Moreover, let $\mathcal{T}_i$ be the subset of $R \times R$ defined as

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

As R is an $(m_1, m_2, k, \lambda_1, \lambda_2, \mu)$-DPDS, each element of V_i occurs in $\mathcal{T}_i$ exactly λ_2 times. Then, for the cardinality $|\mathcal{T}_i|$ of $\mathcal{T}_i$, using (3.2), we obtain that

$$|\mathcal{T}_i| = \mu |T_i| + \lambda_2 = \mu(m_1 - 1) + \lambda_2. \tag{3.3}$$

Similarly, for the cardinality $|\mathcal{T}_0|$ of $\mathcal{T}_0$, we obtain that

$$|\mathcal{T}_0| = \lambda_1 |T_0| = \lambda_1 (m_1 - 1). \tag{3.4}$$

For $1 \leq i \leq m_2 - 1$ and $0 \leq j \leq m_2 - 1$, let $\mathcal{T}_{i,j}$ be the subset of $\mathcal{T}_i$ defined as

$$\mathcal{T}_{i,j} = \{(\beta_1, \beta_2) \in \mathcal{T}_i : \varphi(\beta_1) = j\}.$$

Then we have

$$|\mathcal{T}_i| = \sum_{j=0}^{m_2-1} |\mathcal{T}_{i,j}|. \tag{3.5}$$

Next we determine $\mathcal{T}_{i,j}$ for $0 \leq i, j \leq m_2 - 1$ and $i \neq 0$. Note that $(\beta_1, \beta_2) \in \mathcal{T}_{i,j}$ if and only if $\beta_1 \in R$, $\varphi(\beta_1) = j$ and $\beta_2 \in R$, $\varphi(\beta_2) = j - i$. Here, $\beta_1 \neq \beta_2$ automatically as $i \neq 0$. Recall that

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

where we define the subscript $j - i$ modulo m_2. Therefore using (3.3) and (3.5) we conclude that

$$(m_1 - 1)\mu + \lambda_2 = \sum_{j=0}^{m_2-1} s_j s_{j-i}. \tag{3.6}$$

Note that it is enough to consider the subset of equations in (3.6) corresponding to $1 \leq i \leq \left\lceil \frac{m_2-1}{2} \right\rceil$ since each equation in (3.6) with $\left\lceil \frac{m_2-1}{2} \right\rceil < i \leq m_2 - 1$ is the same as an equation in (3.6) with $1 \leq i \leq \left\lceil \frac{m_2-1}{2} \right\rceil$.

Finally, we determine $\mathcal{T}_{0,j}$ for $0 \leq j \leq m_2 - 1$. Note that $(\beta_1, \beta_2) \in \mathcal{T}_{0,j}$ if and only if $\beta_1 \in R$, $\varphi(\beta_1) = j$ and $\beta_2 \in R$, $\varphi(\beta_2) = j$ and $\beta_1 \neq \beta_2$. Hence, we get that for $0 \leq j \leq m_2 - 1$

$$|\mathcal{T}_{0,j}| = s_j(s_j - 1).$$

Then using (3.1), (3.4) and (3.5) we conclude that

$$(m_1 - 1)\lambda_1 = \sum_{j=0}^{m_2-1} s_j(s_j - 1) = \sum_{j=0}^{m_2-1} (s_j^2 - s_j) = \sum_{j=0}^{m_2-1} s_j^2 - \sum_{j=0}^{m_2-1} s_j = \sum_{j=0}^{m_2-1} s_j^2 - k,$$

and hence

$$\sum_{j=0}^{m_2-1} s_j^2 = (m_1 - 1)\lambda_1 + k.$$

□

Proposition 3.1.1 together with Theorem 1.2.2 imply a nice property of nearly perfect sequences.

Corollary 3.1.2 *Let $p, n, G, \underline{a}$ and R be defined as in Theorem 1.2.2. Let R have s_j many elements having j in the second component for $j = 0, 1, 2, \ldots, p - 1$. Then*

(i.) If $\underline{a}$ is an almost p-ary NPS of type I, then following equalities hold

$$\sum_{j=0}^{p-1} s_j s_{j-i} = \frac{n^2}{p} \text{ for each } i = 0, 1, 2, \ldots, \lceil (p-1)/2 \rceil . \tag{3.7}$$

(ii.) If $\underline{a}$ is an almost p-ary NPS of type II, then following equalities hold

$$\sum_{j=0}^{p-1} s_j^2 = \frac{n(n-2)}{p} + 2n \tag{3.8}$$

and

$$\sum_{j=0}^{p-1} s_j s_{j-i} = \frac{n(n-2)}{p} \text{ for each } i = 1, 2, \ldots, \lceil (p-1)/2 \rceil . \tag{3.9}$$

Let p be a prime number and $n \in \mathbb{Z}^+$ be divisible by p. We note that a tuple $(s_0, s_1, s_2, \ldots, s_{p-1})$ such that $s_j = \frac{n}{p}$ is a solution to the system of equations given in (3.7). However, there are some integers n such that system of equations given in (3.8) and (3.9) does not have a solution. This directly implies the nonexistence of almost p-ary NPS of type II with period $n+1$. Hence, in the remaining sections we will study the nonexistence of almost p-ary NPS of type II for some periods $n+1$.

3.2 Nonexistence of certain almost binary NPS of type II

In this section we will show that almost binary NPS of type II with period $n+1$ does not exist if $n/2$ is not a square integer.

Theorem 3.2.1 *Let n be an even positive integer such that $n/2$ is non-square. Then, there do not exist almost binary nearly perfect sequence of type II with period $n+1$.*

Proof. Assume that there exists an almost binary nearly perfect sequence of type II with period $n+1$ where $n/2$ is not a square. Then, by Corollary 3.1.2(ii) we have equalities (3.8) and (3.9) for $p = 2$ as follows

$$\begin{aligned} s_0 + s_1 &= n \\ s_0^2 + s_1^2 &= \frac{n^2 + 2n}{2} \end{aligned} \tag{3.10}$$

for some nonnegative integers s_0 and s_1. By substituting $s_0 = n - s_1$ into second equality of (3.10) we obtain that

$$s_1^2 - ns_1 + \frac{n^2 - 2n}{4} = 0. \tag{3.11}$$

Discriminant of (3.11) is $2n$. Therefore, (3.11) has a solution over integers when $2n$ is a square. However, this contradicts the condition that $n/2$ is not a square. □

3.3 Nonexistence of certain almost 3-ary NPS of type II

In this section we will show that almost p-ary NPS of type II with period $n + 1$ does not exist for certain values of n for $p = 3$.

Theorem 3.3.1 *Let n be a positive integer such that $n \equiv 5 \cdot 2^{2m-2}$ mod $3 \cdot 2^{2m-1}$ for some $m \in \mathbb{Z}^+$. Then, there do not exist almost 3-ary nearly perfect sequence of type II with period $n + 1$.*

In order to prove above theorem we state following two lemmas.

Lemma 3.3.2 *Let $p = 2$ and let s_0, s_1 and s_2 be nonnegative integers satisfying*

$$p^m \mid s_0 + s_1 + s_2 \tag{3.12}$$

$$p^{2m-1} \mid s_0s_1 + s_0s_2 + s_1s_2 \tag{3.13}$$

for some integer $m \geq 1$. Then $p^m \mid s_j$ for all $j = 0, 1, 2$, and so $p^{2m} \mid s_0s_1 + s_0s_2 + s_1s_2$.

Proof. We prove by induction on integer m. We first show that it holds for $m = 1$. As the sum $s_0 + s_1 + s_2$ is an even integer, either only one of s_0, s_1, s_2 is even or all of s_0, s_1, s_2 are even. If the former case holds, then $s_0s_1 + s_0s_2 + s_1s_2$ becomes an odd integer, which contradicts to (3.13). Assume that it holds for for the case $m = i$ for some integer $i \geq 2$. Now, let us consider the case $m = i + 1$. Let the following statements hold

$$\begin{aligned} 2^{i+1} &\mid s_0 + s_1 + s_2 \\ 2^{2(i+1)-1} &\mid s_0s_1 + s_0s_2 + s_1s_2. \end{aligned} \tag{3.14}$$

Then, by induction step we have

$$2^i \mid s_j \text{ for all } j = 0, 1, 2.$$

Let $s_j = 2^i k_j$ for some integer k_j and $j = 0, 1, 2$. Then, (3.14) reduces to

$$2 \mid k_0 + k_1 + k_2$$
$$2 \mid k_0k_1 + k_0k_2 + k_1k_2.$$

By the first step of the induction, we have $2 \mid k_j$ for all $j = 0, 1, 2$. Hence, we observe the required result $2^{i+1} \mid s_j$ for all $j = 0, 1, 2$. Therefore we complete the proof. □

Lemma 3.3.3 *Let n be an integer satisfying $n \equiv 5 \cdot 2^{2m-2}$ mod $3 \cdot 2^{2m-1}$ for some $m \in \mathbb{Z}^+$. Then the system of equations in variables s_0, s_1, s_2*

$$\begin{aligned} s_0 + s_1 + s_2 &= n \\ s_0s_1 + s_0s_2 + s_1s_2 &= \frac{n(n-2)}{3} \end{aligned} \tag{3.15}$$

has no solution over $\mathbb{Z}^+ \cup \{0\}$.

Proof. We prove by contradiction. Assume that s_0, s_1, s_2 is a solution to (3.15). Let $n = 3 \cdot 2^{2m-1}k + 5 \cdot 2^{2m-2}$ for some nonnegative integer k.

First of all consider the case $m = 1$. In this case, $n = 6k + 5$. Hence, n is an odd integer. Since sum of s_0, s_1 and s_2 is an odd integer, either only one of them is odd or all of them are odd. We will show that both of these cases are not possible. Suppose that only one of s_0, s_1 and s_2 is an odd integer. Without loss of generality, let s_0 be odd and others be even. Then the sum

$$s_0s_1 + s_0s_2 + s_1s_2$$

becomes even. This contradicts to the second equality of (3.15), whose right hand side is an odd integer for an odd n.

Next suppose that all of s_0, s_1 and s_2 are odd integers. Let they satisfy

$$s_0 = 6k_0 + 2a_0 + 1$$
$$s_1 = 6k_1 + 2a_1 + 1$$
$$s_2 = 6k_2 + 2a_2 + 1$$

for some nonnegative integers k_0, k_1, k_2 and a_0, a_1, a_2.

Now, we check both sides of the equality

$$s_0s_1 + s_0s_2 + s_1s_2 \quad = \quad \frac{n(n-2)}{3}$$

modulo 4. We substitute s_j for $j = 0, 1, 2$ into left hand side of the equation. We obtain that

$$\begin{aligned}
s_0s_1 + s_0s_2 + s_1s_2 &= 36(k_0k_2 + k_1k_0 + k_2k_1) \\
&\quad +6(k_0(2a_2 + 1) + k_0(2a_1 + 1) \\
&\qquad +k_1(2a_0 + 1) + k_1(2a_2 + 1) \\
&\qquad +k_2(2a_1 + 1) + k_2(2a_0 + 1)) \\
&\quad +4a_0a_2 + 2a_0 + 2a_2 + 1 + 4a_1a_0 + 2a_1 + 2a_0 + 1 \\
&\quad +4a_2a_1 + 2a_2 + 2a_1 + 1 \\
&= 36(k_0k_2 + k_1k_0 + k_2k_1) \\
&\quad +12(k_0(a_2 + a_1 + 1) + k_1(a_0 + a_2 + 1) \\
&\qquad +k_2(a_1 + a_0 + 1)) \\
&\quad +4(a_0a_2 + a_0a_1 + a_1a_2 + a_0 + a_2 + a_1) + 3
\end{aligned}$$

On the other hand, we have

$$\frac{n(n-2)}{3} = (6k + 5)(2k + 1) = 12k^2 + 16k + 5$$

However, both sides of the above equation are not equal to each other modulo 4. This shows that the case that all of s_0, s_1 and s_2 are odd integers is also not possible. Therefore, we complete the proof of the case $m = 1$.

Next, we consider the case $m \geq 2$. As $n = 3 \cdot 2^{2m-1}k + 5 \cdot 2^{2m-2}$ is divisible by 2^{2m-2}, we also have

$$\begin{aligned}
\frac{n(n-2)}{3} &= \frac{(3 \cdot 2^{2m-1}k + 5 \cdot 2^{2m-2})(3 \cdot 2^{2m-1}k + 5 \cdot 2^{2m-2} - 2)}{3} \\
&= \frac{2(3 \cdot 2^{2m-1}k + 5 \cdot 2^{2m-2})(3 \cdot 2^{2m-2}k + 5 \cdot 2^{2m-3} - 1)}{3}
\end{aligned}$$

is divisible by 2^{2m-1}, but not divisible by 2^{2m}. Then, by Lemma 3.3.2 we obtain that 2^{2m} must divide $s_0s_1 + s_0s_2 + s_1s_2$. On the other hand, this contradicts to the condition that $\frac{n(n-2)}{3}$ is not divisible by 2^{2m}. Therefore we complete the proof. □

Proof of Theorem 3.3.1 Assume that there exist an almost 3-ary nearly perfect sequence of type II with period $n+1$ where $n \equiv 5 \cdot 2^{2m-2} \bmod 3 \cdot 2^{2m-1}$ for some $m \in \mathbb{Z}^+$. Then, by Corollary 3.1.2(ii) we have equalities (3.8) and (3.9). However, by Lemma 3.3.3 we know that these equalities have no solution over $\mathbb{Z}^+ \cup \{0\}$, which is a contradiction. □

It is easy to observe that Lemma 3.3.2 is also valid for any $p \equiv 2 \bmod 3$ (see Lemma 3.3.5 below), and so we also have the following nonexistence result.

Theorem 3.3.4 *Let $p > 3$ be a prime number such that $p \equiv 2$ mod 3. Let n be an integer such that $n \equiv p^{2m-1}$ mod $3 \cdot p^{2m}$ for some $m \in \mathbb{Z}^+$. Then, there do not exist almost 3-ary nearly perfect sequence of type II with period $n+1$.*

The proof of this theorem is very similar to the proof of Theorem 3.3.1. To do that, we first need to state and prove similar results. Then proof of Theorem 3.3.4 will be a direct consequence of these results.

Lemma 3.3.5 *Let $p > 3$ be a prime number such that $p \equiv 2$ mod 3, and let s_0, s_1 and s_2 be nonnegative integers satisfying*

$$p^m \mid s_0 + s_1 + s_2 \tag{3.16}$$

$$p^{2m-1} \mid s_0 s_1 + s_0 s_2 + s_1 s_2 \tag{3.17}$$

for some integer $m \geq 1$. Then $p^m \mid s_j$ for all $j = 0, 1, 2$, and so $p^{2m} \mid s_0 s_1 + s_0 s_2 + s_1 s_2$.

Proof. We first show that it holds for $m = 1$, then it will follow by induction. As the sum $s_0 + s_1 + s_2$ is divisible by p, we have three cases

(i.) Only one of s_0, s_1, s_2 is equivalent to 0 modulo p,

(ii.) None of s_0, s_1, s_2 is equivalent to 0 modulo p, or

(iii.) All of s_0, s_1, s_2 are equivalent to 0 modulo p.

If the first case holds, then $s_0 s_1 + s_0 s_2 + s_1 s_2$ would equal to a nonzero integer modulo p, which contradicts to (3.17).

Now, we will observe that case (ii.) is also not possible. Assume it holds, then we have $s_2 \equiv -(s_0 + s_1) \bmod p$. Substitute this into (3.17), and obtain the equivalence

$$s_0^2 + s_0 s_1 + s_1^2 \equiv 0 \bmod p. \tag{3.18}$$

As $p \nmid s_1$, (3.18) is a quadratic equivalence

$$(\frac{s_0}{s_1})^2 + \frac{s_0}{s_1} + 1 \equiv 0 \bmod p. \tag{3.19}$$

Discriminant of (3.19) equals to -3, which is not quadratic residue modulo p for $p \equiv 2 \bmod 3$ and $p > 3$. Hence, (3.19) has no solution, and so case (ii.) is not possible.

Therefore, only case (iii.) is possible. This proves the first case m=1 of the induction.

Assume that it holds for the case $m = i$ for some integer $i \geq 2$. Now, let us consider the case $m = i + 1$. Let the following statements hold

$$\begin{aligned} p^{i+1} &\mid s_0 + s_1 + s_2 \\ p^{2(i+1)-1} &\mid s_0 s_1 + s_0 s_2 + s_1 s_2. \end{aligned} \tag{3.20}$$

Then, by induction step we have

$$p^i \mid s_j \text{ for all } j = 0, 1, 2.$$

Let $s_j = p^i k_j$ for some integer k_j and $j = 0, 1, 2$. Then, (3.20) reduces to

$$\begin{aligned} p &\mid k_0 + k_1 + k_2 \\ p &\mid k_0 k_1 + k_0 k_2 + k_1 k_2. \end{aligned}$$

By the first step of the induction, we have $p \mid k_j$ for all $j = 0, 1, 2$. Hence, we observe the required result $p^{i+1} \mid s_j$ for all $j = 0, 1, 2$. Therefore we complete the proof. □

Lemma 3.3.6 *Let $p > 3$ be a prime number such that $p \equiv 2$ mod 3. Let n be an integer satisfying $n \equiv p^{2m-1}$ mod $3 \cdot p^{2m}$ for some $m \in \mathbb{Z}^+$. Then the system of equations in variables s_0, s_1, s_2*

$$\begin{aligned} s_0 + s_1 + s_2 &= n \\ s_0 s_1 + s_0 s_2 + s_1 s_2 &= \frac{n(n-2)}{3} \end{aligned} \tag{3.21}$$

has no solution over $\mathbb{Z}^+ \cup \{0\}$.

Proof. We prove by contradiction. Assume that s_0, s_1, s_2 is a solution to (3.21). Let $n = 3 \cdot p^{2m}k + p^{2m-1}$ for some nonnegative integer k. As n is divisible by p^{2m-1}, we also have

$$\frac{n(n-2)}{3} = \frac{(3 \cdot p^{2m}k + p^{2m-1})(3 \cdot p^{2m}k + p^{2m-1} - 2)}{3}$$

is divisible by p^{2m-1}, but not divisible by p^{2m}. However, Lemma 3.3.5 implies that p^{2m} must divide $s_0s_1 + s_0s_2 + s_1s_2$. This contradicts to the condition that $\frac{n(n-2)}{3}$ is not divisible by p^{2m}. Therefore we complete the proof. □

We now list values of $n \leq 1000$ for which 3-ary NPS of type II with period $n+1$ is not existing in Table A.7. Each n value presented in the table satisfies either Theorem 3.3.1 or Theorem 3.3.4, which is also indicated in the Existence column. We list values upto $n \leq 1000$ to show the coverage of Theorems 3.3.1 and 3.3.4 explicitly. Existence status in the remaining values of n are not known.

3.4 Nonexistence of certain almost 5-ary NPS of type II

In this section we present analogue results of those we obtained in the 3-ary case. Here we will deal with the nonexistence of almost 5-ary NPS type II.

Theorem 3.4.1 *Let n be an integer satisfying one of the following congruences*

(i.) $n \equiv 7 \cdot 2^{4m-4}$ *mod* $5 \cdot 2^{4m-3}$

(ii.) $n \equiv 3 \cdot 2^{4m-2}$ *mod* $5 \cdot 2^{4m-1}$

for some integer $m \geq 1$. *Then, there do not exist almost* 5*-ary nearly perfect sequence of type II with period* $n + 1$.

We prove two lemmas useful in proving the above theorem.

Lemma 3.4.2 *Let* $p = 2$ *and let* s_0, s_1, s_2, s_3 *and* s_4 *be positive integers satisfying each of the following*

$$p^m \mid s_0 + s_1 + s_2 + s_3 + s_4 \tag{3.22}$$

$$p^{2m-1} \mid s_0s_4 + s_1s_0 + s_2s_1 + s_3s_2 + s_4s_3 \tag{3.23}$$

$$p^{2m-1} \mid s_0s_3 + s_1s_4 + s_2s_0 + s_3s_1 + s_4s_2 \tag{3.24}$$

for some $m \geq 1$. *Then* $p^m \mid s_j$ *for all* $j = 0, 1, 2, 3, 4$ *and so* $p^{2m} \mid s_0s_4 + s_1s_0 + s_2s_1 + s_3s_2 + s_4s_3$ *and* $p^{2m} \mid s_0s_3 + s_1s_4 + s_2s_0 + s_3s_1 + s_4s_2$.

Proof. We prove by induction on integer m. First, consider the case $m = 1$. As sum of s_0, s_1, s_2, s_3, s_4 is an even integer, one of the following cases to be satisfied:

(i.) Only one of s_0, s_1, s_2, s_3, s_4 is even.

(ii.) Three of s_0, s_1, s_2, s_3, s_4 are even.

(iii.) All of s_0, s_1, s_2, s_3, s_4 are even.

First case forces $s_0s_4 + s_1s_0 + s_2s_1 + s_3s_2 + s_4s_3$ to be an odd integer, which is a contradiction to (3.23). Similarly, second case makes either $s_0s_4 + s_1s_0 + s_2s_1 + s_3s_2 + s_4s_3$ or $s_0s_3 + s_1s_4 + s_2s_0 + s_3s_1 + s_4s_2$ an odd integer, which is a contradiction to (3.23) or (3.24), respectively. Therefore, only the third case can be valid. This proves the case $m = 1$.

Assume that it holds for the case $m = i$ for some integer $i \geq 2$. Now, let us consider the case $m = i + 1$. Let the following hold

$$\begin{aligned} 2^{i+1} &\mid s_0 + s_1 + s_2 + s_3 + s_4, \\ 2^{2(i+1)-1} &\mid s_0s_4 + s_1s_0 + s_2s_1 + s_3s_2 + s_4s_3, \\ 2^{2(i+1)-1} &\mid s_0s_3 + s_1s_4 + s_2s_0 + s_3s_1 + s_4s_2. \end{aligned} \tag{3.25}$$

Then, by induction step we have

$$2^i \mid s_j \text{ for all } j = 0, 1, 2, 3, 4.$$

Let $s_j = 2^i k_j$ for some integer k_j and $j = 0, 1, 2, 3, 4$. Then, (3.25) reduces to

$$\begin{aligned} 2 &\mid k_0 + k_1 + k_2 + k_3 + k_4, \\ 2 &\mid k_0k_4 + k_1k_0 + k_2k_1 + k_3k_2 + k_4k_3, \\ 2 &\mid k_0k_3 + k_1k_4 + k_2k_0 + k_3k_1 + k_4k_2. \end{aligned} \tag{3.26}$$

By the first step of the induction, we have $2 \mid k_j$ for all $j = 0, 1, 2, 3, 4$. Hence, we observe the required result $2^{i+1} \mid s_j$ for all $j = 0, 1, 2, 3, 4$. Therefore we complete the proof. ■

Lemma 3.4.3 *Let n be an integer satisfying one of the following*

(i.) $n \equiv 7 \cdot 2^{4m-4}$ *mod* $5 \cdot 2^{4m-3}$

(ii.) $n \equiv 3 \cdot 2^{4m-2}$ *mod* $5 \cdot 2^{4m-1}$

for some integer $m \geq 1$. *Then the system of equations in variables* s_0, s_1, s_2, s_3, s_4

$$\begin{aligned} s_0 + s_1 + s_2 + s_3 + s_4 &= n \\ s_0s_4 + s_1s_0 + s_2s_1 + s_3s_2 + s_4s_3 &= \frac{n(n-2)}{5} \\ s_0s_3 + s_1s_4 + s_2s_0 + s_3s_1 + s_4s_2 &= \frac{n(n-2)}{5} \end{aligned} \tag{3.27}$$

has no solution over $\mathbb{Z}^+ \cup \{0\}$.

Proof.

(i.) We will prove by contradiction. Assume that $(s_0, s_1, s_2, s_3, s_4)$ is a solution to (3.27). Let n satisfy $n = 5 \cdot 2^{4m-3}k + 7 \cdot 2^{4m-4}$ for some nonnegative integer k.

We will first deal with the case $m = 1$. In this case $n = 10k + 7$ is an odd integer, and so integers on the right hand side of the each equalities of (3.27) are odd. So, left hand sides are also odd integers. By this observation and first equality of (3.27), we say that number of odd integer $s_j \in \{s_0, s_1, \ldots, s_4\}$ is an odd integer. In fact, none of them can be an even integer. Because otherwise left hand sides of second or third equation becomes even. Hence, all of $\{s_0, s_1, \ldots, s_4\}$ are odd integers. Let they satisfy

$$\begin{aligned} s_0 &= 10k_0 + 2a_0 + 1 \\ s_1 &= 10k_1 + 2a_1 + 1 \\ &\vdots \\ s_4 &= 10k_4 + 2a_4 + 1 \end{aligned}$$

for some nonnegative integers $k_0, k_1, \ldots, k_4$ and $a_0, a_1, \ldots, a_4$. Now, we check both sides of the equality

$$s_0s_4 + s_1s_0 + s_2s_1 + s_3s_2 + s_4s_3 = \frac{n(n-2)}{5} \tag{3.28}$$

modulo 4. We substitute s_j for $j = 1, 2, \ldots, 4$ into left hand side of the equation. We

obtain that

$$\begin{aligned}
\textstyle\sum_{j=0}^{4} s_j s_{j-1} &= 100(k_0k_4 + k_1k_0 + \ldots + k_4k_3) \\
&\quad +10(k_0(2a_4 + 1) + k_0(2a_1 + 1) + \ldots \\
&\quad\quad +k_4(2a_3 + 1) + k_4(2a_0 + 1)) \\
&\quad +4a_0a_4 + 2a_0 + 2a_4 + 1 + \ldots \\
&\quad\quad +4a_4a_3 + 2a_4 + 2a_3 + 1 \\
&= 100(k_0k_4 + k_1k_0 + \ldots + k_4k_3) \\
&\quad +20(k_0(a_1 + a_4 + 1) + \ldots + k_4(a_0 + a_3 + 1)) \\
&\quad +4(a_0a_4 + \ldots + a_4a_3 + a_0 + \ldots + a_4) + 5
\end{aligned}$$

On the other hand, we have

$$\frac{n(n-2)}{5} = (10k + 7)(2k + 1) = 20k^2 + 24pk + 7$$

We observed that both sides of equation (3.28) modulo 4 are not equal to each other, which is a contradiction. Therefore, this completes the proof of case $m = 1$.

Next, we consider the case $m \geq 2$. As $n = 5 \cdot 2^{4m-3}k + 7 \cdot 2^{4m-4}$ is divisible by $2^{2(2m-2)}$, we also have

$$\begin{aligned}
\frac{n(n-2)}{5} &= \frac{(5 \cdot 2^{4m-3}k + 7 \cdot 2^{4m-4})(5 \cdot 2^{4m-3}k + 7 \cdot 2^{4m-4} - 2)}{5} \\
&= \frac{2(5 \cdot 2^{4m-3}k + 7 \cdot 2^{4m-4})(5 \cdot 2^{4m-4}k + 7 \cdot 2^{4m-3} - 1)}{5}
\end{aligned}$$

is divisible by $2^{2(2m-2)+1} = 2^{2(2m-1)-1}$, but not divisible by $2^{2(2m-1)}$. Then, by Lemma 3.4.2 we obtain that $2^{2(2m-1)}$ must divide $s_0s_4 + s_1s_0 + s_2s_1 + s_3s_2 + s_4s_3$. On the other hand, this contradicts to the condition that $\frac{n(n-2)}{5}$ is not divisible by $2^{2(2m-1)}$. Therefore we complete the proof of (i).

(ii.) Assume that integers $s_0, s_1, s_2, s_3, s_4 \in \mathbb{Z}^+$ satisfy (3.27). Let $n = 5 \cdot 2^{4m-1}k + 3 \cdot 2^{4m-2}$ for some nonnegative integer k. In this case n is divisible by $2^{2(2m-1)}$. And, it is easy to see that

$$\begin{aligned}
\frac{n(n-2)}{5} &= \frac{(5 \cdot 2^{4m-1}k + 3 \cdot 2^{4m-2})(5 \cdot 2^{4m-1}k + 3 \cdot 2^{4m-2} - 2)}{5} \\
&= \frac{2(5 \cdot 2^{4m-1}k + 3 \cdot 2^{4m-2})(5 \cdot 2^{4m-2}k + 3 \cdot 2^{4m-3} - 1)}{5}
\end{aligned}$$

is divisible by $2^{2(2m-1)+1} = 2^{2(2m)-1}$, but not by 2^{4m}. On the other hand, we know that 2^{4m} must divide $s_0s_4+s_1s_0+s_2s_1+s_3s_2+s_4s_3$ by Lemma 3.4.2, which is a contradiction. Therefore we complete the proof of (ii).

□

Proof of Theorem 3.4.1 Similar to proof of Theorem 3.3.1, Lemma 3.4.3 and Corollary 3.1.2(ii) directly imply the result. □

Next, we extend Theorem 3.4.1 for general primes.

Theorem 3.4.4 *Let $p \neq 5$ be an odd prime number such that $p \not\equiv 1 \bmod 5$. Let n be an integer such that $n \equiv 2 \bmod 5$ and $n \equiv p^{2m-1} \bmod p^{2m}$ for some integer $m \geq 1$. Then, there do not exist almost 5-ary nearly perfect sequence of type II with period $n+1$.*

Proof of Theorem 3.4.4 is very similar to proof of Theorem 3.4.1, and it is direct consequence of Lemma 3.4.5 and Lemma 3.4.6.

Lemma 3.4.5 *Let $p \neq 5$ be an odd prime number such that $p \not\equiv 1 \bmod 5$, and let s_0, s_1, s_2, s_3 and s_4 be positive integers satisfying each of the following statements*

$$p^m \mid s_0 + s_1 + s_2 + s_3 + s_4 \tag{3.29}$$

$$p^{2m-1} \mid s_0s_4 + s_1s_0 + s_2s_1 + s_3s_2 + s_4s_3 \tag{3.30}$$

$$p^{2m-1} \mid s_0s_3 + s_1s_4 + s_2s_0 + s_3s_1 + s_4s_2 \tag{3.31}$$

for some $m \geq 1$. Then $p^m \mid s_j$ for all $j = 0, 1, 2, 3, 4$ and so $p^{2m} \mid s_0s_4+s_1s_0+s_2s_1+s_3s_2+s_4s_3$ and $p^{2m} \mid s_0s_3 + s_1s_4 + s_2s_0 + s_3s_1 + s_4s_2$.

Proof. We prove by induction on integer m. First, consider the case $m = 1$. We consider all the following cases:

(i.) Only one of s_0, s_1, s_2, s_3, s_4 is not divisible by p.

(ii.) Only two of s_0, s_1, s_2, s_3, s_4 are not divisible by p.

(iii.) Only three of s_0, s_1, s_2, s_3, s_4 are not divisible by p.

(iv.) Only four of s_0, s_1, s_2, s_3, s_4 are not divisible by p.

(v.) None of s_0, s_1, s_2, s_3, s_4 is divisible by p.

(vi.) All of s_0, s_1, s_2, s_3, s_4 are divisible by p.

We will show that first five cases are not possible under the assumptions of the lemma. To begin with, first case contradicts to (3.29). Next, we consider the second case. If elements divisible by p are consecutive, this case contradicts to (3.31), otherwise contradicts to (3.30). Similarly, for the third case, if elements divisible by p are consecutive, this case contradicts to (3.31), otherwise contradicts to (3.30).

Now, we need much effort to show that fourth case is also not possible. WLOG let only s_4 is divisible by p. Then, (3.29) implies that

$$s_0 \equiv -(s_1 + s_2 + s_3) \bmod p. \tag{3.32}$$

By substituting (3.32) into equations (3.30) and (3.31) we obtain the equivalences

$$\begin{aligned} s_1^2 + s_1 s_3 - s_2 s_3 &\equiv 0 \bmod p \\ s_3^2 + 2s_2 s_3 + s_2^2 + s_1 s_2 &\equiv 0 \bmod p. \end{aligned} \tag{3.33}$$

The system (3.33) has resultant

$$s_1^4 - s_1^3 s_2 + s_1^2 s_2^2 - s_1 s_2^3 + s_2^4 \tag{3.34}$$

with respect to s_3. If one divides (3.34) by nonzero s_2^4 then, it reduces to

$$(\frac{s_1}{s_2})^4 - (\frac{s_1}{s_2})^3 + (\frac{s_1}{s_2})^2 - (\frac{s_1}{s_2}) + 1. \tag{3.35}$$

Now, consider the polynomial

$$f(x) = x^4 - x^3 + x^2 - x + 1, \tag{3.36}$$

It's splitting field is cyclotomic field of 5-th root of unity as $p \neq 5$. The law of decomposition in cyclotomic field of degree 5 tells us that f splits completely modulo p if and only if $p \equiv 1 \bmod 5$ (see [12, Proposition 10.3]). However, this is not covered by the assumption of the lemma. Therefore, f is not solvable modulo p if $p \not\equiv 1 \bmod 5$. This implies that fourth case is not possible.

Next, we will show that fifth case is not possible. Now, we have following system of equations

$$\begin{aligned} &s_0 + s_1 + s_2 + s_3 + s_4 \equiv 0 \bmod p \\ &s_0s_4 + s_1s_0 + s_2s_1 + s_3s_2 + s_4s_3 \equiv 0 \bmod p \\ &s_0s_3 + s_1s_4 + s_2s_0 + s_3s_1 + s_4s_2 \equiv 0 \bmod p, \end{aligned} \tag{3.37}$$

and none of s_0, s_1, s_2, s_3, s_4 is divisible by p. We multiply first equation of (3.37) by s_0^{-1} and the others by $(s_0^{-1})^2$, and we apply the substitutions

$$b_1 = s_1s_0^{-1},\ b_2 = s_2s_0^{-1},\ b_3 = s_3s_0^{-1},\ b_4 = s_4s_0^{-1}$$

to them. Then, we observe the equalities

$$\begin{aligned} &1 + b_1 + b_2 + b_3 + b_4 \equiv 0 \bmod p \\ &b_4 + b_1 + b_2b_1 + b_3b_2 + b_4b_3 \equiv 0 \bmod p \\ &b_3 + b_1b_4 + b_2 + b_3b_1 + b_4b_2 \equiv 0 \bmod p \end{aligned} \tag{3.38}$$

Then, we further substitute $b_1 \equiv -(1 + b_2 + b_3 + b_4)$, that we obtain from first equality, to last two equations and then we have:

$$\begin{aligned} &b_2^2 + 2b_2 + 1 + b_3 + b_2b_4 - b_3b_4 \equiv 0 \bmod p \\ &b_3^2 + 2b_3b_4 + b_4^2 + b_4 - b_2 + b_2b_3 \equiv 0 \bmod p \end{aligned} \tag{3.39}$$

The system (3.39) has resultant of

$$\begin{aligned} b_3^4 + (2 - b_2)b_3^3 + (b_2^2 + b_2 + 4)b_3^2 + (-b_2^3 + b_2^2 + 3b_2 + 3)b_3 \\ + (b_2^4 + 2b_2^3 + 4b_2^2 + 3b_2 + 1) \end{aligned} \tag{3.40}$$

with respect to b_4. Define equation (3.40) as a quartic polynomial

$$\begin{aligned} f(x) = x^4 + (2 - b_2)x^3 + (b_2^2 + b_2 + 4)x^2 + (-b_2^3 + b_2^2 + 3b_2 + 3)x \\ + b_2^4 + 2b_2^3 + 4b_2^2 + 3b_2 + 1 \end{aligned}$$

Polynomial f has the following 4 roots

$$\begin{aligned} x_{1,2} &= \frac{2 - b_2 - \sqrt{5}b_2 \pm (3 + \sqrt{5} + 2b_2)\sqrt{(-5 + \sqrt{5})/2}}{-4} \\ x_{3,4} &= \frac{-2 + b_2 - \sqrt{5}b_2 \pm (-3 + \sqrt{5} - 2b_2)\sqrt{(-5 - \sqrt{5})/2}}{4} \end{aligned}$$

Hence, polynomial f splits modulo p if and only if 5 and $(-5 \pm \sqrt{5})/2$ are quadratic residues modulo p. To begin with, we note that $p \neq 5$ is an odd prime number. Then, 5 is quadratic

residue modulo p for values $p \equiv \pm 1 \bmod 5$. And, it can be easily checked that $\sqrt{(-5 \pm \sqrt{5})/2}$ lie in cyclotomic field of degree 5. For instance, $\sqrt{(-5 - \sqrt{5})/2} = \zeta_5^3 - \zeta_5^4$, where ζ_5 is fifth root of 1. Therefore, $(-5 \pm \sqrt{5})/2$ are quadratic residues modulo p if and only if $p \equiv 1 \bmod 5$ by the law of decomposition in cyclotomic field of degree 5 (see [12, Proposition 10.3]). However, such values of p are not covered by the assumption of the lemma. Hence, fifth case is also not possible. This completes the proof of initial step of induction.

Assume that it holds for for the case $m = i$ for some integer $i \geq 2$. Now, let us consider the case $m = i + 1$. Let the following hold

$$\begin{aligned} p^{i+1} &\mid s_0 + s_1 + s_2 + s_3 + s_4, \\ p^{2(i+1)-1} &\mid s_0 s_4 + s_1 s_0 + s_2 s_1 + s_3 s_2 + s_4 s_3, \\ p^{2(i+1)-1} &\mid s_0 s_3 + s_1 s_4 + s_2 s_0 + s_3 s_1 + s_4 s_2. \end{aligned} \tag{3.41}$$

Then, by induction step we have

$$p^i \mid s_j \text{ for all } j = 0, 1, 2, 3, 4.$$

Let $s_j = p^i k_j$ for some integer k_j and $j = 0, 1, 2, 3, 4$. Then, (3.41) reduces to

$$\begin{aligned} p &\mid k_0 + k_1 + k_2 + k_3 + k_4, \\ p &\mid k_0 k_4 + k_1 k_0 + k_2 k_1 + k_3 k_2 + k_4 k_3, \\ p &\mid k_0 k_3 + k_1 k_4 + k_2 k_0 + k_3 k_1 + k_4 k_2. \end{aligned} \tag{3.42}$$

By the first step of the induction, we have $p \mid k_j$ for all $j = 0, 1, 2, 3, 4$. Hence, we observe the required result $p^{i+1} \mid s_j$ for all $j = 0, 1, 2, 3, 4$. Therefore we complete the proof. ■

Lemma 3.4.6 *Let $p \neq 5$ be an odd prime number such that $p \not\equiv 1 \bmod 5$. Let n be an integer such that $n \equiv 2 \bmod 5$ and $n \equiv p^{2m-1} \bmod p^{2m}$ for some integer $m \geq 1$. Then the system of equations in variables s_0, s_1, s_2, s_3, s_4*

$$\begin{aligned} s_0 + s_1 + s_2 + s_3 + s_4 &= n \\ s_0 s_4 + s_1 s_0 + s_2 s_1 + s_3 s_2 + s_4 s_3 &= \frac{n(n-2)}{5} \\ s_0 s_3 + s_1 s_4 + s_2 s_0 + s_3 s_1 + s_4 s_2 &= \frac{n(n-2)}{5} \end{aligned} \tag{3.43}$$

has no solution over $\mathbb{Z}^+ \cup \{0\}$.

Proof. Assume that s_0, s_1, s_2, s_3, s_4 is a solution to (3.43). Let $n = p^{2m}k + p^{2m-1}$ for some nonnegative integer k. As n is divisible by p^{2m-1}, we also have

$$\frac{n(n-2)}{5} = \frac{(p^{2m}k + p^{2m-1})(p^{2m}k + p^{2m-1} - 2)}{5}$$

is divisible by p^{2m-1}, but not divisible by p^{2m}. However, Lemma 3.4.5 implies that $p^{2m} \mid s_0s_4 + s_1s_0 + s_2s_1 + s_3s_2 + s_4s_3$. This contradicts to the condition that $\frac{n(n-2)}{5}$ is not divisible by p^{2m}. Therefore we complete the proof. □

We list values of n for which 5-ary NPS of type II with period $n+1$ is not existing in Table A.8. Each n value presented in the table satisfies either Theorem 3.4.1 or Theorem 3.4.4, which is also indicated in the Existence column. We list values upto $n \leq 1000$ to show the coverage of Theorems 3.4.1 and 3.4.4 explicitly. Existence status in the remaining values of n are not known.

Remark 3.4.7 *Further extension of Lemma 3.4.3 and Lemma 3.4.6 for almost q-ary sequences $q \geq 7$ is not possible. For instance, consider the case $q = 7$ and $n = 9$. In this case $(s_0, s_1, s_2, s_3, s_4, s_5, s_6) = (3, 3, 0, 3, 0, 0, 0)$ is a solution to equations (3.8) and (3.9). Similarly, $(0, 0, 4, 0, 4, 4, 4)$ and $(1, 1, 2, 6, 6, 1, 6)$ are solutions for $n = 16$ and $n = 23$, respectively. And similar examples also exist for $q > 7$.*

CHAPTER 4

CONCLUSIONS

Although we partially answered the questions posed in ([6]), there are still several open cases. For instance, our method couldn't overcome the existence problem of almost p-ary perfect sequence of period $n+1$ for $n = 77$. Another point drawing attention in the existence results of ([6]) is that almost p-ary perfect sequences are rarely exists. Ma and Ng have also a similar remark in ([2]) for the existence of p-ary perfect and nearly perfect sequences and they concluded that it might be possible to have more existence results if we study m-ary sequences for composite m.

From application point of view, though perfect binary sequences have already been utilized on various fields for fifty years (see chapter 1 of [3]), p-ary perfect and nearly perfect sequences appear to be a relatively new subject for engineers. So that it might be a productive research to find out how to apply those sequences in practice. During this study, we have submitted two articles, one has already been published as [13], the other is still under review.

REFERENCES

[1] D. Jungnickel, A. Pott, *Perfect and almost perfect sequences*, Discrete Applied Mathematics 95(1-3), 331–359 (1999).

[2] S.L. Ma, W.S. Ng, *On nonexistence of perfect and nearly perfect sequences*, Int. J. Inf. Coding Theory 1 (1), 14–38 (2009).

[3] S. W. Golomb, *Shift Register Sequences*, Holden-Day, Inc.(1967)

[4] J. Wolfmann, *Almost perfect autocorrelation sequences*, IEEE Trans. Inform. Theory 38 1412–1418 (1992)

[5] A. Pott, S.P. Bradley *Existence and nonexistence of almost-perfect autocorrelation sequences*, IEEE Trans. Inform. Theory 41 301–304 (1995)

[6] Y. M. Chee, Y. Tan, Y. Zhou, *Almost p-Ary Perfect Sequences*, Carlet, C. Pott, A. (Eds.), SETA 2010 LNCS, pp. 399–415, (2010).

[7] D. R. Stinson, *Combinatorial Designs Constructions and Analysis*, Springer-Verlag New York (2004)

[8] J.E.H. Elliott, A.T. Butson, *Relative Difference Sets*, Illinois J.Math. 10, 517–531 (1966)

[9] A. Pott, *Finite Geometry and Character Theory* LNM, vol. 1601. Springer, Heidelberg (1995)

[10] T. Beth, D. Jungnickel, H. Lenz, *Design Theory* 2nd. edn., Cambridge University Press, New York (1999).

[11] M.J. Ganley, *Direct product difference sets*, Journal of Combinatorial Theory, Series A 23, (1977), no. 3, 321-332.

[12] J. Neukirch, *Algebraic number theory*, 322, Springer-Verlag, Berlin, 1999.

[13] F. Özbudak, O. Yayla, C.C. Yıldırım, *Nonexistence of certain almost p-ary perfect sequences*, Sequences and Their Applications-SETA 2012, Lecture Notes in Comput. Sci., 7280, Springer-Verlag, Berlin, 2012, pp. 13-24.

APPENDIX A

TABLES

Table A.1: Orbits of $G = \mathbb{Z}_{101} \times \mathbb{Z}_3$ under $x \to 16x$

{ (0, 0) } { (0, 1) } { (0, 2) }
{ (88, 0), (84, 0), (5, 0), (24, 0), (19, 0), (92, 0), (58, 0), (79, 0), (25, 0), (68, 0), (52, 0), (81, 0), (36, 0), (1, 0), (54, 0), (87, 0), (97, 0), (37, 0), (56, 0), (80, 0), (31, 0), (71, 0), (16, 0), (95, 0), (78, 0) } { (88, 1), (84, 1), (5, 1), (24, 1), (19, 1), (92, 1), (58, 1), (79, 1), (25, 1), (68, 1), (52, 1), (81, 1), (36, 1), (1, 1), (54, 1), (87, 1), (97, 1), (37, 1), (56, 1), (80, 1), (31, 1), (71, 1), (16, 1), (95, 1), (78, 1) } { (88, 2), (84, 2), (5, 2), (24, 2), (19, 2), (92, 2), (58, 2), (79, 2), (25, 2), (68, 2), (52, 2), (81, 2), (36, 2), (1, 2), (54, 2), (87, 2), (97, 2), (37, 2), (56, 2), (80, 2), (31, 2), (71, 2), (16, 2), (95, 2), (78, 2) }
{ (89, 0), (73, 0), (2, 0), (55, 0), (74, 0), (3, 0), (93, 0), (32, 0), (38, 0), (61, 0), (11, 0), (83, 0), (7, 0), (15, 0), (72, 0), (75, 0), (48, 0), (10, 0), (67, 0), (35, 0), (57, 0), (50, 0), (41, 0), (59, 0), (62, 0) } { (89, 1), (73, 1), (2, 1), (55, 1), (74, 1), (3, 1), (93, 1), (32, 1), (38, 1), (61, 1), (11, 1), (83, 1), (7, 1), (15, 1), (72, 1), (75, 1), (48, 1), (10, 1), (67, 1), (35, 1), (57, 1), (50, 1), (41, 1), (59, 1), (62, 1) } { (89, 2), (73, 2), (2, 2), (55, 2), (74, 2), (3, 2), (93, 2), (32, 2), (38, 2), (61, 2), (11, 2), (83, 2), (7, 2), (15, 2), (72, 2), (75, 2), (48, 2), (10, 2), (67, 2), (35, 2), (57, 2), (50, 2), (41, 2), (59, 2), (62, 2) }
{ (14, 0), (20, 0), (17, 0), (6, 0), (77, 0), (100, 0), (82, 0), (64, 0), (45, 0), (70, 0), (43, 0), (65, 0), (13, 0), (4, 0), (9, 0), (21, 0), (49, 0), (85, 0), (23, 0), (30, 0), (76, 0), (47, 0), (22, 0), (33, 0), (96, 0) } { (14, 1), (20, 1), (17, 1), (6, 1), (77, 1), (100, 1), (82, 1), (64, 1), (45, 1), (70, 1), (43, 1), (65, 1), (13, 1), (4, 1), (9, 1), (21, 1), (49, 1), (85, 1), (23, 1), (30, 1), (76, 1), (47, 1), (22, 1), (33, 1), (96, 1) } { (14, 2), (20, 2), (17, 2), (6, 2), (77, 2), (100, 2), (82, 2), (64, 2), (45, 2), (70, 2), (43, 2), (65, 2), (13, 2), (4, 2), (9, 2), (21, 2), (49, 2), (85, 2), (23, 2), (30, 2), (76, 2), (47, 2), (22, 2), (33, 2), (96, 2) }
{ (18, 0), (86, 0), (66, 0), (46, 0), (53, 0), (8, 0), (90, 0), (12, 0), (29, 0), (63, 0), (34, 0), (94, 0), (44, 0), (98, 0), (99, 0), (26, 0), (28, 0), (69, 0), (42, 0), (39, 0), (27, 0), (51, 0), (60, 0), (40, 0), (91, 0) } { (18, 1), (86, 1), (66, 1), (46, 1), (53, 1), (8, 1), (90, 1), (12, 1), (29, 1), (63, 1), (34, 1), (94, 1), (44, 1), (98, 1), (99, 1), (26, 1), (28, 1), (69, 1), (42, 1), (39, 1), (27, 1), (51, 1), (60, 1), (40, 1), (91, 1) } { (18, 2), (86, 2), (66, 2), (46, 2), (53, 2), (8, 2), (90, 2), (12, 2), (29, 2), (63, 2), (34, 2), (94, 2), (44, 2), (98, 2), (99, 2), (26, 2), (28, 2), (69, 2), (42, 2), (39, 2), (27, 2), (51, 2), (60, 2), (40, 2), (91, 2) }

Table A.2: Orbits of $G = \mathbb{Z}_{51} \times \mathbb{Z}_7$ under $x \to 4x$

{ (0, 0) } { (34, 0) } { (17, 0) }
{ (34, 5), (34, 6), (34, 3) } { (34, 1), (34, 4), (34, 2) } { (17, 2), (17, 4), (17, 1) }
{ (17, 6), (17, 3), (17, 5) } { (0, 6), (0, 5), (0, 3) } { (0, 1), (0, 2), (0, 4) }
{ (43, 0), (19, 0), (49, 0), (25, 0) } { (23, 0), (44, 0), (41, 0), (11, 0) }
{ (48, 0), (12, 0), (39, 0), (3, 0) } { (35, 0), (38, 0), (50, 0), (47, 0) }
{ (37, 0), (22, 0), (31, 0), (46, 0) } { (21, 0), (30, 0), (33, 0), (18, 0) }
{ (27, 0), (45, 0), (6, 0), (24, 0) } { (10, 0), (7, 0), (40, 0), (28, 0) }
{ (9, 0), (36, 0), (42, 0), (15, 0) } { (13, 0), (1, 0), (4, 0), (16, 0) }
{ (20, 0), (5, 0), (14, 0), (29, 0) } { (2, 0), (32, 0), (26, 0), (8, 0) }
{ (44, 5), (41, 3), (11, 3), (44, 3), (41, 5), (41, 6), (23, 3), (11, 6), (23, 5), (11, 5), (23, 6), (44, 6) }
{ (23, 2), (44, 1), (11, 4), (23, 1), (41, 2), (44, 4), (23, 4), (41, 1), (11, 1), (44, 2), (41, 4), (11, 2) }
{ (26, 4), (32, 2), (2, 2), (26, 2), (26, 1), (32, 4), (32, 1), (8, 2), (2, 1), (2, 4), (8, 4), (8, 1) }
{ (33, 2), (30, 2), (33, 1), (33, 4), (18, 1), (30, 1), (18, 4), (21, 1), (21, 4), (30, 4), (21, 2), (18, 2) }
{ (36, 1), (9, 2), (36, 2), (42, 2), (9, 4), (15, 4), (15, 2), (42, 4), (42, 1), (9, 1), (36, 4), (15, 1) }
{ (50, 6), (38, 3), (50, 5), (47, 3), (47, 6), (50, 3), (35, 5), (38, 6), (35, 3), (47, 5), (35, 6), (38, 5) }
{ (30, 3), (18, 5), (30, 6), (21, 3), (33, 6), (33, 5), (18, 3), (21, 6), (18, 6), (30, 5), (21, 5), (33, 3) }
{ (42, 3), (36, 6), (42, 5), (15, 6), (9, 5), (36, 3), (15, 3), (15, 5), (36, 5), (42, 6), (9, 3), (9, 6) }
{ (3, 3), (3, 5), (48, 5), (39, 3), (39, 6), (3, 6), (48, 6), (12, 5), (48, 3), (39, 5), (12, 6), (12, 3) }
{ (40, 4), (28, 4), (40, 1), (40, 2), (28, 1), (10, 2), (28, 2), (7, 2), (10, 4), (7, 1), (10, 1), (7, 4) }
{ (1, 6), (4, 5), (4, 3), (13, 3), (1, 5), (13, 6), (13, 5), (16, 6), (4, 6), (16, 3), (16, 5), (1, 3) }
{ (5, 5), (29, 6), (20, 5), (14, 3), (20, 3), (29, 5), (5, 3), (29, 3), (20, 6), (5, 6), (14, 6), (14, 5) }
{ (43, 4), (43, 2), (49, 4), (19, 2), (25, 4), (43, 1), (49, 2), (25, 2), (49, 1), (19, 1), (25, 1), (19, 4) }
{ (27, 6), (45, 5), (27, 3), (24, 3), (45, 3), (27, 5), (24, 5), (6, 3), (45, 6), (6, 6), (6, 5), (24, 6) }
{ (26, 3), (26, 5), (32, 3), (8, 5), (32, 6), (2, 5), (8, 3), (32, 5), (8, 6), (26, 6), (2, 3), (2, 6) }
{ (31, 3), (37, 6), (22, 6), (22, 3), (31, 6), (31, 5), (46, 3), (37, 5), (22, 5), (37, 3), (46, 5), (46, 6) }
{ (50, 4), (35, 4), (47, 4), (50, 2), (35, 2), (50, 1), (38, 2), (47, 2), (38, 4), (47, 1), (38, 1), (35, 1) }
{ (46, 2), (37, 4), (31, 2), (31, 1), (22, 1), (46, 4), (37, 2), (22, 4), (37, 1), (22, 2), (31, 4), (46, 1) }
{ (45, 1), (45, 2), (27, 2), (24, 4), (6, 2), (24, 2), (6, 1), (27, 4), (27, 1), (45, 4), (24, 1), (6, 4) }
{ (48, 2), (48, 4), (12, 4), (3, 1), (39, 1), (48, 1), (3, 2), (12, 1), (39, 4), (12, 2), (3, 4), (39, 2) }
{ (13, 2), (1, 2), (16, 4), (16, 2), (1, 1), (4, 4), (1, 4), (4, 1), (13, 4), (16, 1), (13, 1), (4, 2) }
{ (28, 5), (10, 6), (40, 6), (10, 3), (28, 6), (40, 3), (40, 5), (28, 3), (10, 5), (7, 5), (7, 6), (7, 3) }
{ (14, 4), (20, 4), (20, 2), (29, 1), (20, 1), (29, 2), (5, 2), (14, 2), (5, 1), (14, 1), (5, 4), (29, 4) }
{ (49, 3), (25, 5), (43, 6), (43, 5), (19, 3), (19, 5), (19, 6), (25, 3), (43, 3), (49, 5), (25, 6), (49, 6) }

Table A.3: Orbits of $G = \mathbb{Z}_{95} \times \mathbb{Z}_{31}$ under $x \to 4x$

{(0,0)}
{ (76, 0), (19, 0) } { (38, 0), (57, 0) }
{ (0, 23), (0, 27), (0, 30), (0, 15), (0, 29) } { (0, 2), (0, 1), (0, 16), (0, 4), (0, 8) } { (0, 22), (0, 11), (0, 13), (0, 26), (0, 21) } { (0, 28), (0, 19), (0, 14), (0, 7), (0, 25) } { (0, 18), (0, 5), (0, 10), (0, 20), (0, 9) } { (0, 6), (0, 24), (0, 12), (0, 17), (0, 3) }
{ (25, 0), (35, 0), (30, 0), (55, 0), (45, 0), (85, 0), (20, 0), (80, 0), (5, 0) } { (15, 0), (10, 0), (40, 0), (50, 0), (60, 0), (90, 0), (70, 0), (65, 0), (75, 0) }
{ (57, 2), (38, 2), (57, 1), (38, 8), (38, 4), (38, 16), (38, 1), (57, 4), (57, 8), (57, 16) } { (76, 2), (19, 8), (76, 16), (76, 1), (19, 2), (19, 16), (19, 1), (76, 4), (76, 8), (19, 4) } { (19, 11), (19, 21), (76, 21), (19, 22), (19, 26), (76, 22), (19, 13), (76, 11), (76, 26), (76, 13) } { (19, 27), (19, 29), (19, 30), (19, 15), (76, 23), (76, 30), (76, 15), (76, 27), (76, 29), (19, 23) } { (38, 20), (38, 9), (57, 5), (57, 20), (38, 5), (57, 9), (38, 18), (38, 10), (57, 18), (57, 10) } { (76, 7), (76, 28), (76, 19), (19, 7), (76, 25), (19, 25), (19, 14), (19, 19), (19, 28), (76, 14) } ...
{ (66, 0), (24, 0), (61, 0), (1, 0), (6, 0), (36, 0), (64, 0), (9, 0), (4, 0),(44, 0), (11, 0), (49, 0), (81, 0), (26, 0), (16, 0), (39, 0), (54,0), (74, 0) } { (62, 0), (93, 0), (82, 0), (43, 0), (92, 0), (63, 0), (58, 0), (68, 0), (83, 0), (7, 0), (77, 0), (17, 0), (23, 0), (28, 0), (42, 0), (47, 0),(87, 0), (73, 0) } { (18, 0), (53, 0), (8, 0), (12, 0), (32, 0), (67, 0), (33, 0), (72, 0), (37, 0), (48, 0), (22, 0), (78, 0), (2, 0), (88, 0), (3, 0), (52, 0), (27,0), (13, 0) } { (86, 0), (46, 0), (41, 0), (59, 0), (29, 0), (84, 0), (14, 0), (94, 0), (34, 0), (71, 0), (79, 0), (89, 0), (69, 0), (56, 0), (21, 0), (31, 0),(51, 0), (91, 0) }
{ (25, 17), (85, 12), (5, 6), (45, 17), (55, 17), (30, 24), (5, 17), (85, 17), (25, 6), (20, 3), (85, 6), (35, 24), (5, 24), (45, 24), (5, 3), (35,12), (25, 24), (30, 17), (30, 12), (5, 12), (80, 3), (45, 3),(55, 24), (80, 17), (55, 12), (80, 6), (80, 12), (55, 3), (80, 24), (20, 17), (85, 24), (85, 3), (25, 3), (35, 17), (20, 24), (25, 12), (30, 6), (55, 6), (45, 6), (30, 3), (35, 6), (35, 3), (20, 6), (20, 12), (45, 12) } ...
{ (48, 29), (22, 15), (88, 15), (72, 27), (37, 29), (32, 27), (53, 30), (18, 15), (72, 15), (22, 23),(8, 27), (13, 30), (33, 27), (18, 27), (8,15), (18, 30), (8, 23), (88, 27), (22, 29), (27, 27), (52, 23), (33, 23), (52, 15), (22, 30), (78, 29), (72, 23), (88, 23), (37, 30), (18, 29), (2,30), (48, 15), (78, 27), (12, 29), (12, 27), (2, 23), (27, 30), (33, 30), (13, 23), (37, 27), (32, 15), (67, 27), (3, 23), (3, 29), (37, 23), (53,23), (53, 15), (88, 30), (52, 27), (33, 29), (78, 23), (33, 15), (12, 15), (48, 30), (12, 23), (27, 15), (22, 27), (2, 15), (8, 29), (3, 30), (67,30), (27, 29), (48, 23), (13, 29), (52, 29), (67, 15), (48, 27), (88, 29), (53, 27), (67, 23), (13, 15),(32, 23), (3, 15), (52, 30), (78, 30), (32,30), (2, 27), (12, 30), (18, 23), (78, 15), (27, 23), (3, 27), (32, 29), (72, 30), (13, 27), (8, 30), (2, 29), (72, 29), (53, 29), (67, 29), (37, 15)} ...

Table A.4: Orbits of $G = \mathbb{Z}_{100} \times \mathbb{Z}_7$ under $x \to 81x$

{ (65, 0) } { (75, 0) } { (45, 0) } { (85, 0) } { (30, 0) } { (35, 0) } { (60, 0) }
{ (10, 0) } { (50, 0) } { (5, 0) } { (80, 0) } { (70, 0) } { (55, 0) } { (25, 0) }
{ (0, 0) } { (20, 0) } { (15, 0) } { (95, 0) } { (90, 0) } { (40, 0) }
{ (65, 3), (65, 6), (65, 5) } { (25, 4), (25, 1), (25, 2) } { (45, 1), (45, 4), (45, 2) }
{ (85, 4), (85, 1), (85, 2) } { (80, 2), (80, 1), (80, 4) } { (50, 6), (50, 5), (50, 3) }
{ (0, 2), (0, 1), (0, 4) } { (35, 4), (35, 2), (35, 1) } { (90, 5), (90, 6), (90, 3) }
{ (55, 5), (55, 6), (55, 3) } { (75, 5), (75, 6), (75, 3) } { (95, 6), (95, 5), (95, 3) }
{ (15, 6), (15, 5), (15, 3) } { (70, 5), (70, 3), (70, 6) }
{ (15, 2), (15, 1), (15, 4) } { (25, 6), (25, 5), (25, 3) }
{ (5, 6), (5, 5), (5, 3) } { (5, 1), (5, 2), (5, 4) } { (75, 4), (75, 2), (75, 1) }
{ (85, 3), (85, 6), (85, 5) } { (90, 1), (90, 2), (90, 4) } { (60, 2), (60, 4), (60, 1) }
{ (20, 3), (20, 5), (20, 6) } { (65, 1), (65, 4), (65, 2) } { (40, 3), (40, 6), (40, 5) }
{ (30, 1), (30, 4), (30, 2) } { (10, 1), (10, 4), (10, 2) } { (45, 5), (45, 6), (45, 3) }
{ (0, 6), (0, 5), (0, 3) } { (35, 3), (35, 5), (35, 6) } { (60, 6), (60, 3), (60, 5) }
{ (80, 3), (80, 6), (80, 5) } { (30, 3), (30, 5), (30, 6) } { (50, 2), (50, 4), (50, 1) }
{ (10, 6), (10, 3), (10, 5) } { (20, 4), (20, 2), (20, 1) } { (95, 4), (95, 2), (95, 1) }
{ (70, 1), (70, 4), (70, 2) } { (40, 4), (40, 1), (40, 2) } { (55, 1), (55, 2), (55, 4) }
{ (36, 0), (96, 0), (76, 0), (16, 0), (56, 0) } { (78, 0), (58, 0), (38, 0), (98, 0), (18, 0) }
{ (23, 0), (43, 0), (83, 0), (63, 0), (3, 0) } { (71, 0), (91, 0), (31, 0), (51, 0), (11, 0) }
{ (93, 0), (13, 0), (53, 0), (73, 0), (33, 0) } { (42, 0), (2, 0), (22, 0), (62, 0), (82, 0) }
{ (94, 0), (34, 0), (14, 0), (54, 0), (74, 0) } { (4, 0), (84, 0), (44, 0), (64, 0), (24, 0) }
{ (37, 0), (57, 0), (17, 0), (97, 0), (77, 0) } { (68, 0), (48, 0), (8, 0), (88, 0), (28, 0) }
{ (1, 0), (21, 0), (41, 0), (61, 0), (81, 0) } { (79, 0), (19, 0), (99, 0), (39, 0), (59, 0) }
{ (9, 0), (89, 0), (69, 0), (49, 0), (29, 0) } { (87, 0), (7, 0), (27, 0), (47, 0), (67, 0) }
{ (66, 0), (86, 0), (26, 0), (6, 0), (46, 0) } { (12, 0), (32, 0), (72, 0), (92, 0), (52, 0) }
{ (91, 6), (31, 6), (91, 5), (11, 6), (31, 3), (51, 3), (51, 5), (11, 3), (51, 6), (11, 5), (31, 5), (71, 3), (91, 3), (71, 5), (71, 6) }
{ (14, 3), (94, 6), (14, 5), (74, 3), (54, 3), (94, 3), (34, 6), (54, 6), (34, 3), (74, 6), (14, 6), (54, 5), (94, 5), (74, 5), (34, 5) }
{ (23, 5), (43, 6), (43, 5), (23, 6), (3, 3), (63, 3), (23, 3), (63, 5), (3, 5), (3, 6), (83, 3), (63, 6), (83, 5), (43, 3), (83, 6) }
{ (9, 2), (49, 4), (89, 4), (69, 2), (9, 4), (69, 1), (29, 1), (29, 2), (89, 1), (49, 2), (69, 4), (89, 2), (49, 1), (9, 1), (29, 4) }
{ (44, 3), (4, 5), (4, 3), (64, 6), (44, 5), (84, 6), (64, 3), (24, 5), (64, 5), (24, 3), (84, 5), (24, 6), (4, 6), (84, 3), (44, 6) }
...

Table A.5: Orbits of $G = \mathbb{Z}_{77} \times \mathbb{Z}_3$ under $x \to 4x$

{ (0, 0) }, { (0, 1) }, { (0, 2) },
{ (22, 0), (44, 0), (11, 0) }, { (22, 1), (44, 1), (11, 1) }, { (22, 2), (44, 2), (11, 2) },
{ (66, 0), (55, 0), (33, 0) }, { (66, 1), (55, 1), (33, 1) }, { (66, 2), (55, 2), (33, 2) },
{ (7, 0), (63, 0), (21, 0), (28, 0), (35, 0) }, { (7, 1), (63, 1), (21, 1), (28, 1), (35, 1) }, { (7, 2), (63, 2), (21, 2), (28, 2), (35, 2) },
{ (14, 0), (49, 0), (70, 0), (56, 0), (42, 0) }, { (14, 1), (49, 1), (70, 1), (56, 1), (42, 1) }, { (14, 2), (49, 2), (70, 2), (56, 2), (42, 2) },
{ (17, 0), (68, 0), (24, 0), (62, 0), (54, 0), (61, 0), (19, 0), (13, 0), (41, 0), (6, 0), (52, 0), (76, 0), (40, 0), (10, 0), (73, 0) }, { (17, 1), (68, 1), (24, 1), (62, 1), (54, 1), (61, 1), (19, 1), (13, 1), (41, 1), (6, 1), (52, 1), (76, 1), (40, 1), (10, 1), (73, 1) }, { (17, 2), (68, 2), (24, 2), (62, 2), (54, 2), (61, 2), (19, 2), (13, 2), (41, 2), (6, 2), (52, 2), (76, 2), (40, 2), (10, 2), (73, 2) },
{ (64, 0), (9, 0), (15, 0), (4, 0), (23, 0), (16, 0), (58, 0), (25, 0), (60, 0), (37, 0), (1, 0), (71, 0), (53, 0), (36, 0), (67, 0) }, { (64, 1), (9, 1), (15, 1), (4, 1), (23, 1), (16, 1), (58, 1), (25, 1), (60, 1), (37, 1), (1, 1), (71, 1), (53, 1), (36, 1), (67, 1) }, { (64, 2), (9, 2), (15, 2), (4, 2), (23, 2), (16, 2), (58, 2), (25, 2), (60, 2), (37, 2), (1, 2), (71, 2), (53, 2), (36, 2), (67, 2) },
{ (48, 0), (45, 0), (31, 0), (27, 0), (69, 0), (26, 0), (20, 0), (38, 0), (5, 0), (47, 0), (75, 0), (3, 0), (34, 0), (12, 0), (59, 0) }, { (48, 1), (45, 1), (31, 1), (27, 1), (69, 1), (26, 1), (20, 1), (38, 1), (5, 1), (47, 1), (75, 1), (3, 1), (34, 1), (12, 1), (59, 1) }, { (48, 2), (45, 2), (31, 2), (27, 2), (69, 2), (26, 2), (20, 2), (38, 2), (5, 2), (47, 2), (75, 2), (3, 2), (34, 2), (12, 2), (59, 2) },
{ (18, 0), (43, 0), (46, 0), (8, 0), (65, 0), (29, 0), (32, 0), (72, 0), (2, 0), (50, 0), (39, 0), (74, 0), (30, 0), (51, 0), (57, 0) }, { (18, 1), (43, 1), (46, 1), (8, 1), (65, 1), (29, 1), (32, 1), (72, 1), (2, 1), (50, 1), (39, 1), (74, 1), (30, 1), (51, 1), (57, 1) }, { (18, 2), (43, 2), (46, 2), (8, 2), (65, 2), (29, 2), (32, 2), (72, 2), (2, 2), (50, 2), (39, 2), (74, 2), (30, 2), (51, 2), (57, 2) },

Table A.6: Orbits of $G = \mathbb{Z}_{101} \times \mathbb{Z}_{11}$ under $x \to 5x$

{ (0, 0)}
{ (0, 2), (0, 6), (0, 10), (0, 7), (0, 8) } { (0, 1), (0, 5), (0, 4), (0, 9), (0, 3) }
{ (40, 4), (8, 3), (66, 3), (39, 1), (86, 3), (28, 9), (51, 5), (12, 9), (53, 3), (27, 4), (94, 5), (90, 3), (29, 9), (42, 5), (18, 5), (63, 4),(91, 1), (98, 5), (60, 1), (46, 4), (44, 1), (69, 1), (26, 4), (34, 9), (99, 9) } { (16, 1), (68, 3), (24, 3), (1, 9), (80, 5), (95, 9), (56, 3), (58, 3), (87, 9), (71, 1), (81, 4), (5, 1), (19, 4), (92, 5), (84, 9), (36, 9), (79,1), (97, 3), (78, 4), (54, 5), (37, 4), (52, 5), (88, 4), (31, 1), (25, 5) } { (12, 6), (26, 10), (63, 10), (66, 2), (60, 8), (40, 10), (69, 8), (46, 10), (34, 6), (51, 7), (28, 6), (53, 2), (39, 8), (91, 8), (8, 2), (27,10), (99, 6), (44, 8), (90, 2), (94, 7), (29, 6), (98, 7), (86, 2), (42, 7), (18, 7) } { (36, 5), (16, 3), (31, 3), (19, 1), (92, 4), (52, 4), (79, 3), (25, 4), (88, 1), (54, 4), (58, 9), (68, 9), (95, 5), (56, 9), (81, 1), (71, 3),(78, 1), (97, 9), (84, 5), (37, 1), (1, 5), (5, 3), (24, 9), (80, 4), (87, 5) } { (54, 1), (24, 5), (25, 1), (80, 1), (56, 5), (52, 1), (16, 9), (97, 5), (19, 3), (79, 9), (71, 9), (31, 9), (78, 3), (84, 4), (81, 3), (5, 9),(92, 1), (36, 4), (88, 3), (95, 4), (1, 4), (37, 3), (58, 5), (68, 5), (87, 4) } { (100, 6), (6, 6), (85, 8), (64, 10), (82, 10), (21, 7), (76, 7), (9, 7), (23, 10), (47, 7), (65, 6), (33, 2), (43, 2), (45, 2), (30, 8), (17, 6),(96, 8), (70, 8), (49, 7), (14, 6), (13, 10), (20, 10), (22, 8), (4, 2), (77, 2) } { (28, 10), (99, 10), (18, 8), (8, 7), (34, 10), (51, 8), (86, 7), (63, 2), (12, 10), (90, 7), (42, 8), (39, 6), (40, 2), (91, 6), (66, 7), (44, 6),(27, 2), (98, 8), (26, 2), (46, 2), (69, 6), (29, 10), (94, 8), (60, 6), (53, 7) } { (88, 0), (84, 0), (5, 0), (24, 0), (19, 0), (92, 0), (58, 0), (79, 0), (25, 0), (68, 0), (52, 0), (81, 0), (36, 0), (1, 0), (54, 0), (87, 0), (97,0), (37, 0), (56, 0), (31, 0), (80, 0), (71, 0), (16, 0), (95, 0), (78, 0) } { (31, 10), (37, 7), (79, 10), (58, 8), (5, 10), (92, 6), (87, 2), (54, 6), (97, 8), (78, 7), (36, 2), (95, 2), (56, 8), (81, 7), (80, 6), (16, 10),(68, 8), (19, 7), (52, 6), (88, 7), (25, 6), (84, 2), (24, 8), (1, 2), (71, 10) } { (1, 1), (79, 5), (52, 3), (58, 4), (68, 4), (37, 9), (95, 1), (71, 5), (24, 4), (97, 4), (16, 5), (88, 9), (36, 1), (5, 5), (56, 4), (78, 9), (19,9), (54, 3), (31, 5), (84, 1), (25, 3), (92, 3), (87, 1), (80, 3), (81, 9) } { (60, 3), (8, 9), (26, 1), (66, 9), (98, 4), (12, 5), (18, 4), (63, 1), (53, 9), (51, 4), (91, 3), (34, 5), (40, 1), (46, 1), (69, 3), (94, 4),(86, 9), (42, 4), (29, 5), (44, 3), (28, 5), (90, 9), (99, 5), (39, 3), (27, 1) } { (28, 3), (12, 3), (51, 9), (98, 9), (44, 4), (39, 4), (29, 3), (8, 1), (60, 4), (42, 9), (26, 5), (63, 5), (66, 1), (90, 1), (18, 9), (91, 4),(34, 3), (46, 5), (69, 4), (99, 3), (53, 1), (40, 5), (86, 1), (94, 9), (27, 5) } { (13, 6), (76, 2), (23, 6), (4, 10), (82, 6), (85, 7), (9, 2), (77, 10), (65, 8), (100, 8), (45, 10), (70, 7), (14, 8), (22, 7), (33, 10), (96, 7),(20, 6), (47, 2), (6, 8), (43, 10), (49, 2), (21, 2), (64, 6), (17, 8), (30, 7) } { (45, 4), (9, 3), (77, 4), (4, 4), (64, 9), (23, 9), (96, 5), (22, 5), (65, 1), (20, 9), (43, 4), (100, 1), (17, 1), (33, 4), (85, 5), (47, 3),(13, 9), (14, 1), (76, 3), (82, 9), (6, 1), (21, 3), (49, 3), (70, 5), (30, 5) } { (89, 2), (83, 6), (74, 7), (73, 2), (32, 10), (11, 8), (3, 6), (75, 7), (61, 7), (2, 2), (57, 10), (15, 8), (67, 2), (10, 10), (35, 8), (50, 6),(59, 6), (62, 10), (72, 2), (38, 7), (93, 8), (41, 10), (48, 8), (7, 6), (55, 7) } { (28, 2), (40, 7), (90, 8), (94, 6), (46, 7), (69, 10), (99, 2), (42, 6), (63, 7), (27, 7), (66, 8), (91, 10), (86, 8), (98, 6), (26, 7), (60, 10),(39, 10), (53, 8), (51, 6), (34, 2), (29, 2), (44, 10), (12, 2), (8, 8), (18, 6) } ...

Table A.7: Nonexistence of almost 3-ary NPS of type II with period n ($n \leq 1000$)

n	Existence
20, 35, 44, 65, 68, 77, 92, 95, 116, 119, 140, 143, 161, 164, 176, 185, 188, 203, 209, 212, 215, 221, 236, 245, 260, 272,275, 284, 287, 299, 308, 320, 323, 329, 332, 335, 341, 356, 365, 368, 371, 377, 395, 404, 407, 413, 425, 428, 437, 452, 464, 473, 476, 485, 497, 500, 515, 524, 527, 533, 539, 545, 548, 551, 560, 572, 575, 581, 596, 611, 620, 623, 629, 635, 644, 656, 665, 668, 671, 689, 692, 695, 704, 707, 713, 716, 725, 731, 740, 749, 752, 764, 767, 779, 785, 788, 791, 803, 812, 815, 833, 836, 845, 848, 851, 860, 869, 875, 893, 899, 908, 917, 923, 932, 935, 944, 956, 959, 965, 989, 995	not exist by Theorem 3.3.1
5, 11, 17, 23, 29, 41, 47, 53, 59, 71, 80, 83, 89, 101, 107, 113, 125, 131, 137, 149, 155, 167, 173, 179, 191, 197, 227, 233, 239, 251, 257, 263, 269, 281, 293, 305, 311, 317, 347, 353, 359, 380, 383, 389, 401, 419, 431, 443, 449, 455, 461, 467, 479, 491, 503, 509, 521, 557, 563, 569, 587, 593, 599, 605, 617, 641, 647, 653, 659, 677, 683, 701, 719, 737, 743, 755, 761, 773, 797, 809, 821, 827, 839, 857, 863, 881, 884, 887, 905, 911, 929, 941, 947, 953, 971, 977, 980, 983	not exist by Theorem 3.3.1 and Theorem 3.3.4
230, 374, 530, 680, 830	not exist by Theorem 3.3.4

Table A.8: Nonexistence of almost 5-ary NPS of type II with period n ($n \leq 1000$)

n	Existence
7, 12, 27, 37, 52, 57, 67, 77, 87, 92, 97, 112, 117, 127, 132, 147, 157, 172, 177, 187, 192, 207, 212, 217, 237, 247, 252, 267, 272, 277, 287, 292, 297, 307, 327, 332, 337, 357, 367, 372, 377, 387, 397, 407, 412, 417, 427, 432, 437, 447, 452, 457, 477, 487, 492, 507, 517, 527, 532, 537, 547, 567, 572, 577, 592, 597, 607, 612, 627, 637, 652, 657, 667, 687, 692, 697, 707, 717, 727, 732, 737, 747, 752, 757, 767, 772, 777, 787, 807, 812, 817, 832, 837, 847, 852, 867, 877, 892, 897, 907, 912, 917, 927, 932, 937, 957, 967, 972, 987, 997	not exist by Theorem 3.4.1
17, 47, 107, 137, 167, 197, 227, 257, 317, 347, 467, 497, 557, 587, 617, 647, 677, 797, 827, 857, 887, 947, 977	not exist by Theorem 3.4.1 and Theorem 3.4.4
23, 29, 53, 56, 59, 83, 89, 113, 149, 173, 179, 182, 203, 233, 239, 263, 269, 293, 350, 353, 359, 380, 383, 389, 419, 443, 449, 479, 503, 509, 563, 569, 593, 599, 644, 653, 659, 683, 689, 719, 743, 773, 791, 809, 839, 863, 884, 929, 938, 53, 983	not exist by Theorem 3.4.4

VITA

PERSONAL INFORMATION

Surname, Name: Yıldırım, Cemal Cengiz
Nationality: Turkish (T.C.)
Date and Place of Birth: 03 December 1974, Erzincan
email:ccengizyildirim@yahoo.com

EDUCATION

Degree	Institution	Year of Graduation
PhD	METU, Institute of Applied Mathematics	2012
MS	Bilkent University, Electrical and Electronics Engineering	2002
BS	Turkish Naval Academy, Electrical and Electronics Engineering	1996

WORK EXPERIENCE

Year	Place	Enrollment
1996-Present	Turkish Armed Forces	Mostly in the area of Communication and Information Systems as System Engineer