Design of sequences with good correlation properties

Dan Zhang

Thesis for the degree of Philosophiae Doctor (PhD)
University of Bergen, Norway
2021

UNIVERSITY OF BERGEN

Design of sequences with good correlation properties

Dan Zhang

Thesis for the degree of Philosophiae Doctor (PhD)
at the University of Bergen

Date of defense: 26.08.2021

Year: 2021

Title: Design of sequences with good correlation properties

Name: Dan Zhang

Print: Skipnes Kommunikasjon / University of Bergen

Acknowledgements

I would like to gratefully acknowledge my supervisors Prof. Dr. Matthew Geoffrey Parker, Prof. Dr. Lilya Budaghyan, Prof. Dr. Tor Helleseth and Dr. Chunlei Li for their patient guidance during these years. Thank you all for your encouragement, support and important advice regarding my work. I am grateful to Prof. Dr. Zhengchun Zhou for his fruitful discussions. I would also like to thank Prof. Dr. Guang Gong for giving me the opportunity to conduct a research visit to the University of Waterloo.

I would like to thank members of the evaluation committee: Prof. Dr. Hong-Yeop Song, Prof. Dr. Sihem Mesnager, Dr. George Petrides, who agreed to review my thesis. Thank you all for your time and valuable comments.

I acknowledge the Department of Informatics for providing us such a nice and friendly working environment. I enjoyed the department's Christmas dinner every year. I would like to thank administrative staff for their support and practical advice in different stages of my PhD research. I am grateful to my mentor Prof. Uwe Egbert Wolter for his support and help. I would also like to thank Stefanie Meyer for organising the department's annual ICT Research School and writing workshops, which were very helpful for my study. Special thanks to IT staff Stanislav Oltu for his technical help.

I would like to thank the Research School of Computer and Information Security (COINS) staff and in particular Tor Helleseth, Øyvind Ytrehus and Hanno Langweg for organising all the summer and winter schools during these years. It was a great opportunity to broaden my research network and meet new friends. I acknowledge the financial supports from the University of Bergen and the COINS research school, which allowed me to travel to conferences and workshops.

I want to thank everyone in Selmer center for making it such a wonderful working place. I enjoyed myself very much being here. I have leaned a lot from such an excellent group. I am grateful to Prof. Igor A. Semaev for his great lectures in Cryptology. I am grateful to my colleagues and friends for their care, support and time spent together: Irene Villa, Isaac A. Canales Martínez, Andrea Tenti, Alessandro Budroni, Diana Davidova, Nikolay Stoyanov Kaleyski, Wrya Kadir, George Petrides, Sachin Valera, Navid Ghaedi Bardeh, Amund Askeland and Stein Dahl.

I would like to thank my friends and family for being the greatest support in my life. In particular, I am grateful to my little niece, whose lovely face shines my life every day. Last but not least, I want to express my love and gratitude to Jan William Johnsen for his love and support, whose encouragements always make me feel better about myself.

Abstract

This thesis is dedicated to exploring sequences with good correlation properties. Periodic sequences with desirable correlation properties have numerous applications in communications. Ideally, one would like to have a set of sequences whose out-of-phase auto-correlation magnitudes and cross-correlation magnitudes are very small, preferably zero. However, theoretical bounds show that the maximum magnitudes of auto-correlation and cross-correlation of a sequence set are mutually constrained, i.e., if a set of sequences possesses good auto-correlation properties, then the cross-correlation properties are not good and vice versa. The design of sequence sets that achieve those theoretical bounds is therefore of great interest. In addition, instead of pursuing the least possible correlation values within an entire period, it is also interesting to investigate families of sequences with ideal correlation in a smaller zone around the origin. Such sequences are referred to as sequences with zero correlation zone or ZCZ sequences, which have been extensively studied due to their applications in 4G LTE and 5G NR systems, as well as quasi-synchronous code-division multiple-access communication systems.

Paper I and a part of Paper II aim to construct sequence sets with low correlation within a whole period. Paper I presents a construction of sequence sets that meets the Sarwate bound. The construction builds a connection between generalised Frank sequences and combinatorial objects, circular Florentine arrays. The size of the sequence sets is determined by the existence of circular Florentine arrays of some order. Paper II further connects circular Florentine arrays to a unified construction of perfect polyphase sequences, which include generalised Frank sequences as a special case. The size of a sequence set that meets the Sarwate bound, depends on a divisor of the period of the employed sequences, as well as the existence of circular Florentine arrays.

Paper III-VI and a part of Paper II are devoted to ZCZ sequences. Papers II and III propose infinite families of optimal ZCZ sequence sets with respect to some bound, which are used to eliminate interference within a single cell in a cellular network. Papers V, VI and a part of Paper II focus on constructions of multiple optimal ZCZ sequence sets with favorable inter-set cross-correlation, which can be used in multi-user communication environments to minimize inter-cell interference. In particular, Paper II employs circular Florentine arrays and improves the number of the optimal ZCZ sequence sets with optimal inter-set cross-correlation property in some cases.

Outline

This thesis consists of an introductory part and six scientific papers. Chapter 1 gives an introduction to the background, objectives and related works, as well as a brief summary of the papers. Discussions and future work are presented in Chapter 2. The papers included in this thesis (Chapter 3) are:

I Dan Zhang and Tor Helleseth, *New optimal sets of perfect polyphase sequences based on circular Florentine arrays*, IEEE International Symposium on Information Theory (ISIT), Los Angeles, CA, USA, pp. 2921-2925 (2020).

II Dan Zhang and Tor Helleseth, *Sequences with good correlations based on circular Florentine arrays*, IEEE Transactions on Information Theory (submitted, Nov 2020).

III Dan Zhang, *Zero correlation zone sequences from a unified construction of perfect polyphase sequences*, IEEE International Symposium on Information Theory (ISIT), Paris, France, pp. 2269-2273 (2019).

IV Dan Zhang, Chunlei Li and Matthew Geoffrey Parker, *New optimal zero-correlation zone sequences based on IF-ZAZ sequences and interleaving technique*, partly presented at the conference SETA (2020) (to be submitted).

V Zhengchun Zhou, Dan Zhang, Tor Helleseth, and Jinming Wen, *A construction of multiple optimal ZCZ sequences with good cross correlation*, IEEE Transactions on Information Theory, vol. 64, no. 2, pp. 1340-1346 (2018).

VI Dan Zhang, Matthew Geoffrey Parker, and Tor Helleseth, *Polyphase zero correlation zone sequences from generalised bent functions*, Cryptography and Communications, **12**, pp. 325-335 (2020).

Contents

Chapter 1

Introduction

Sequences and their properties have been widely studied in different research areas because their valuable characteristics are used in many applications. Correlation functions are a measure of similarity among sequences. Specifically, the auto-correlation (AC) function assesses the similarity of a sequence with its cyclic shifts, and the cross-correlation (CC) function represents the similarity between two different sequences. Sequences with desirable correlation properties have been used in communication systems and radar systems for identification, synchronization, ranging, and interference mitigation [27].

Multiple Access Interference (MAI) and Multipath Interference (MPI) are two common interferences that corrupt signal transmission in wireless communication environments. MAI is caused by a device, access point or base-station when several users simultaneously try to communicate with it, while MPI occurs when the transmitted signal undergoes different propagation paths to reach a specific receiver. In the following, we briefly explain how correlation functions of sequences are used to mitigate the MAI and MPI in Code-Division Multiple Access (CDMA) systems [78].

Each user in a CDMA system is assigned with a spreading sequence to modulate their signal. The best performance occurs when there is good separation between the signal of a desired user and the signals of other users. The separation of the signals is made by correlating the transmitted signal with the spreading sequence of the desired user. If the signal matches a user's spreading sequence, i.e., they are the same sequence, the correlator at the receiver gives the AC values which allow the system to extract the signal. To mitigate MPI, the AC value at any non-zero time offset should be as close to zero as possible. If a user's spreading sequence has nothing in common with the signal, the (cross) correlation should be as close to zero as possible and then the signal will not be extracted. So low CC is used to separate the appropriate signal from signals meant for other receivers, thereby mitigating MAI. Sequences with low AC sidelobes and CC values are usually sought in the design of sequence families.

CDMA technique uses spreading sequences with desired correlation properties to spread data signals and to be assigned to individual users. Correlation property is a main feature for the selection of spreading sequences. According to new requirements in some specific environments, new metrics such as Metric Factor, Peak-to-Sidelobe

Level (PSL) and Peak to Average Power Ratio (PAPR) are recently considered as new criteria for sequence selection. For example, developing power-efficient and low energy consumption technologies becomes a new trend in communication systems, and this can be improved by a proper selection of properties of sequences to be used [9]. Some desirable characteristics of sequence sets, as described in [45], are 1) long length of the sequences; 2) large number of available sequences in the set; 3) good correlation (AC and CC) properties; 4) low complexity in construction and storing; 5) and good performance in metrics such as PSL, PAPR and Metric Factor. In this thesis, we mainly consider the first three characteristics of sequences.

The ultimate goal in sequence design with respect to the correlation property is to have a sequence set whose AC values at all non-zero shifts and CC values at all shifts are zero. Unfortunately, such an ideal sequence set does not exist according to some theoretical bounds such as Welch, Sidelnikov, and Sarwate bounds [79, 83, 104]. In practice, the values of AC and CC functions can be balanced according to desired properties. There are different ways to achieve a good trade-off between them. For example, it is possible to define the following two families of sequences:

- a family of sequences exhibiting ideal AC values at all non-zero shifts and low CC values at all shifts, i.e., the CC values are permitted to be different from zero;

- a family of sequences having ideal AC values and CC values at some zone of shifts around the origin, i.e., the AC and CC values are allowed to be non-zero outside the zone.

The second family is referred to as a sequence set with zero correlation zone (ZCZ). Constructing these two desirable families of sequences is the main goal of this thesis.

The rest of Introduction is organised as follows. Section 1.1 presents some basic notations and definitions, as well as the mathematical formulations of the two research questions mentioned above. Section 1.2 focuses on the first research question. Some known and related works are given, after which we briefly introduce the main results of Papers I and II. Section 1.3 addresses the second research question. Some related work and main contributions of this thesis are presented.

1.1 Sequences

We confine our discussion to periodic sequences in this thesis. Basic definitions of sequences and some related theoretical bounds are introduced in Section 1.1.1. Section 1.1.2 briefly presents some known work on the design of sequences with good correlation. Section 1.1.3 introduces the research objectives in this thesis.

1.1.1 Sequences and correlation bounds

Periodic sequences

In digital communications, sequences are often categorized by constellations over which they are defined, e.g., PSK (phase shift keying), ASK (amplitude shift keying), APSK (amplitude and phase shift keying), QAM (quadrature amplitude modulation), etc. When the PSK modulation is employed in digital communications, sequences are frequently defined over complex numbers with magnitude 1. Polyphase (q-ary) sequences are a special subset of PSK sequences, which are the main focus in this thesis.

A sequence $\mathbf{s} = (s(0), s(1), \cdots)$ is called a complex q-ary or polyphase sequence if all the coordinates are q-th roots of unity, i.e., $s(t) = \omega_q^{f(t)}$ for $t \geq 0$, where ω_q is a primitive q-th root of unity in $\mathbb{C}$ and $f(t) \in \{0, 1, \cdots, q-1\}$. A sequence $\mathbf{s}$ is called a *binary* sequence when $q = 2$, i.e., $s(t) \in \{-1, 1\}$ for all $t \geq 0$, and it is called a *quaternary* sequence when $q = 4$.

A sequence $\mathbf{s}$ is said to be *periodic* if $s(t) = s(t+N)$ for all $t \geq 0$, where N is a positive integer. The integer N is called the *period* of $\mathbf{s}$ if N is the smallest integer such that $s(t) = s(t+N)$ for all $t \geq 0$. For convenience, a sequence $\mathbf{s}$ of period N is denoted by $\mathbf{s} = (s(0), s(1), \cdots, s(N-1))$ or $\mathbf{s} = \{s(t)\}_{t=0}^{N-1}$.

Two sequences $\mathbf{s}_1$ and $\mathbf{s}_2$ are said to be cyclically equivalent if there exists an integer τ such that

$$s_1(t) = s_2(t+\tau)$$

for all t, otherwise they are said to be cyclically distinct.

Correlation Functions

Let $\mathcal{S} = \{\mathbf{s}_0, \mathbf{s}_1, \cdots, \mathbf{s}_{M-1}\}$ denote an (N, M) sequence set, where N is the period of each sequence and M is the size of the sequence set $\mathcal{S}$. For $0 \leq i, j \leq M-1$, the (periodic) *cross-correlation* function of $\mathbf{s}_i$ and $\mathbf{s}_j$ at shift τ is defined as

$$R_{\mathbf{s}_i,\mathbf{s}_j}(\tau) = \sum_{t=0}^{N-1} s_i(t+\tau)[s_j(t)]^*,$$

where $t+\tau$ is reduced modulo N and $[s_j(t)]^*$ is the complex conjugate of the complex number $s_j(t)$. When $\mathbf{s}_i = \mathbf{s}_j$, $R_{\mathbf{s}_i,\mathbf{s}_i}(\tau)$ is called the *auto-correlation* function of $\mathbf{s}_i$. In this case, we write $R_{\mathbf{s}_i}(\tau) = R_{\mathbf{s}_i,\mathbf{s}_i}(\tau)$ for short. Note that $R_{\mathbf{s}_i}(\tau)$ is always equal to N when $\tau \equiv 0 \bmod N$. We call $R_{\mathbf{s}_i}(\tau)$, $\tau \not\equiv 0 \bmod N$, out-of-phase AC values. Correlation functions have the following properties [79, 82]:

- $R_{\mathbf{s}_i,\mathbf{s}_j}(\tau) = R_{\mathbf{s}_i,\mathbf{s}_j}(\tau+N)$;
- $R_{\mathbf{s}_i,\mathbf{s}_j}(-\tau) = [R_{\mathbf{s}_j,\mathbf{s}_i}(\tau)]^*$;
- $R_{\mathbf{s}_i}(-\tau) = [R_{\mathbf{s}_i}(\tau)]^*$;

- $\sum_{\tau=0}^{N-1} R_{\mathbf{s}_i,\mathbf{s}_j}(\tau) = \sum_{\tau=0}^{N-1} \mathbf{s}_i(\tau) \sum_{\tau=0}^{N-1} [\mathbf{s}_j(\tau)]^*$;
- $\sum_{\tau=0}^{N-1} |R_{\mathbf{s}_i,\mathbf{s}_j}(\tau)|^2 = \sum_{\tau=0}^{N-1} R_{\mathbf{s}_i}(\tau)[R_{\mathbf{s}_j}(\tau)]^*$,

where $|x|$ is the magnitude of a complex number x.

A sequence $\mathbf{s}$ is said to be *perfect* or have *ideal AC* if all the out-of-phase AC values are equal to zero, i.e.,

$$R_{\mathbf{s}}(\tau) = \begin{cases} 0 & for\ \forall \tau \neq 0 \in \mathbb{Z}_N; \\ N & for\ \tau = 0 \in \mathbb{Z}_N, \end{cases}$$

where $\mathbb{Z}_N$ denotes the ring of integers modulo N. However, perfect sequences are rare in general (more details about perfect sequences are introduced in Section 1.2.1).

A set $\mathcal{S}$ is called *periodically uncorrelated* if the CC value between any two distinct sequences in $\mathcal{S}$ at any shift is zero, i.e.,

$$R_{\mathbf{s}_i,\mathbf{s}_j}(\tau) = 0, \forall \tau \in \mathbb{Z}_N, \forall \mathbf{s}_i, \mathbf{s}_j \in \mathcal{S} \text{ with } i \neq j.$$

A set $\mathcal{S}$ is called *periodically complementary* if the sum of all ACs of sequences in $\mathcal{S}$ at the same nonzero shift is zero, namely,

$$\sum_{\mathbf{s}\in\mathcal{S}} R_{\mathbf{s}}(\tau) = 0, \forall \tau \in \mathbb{Z}_N \text{ with } \tau \neq 0.$$

The term *good AC* refers to maximum value at the origin and low magnitudes of AC values for all out-of-phase time shifts, while the term *good CC* refers to low magnitudes of CC values at all time shifts.

Correlation Bounds

Given a set of M sequences of period N, the maximum out-of-phase periodic AC magnitude, denoted by θ_a, and maximum periodic CC magnitude, denoted by θ_c, are defined by

$$\theta_a = \max\{|R_{\mathbf{s}_i}(\tau)| : \mathbf{s}_i \in \mathcal{S}, 0 < \tau < N\},$$

and

$$\theta_c = \max\{|R_{\mathbf{s}_i,\mathbf{s}_j}(\tau)| : \mathbf{s}_i \neq \mathbf{s}_j \in \mathcal{S}, 0 \leq \tau < N\},$$

respectively. The maximum periodic correlation magnitude is defined by $\theta_{max} = \max(\theta_a, \theta_c)$. Three important bounds on periodic correlation functions are as follows.

- *Welch's bound* [104]: It is based on the squares of the magnitudes of the inner product between all pair of sequences. A lower bound on $\theta_{\max}$ depending on the number of the sequences M and the period of the sequences N is given by

$$\theta_{\max} \geq N\sqrt{\frac{M-1}{MN-1}}.$$

- *Sidelnikov's bound* [83]: For any (N, M) sequence set with $M \geq N$,

$$\theta_{\max} \gtrsim \begin{cases} \sqrt{2N} & \text{for the binary case;} \\ \sqrt{N} & \text{for other cases.} \end{cases}$$

- *Sarwate's bound* [79]: It was shown that θ_a and θ_c are related through the inequality

$$\frac{\theta_c^2}{N} + \frac{N-1}{N(M-1)} \frac{\theta_a^2}{N} \geq 1,$$

which provides a lower bound on one of the maxima if the value of the other is specified. Compared with the Welch bound, the Sarwate bound treats the inner products corresponding to AC and CC separately. When θ_c and θ_a are replaced by θ_{max}, the Welch bound can be obtained.

1.1.2 Sequences with good correlation

Sequence design has gradually become a broad research area as different communication scenarios impose different requirements on the properties of sequences. Researchers have various focuses as well. Some of them concentrate on binary sequences or quaternary sequences, while others are interested in q-ary sequences. Some researchers focus only on sequences with good AC, while others investigate sequences with both good AC and CC. In the following, we briefly give an overview of some known works on sequences with good correlation.

Sequences with good AC

Sequences with good AC have applications in pulse compression radars, synchronization systems, cryptography, in addition to spread spectrum communication systems such as CDMA [27]. In the following, we roughly classify sequences based on their alphabets and discuss the best AC property they can achieve.

i) Binary and quaternary sequences

For a binary sequence $\mathbf{s}$ of period N, it is well known that the smallest possible value of AC function $R_{\mathbf{s}}(\tau)$ for all $0 < \tau < N$ can be classified into the following four types [43]:

i) $R_{\mathbf{s}}(\tau) \in \{0, 4\}$ if $N \equiv 0 \bmod 4$;

ii) $R_{\mathbf{s}}(\tau) \in \{1, -3\}$ if $N \equiv 1 \bmod 4$;

iii) $R_{\mathbf{s}}(\tau) \in \{2, -2\}$ if $N \equiv 2 \bmod 4$;

iv) $R_{\mathbf{s}}(\tau) \in \{-1, 3\}$ if $N \equiv 3 \bmod 4$.

For the first case, when $R_{\mathbf{s}}(\tau) = 0$ for all $0 < \tau < N$, i.e., the maximum out-of-phase periodic AC magnitude $\theta_a = 0$, then $\mathbf{s}$ is a perfect binary sequence. Unfortunately, the

only known example is $(1, 1, 1, -1)$ and it is shown [51] that perfect binary sequences do not exist for length < 12100, except for length 4. Binary sequences with AC values dropping in the above four cases are said to be *optimal*. Many known families of optimal binary sequences are constructed from combinatorial objects. For example, the well-known binary m-sequences and Gordon-Wills-Welch (GMW) sequences with optimal AC correspond to difference sets with Singer parameters in combinatorics [29].

Perfect quaternary sequences have only been found for periods 2, 4, 8 and 16. It is conjectured in [14] that no perfect sequences with period larger than 16 exist. Therefore, quaternary sequences with $\theta_a = 1$ for odd N and $\theta_a = 2$ for even N are said to have optimal AC. We refer the reader to [8, 24, 38, 41, 43, 58, 59] for further information on optimal binary and quaternary sequences.

ii) Polyphase or q-ary sequences

Non-binary sequences may be divided into two classes [38]. The first class consists of sequences whose alphabet size can be some small integer compared with their periods, while the second comprises sequences whose alphabet size is of the order of the period of the sequences. We introduce these two families of sequences in the following, respectively.

i) q-ary sequences with small alphabet: No perfect q-ary sequences with small alphabet have been reported. In this case, q-ary sequences with $\theta_a = 1$ are said to be *optimal*.

For example, a q-ary m-sequence with period $q^m - 1$ is defined by

$$\mathbf{s} = \{s(t) = \omega_q^{\mathrm{Tr}_m(\alpha^t)}\}_{t=0}^{q^m-1},$$

where q is a prime, $m \geq 1$ is an integer, $\mathrm{Tr}_m(x) = \sum_{i=0}^{m-1} x^{q^i}$ is the absolute trace function from the finite field $\mathbb{F}_{q^m}$ to the subfield $\mathbb{F}_q$, and α is a primitive element in $\mathbb{F}_{q^m}$. Then

$$R_{\mathbf{s}}(\tau) = \begin{cases} -1 & if\ \tau \not\equiv 0 \bmod q^m - 1, \\ q^m - 1 & if\ \tau \equiv 0 \bmod q^m - 1. \end{cases}$$

In particular, when $q = 2$, $\mathbf{s}$ is an optimal binary m-sequence. Many other optimal q-ary sequences have been proposed such as GMW sequences [29], Dillon sequences [13], Helleseth-Gong sequences [37]. We refer the reader to [4, 38] for further information.

ii) q-ary sequences with large alphabet: Even though the large size of the alphabet might be a disadvantage in some applications, there exist infinite families of perfect polyphase sequences in this case. For a sequence $\mathbf{s} = \{s(t) = \omega_q^{f(t)}\}$, $\{f(t)\}$ in this case are often defined over the ring of integers modulo q, i.e., $\mathbb{Z}_q$. Therefore, q-ary (polyphase) sequences with large alphabet are also referred to as $\mathbb{Z}_q$-sequences.

The research topics in this thesis are based on perfect polyphase sequences. A list of known perfect polyphase sequences will be given in Section 1.2.1. We omit here to avoid repetition.

We have introduced the smallest possible AC values for q-ary sequences. As we have mentioned, perfect sequences are relatively rare, and only q-ary sequences with large alphabet have infinite families of perfect sequences. A family of sequences, named *almost perfect sequences*, have been intensively studied as well. Instead of focusing on the smallest possible AC values, almost perfect sequences are defined as complex periodic sequences such that the out-of-phase AC values are zero with one exception. Of course, it would be useful if the exceptional value is also small, but this is not required. More information on almost perfect sequences can be found in [43, 75, 105].

Sequences sets with good correlation

Since numerous sequences with good AC have been studied, it is natural to investigate their cross-correlation properties. It is well known that the d-decimation of an m-sequence $\mathbf{s}^d = \{s(dt) = \mathrm{Tr}_m(\alpha^{dt})\}_{t=0}^{q^m-1}$ is also an m-sequence, provided that d is co-prime to the period $N = q^m - 1$. The cross-correlation function between an m-sequence and its d-decimated sequence has been completely determined for some values of d. For example, binary cases $d = 2^{\frac{m}{2}+1} - 1$ and $m \equiv 0 \bmod 4$ by Niho [68] and $d = 2^{\frac{m}{2}} + 3$ and m even by Helleseth [36]. For more information on different values of d for non-binary cases, readers are referred to [38, 107].

A natural way to construct families of sequences with low correlation, is to choose from sequences with optimal or ideal AC in which any pair of sequences maintains low CC values. Due to the theoretical bounds, it is of great interest to design a sequence set with $\sqrt{N} \leq \theta_{\max} \leq \sqrt{2N}$, where N is the period of the sequences in the family.

Two known families based on binary m-sequences are families of Gold and Kasami sequences [26] [44]. Let $\mathbf{s} = \{s(t)\}$ be an m-sequence of period $N = 2^m - 1$.

- Gold sequences: Let $d = 2^k + 1$ with $\gcd(k, m) = 1$. The Gold sequence set of size $N + 2$ is defined by

$$\mathcal{S} = \{s(t)\} \cup \{s(dt)\} \cup \{s(t) + s(d(t+\tau))|0 \leq \tau < N\},$$

  where $\theta_{max} = \sqrt{2(N+1)} + 1$.

- Kasami sequences: Let $d = 2^{\frac{m}{2}} + 1$ and m be an even integer. The Kasami sequence set of size $2^{\frac{m}{2}}$ is defined by

$$\mathcal{S} = \{s(t)\} \cup \{s(t) + s(d(t+\tau))|0 \leq \tau < 2^{\frac{m}{2}} - 1\},$$

  where $\theta_{max} = 2^{\frac{m}{2}} + 1$.

Note that both sets do not strictly meet theoretical bounds. But they are optimal with respect to Sidelnikov's bound and Welch's bound, respectively, because they are

proven to have the least possible values of θ_{max} for the given alphabet, period and family size. Other families that are asymptotically optimal with respect to Welch bound are bent sequences by Olsen, Scholtz and Welch [69], and sequences constructed by Sidelnikov [83]. Many families of q-ary sequences having small alphabet with low correlation have also been proposed. Excellent surveys and fundamental discussions on related topics can be found [24, 38].

For q-ary sequences with large alphabet, there exist several classes of known constructions of perfect sequences (see Section 1.2.1). Families of perfect sequences with low CC are one of the main focuses in this thesis. To avoid repetition, more details about related work are presented in Section 1.2.2. Some other constructions of sequences with large alphabet and low correlation are reported in [1, 64, 80].

1.1.3 Research objectives

Following the previous discussion on sequences with good correlation, we introduce two research topics in this thesis.

As we have mentioned, there exist known infinite families of perfect polyphase sequences. Choosing sequences from these families such that they exhibit low CC values is one of the research objectives in this thesis. In the following, we investigate what is the best CC property they can achieve according to the theoretical bound.

Different from Welch's bound and Sidelnikov's bound that give lower bounds on $\theta_{\max}$, Sarwate's bound shows that θ_a and θ_c are related through

$$\frac{\theta_c^2}{N} + \frac{N-1}{N(M-1)}\frac{\theta_a^2}{N} \geq 1. \tag{1.1}$$

When each sequence in a set is perfect, i.e., $\theta_a = 0$, then a lower bound on θ_c implied by (1.1) is

$$\theta_c \geq \sqrt{N},$$

where N is the period of the sequences in the set. A pair of perfect sequences with $\theta_c = \sqrt{N}$ is said to be *an optimal pair*. A set of perfect sequences is said to have *optimal correlation* when each pair in the set is an optimal pair.

Due to practical applications, one would like the number of perfect sequences with optimal correlation to be as large as possible. We see from (1.1) that the parameter M vanishes when $\theta_a = 0$ is zero. It is unknown how large a set of perfect sequences with optimal correlation can be. A list of known works on this topic as well as the constructions in this thesis is presented in Section 1.2.

All three theoretical bounds introduced in Section 1.1.1 imply that it is impossible to have sequences which have simultaneously zero out-of-phase AC and zero CC during an entire period. However, sequences with both simultaneously being zero in a smaller zone around the origin do exist. Such sequences with zero correlation zone (ZCZ) are called *ZCZ sequences*. The other research objective of this thesis is to construct optimal ZCZ sequence sets with respect to some theoretical bound. More details about ZCZ

sequences including related works and new results are given in Section 1.3.

1.2 Perfect polyphase sequences with optimal correlation

In this section, we focus on sets of perfect polyphase sequences whose maximum cross-correlation magnitude meets the Sarwate bound. It is worth mentioning that such families of sequences also asymptotically meet the Sidelnikov bound, and they nearly meet the Welch bound when the number of sequences is close to the period of the sequences. Since they are based on perfect polyphase sequences, we first give a brief introduction to all known perfect polyphase sequences in Section 1.2.1, after which related works are presented in Section 1.2.2. Finally, we give summaries of Paper I and a part of Paper II that describe our contributions on this topic in Section 1.2.3.

1.2.1 Perfect polyphase sequences

Perfect sequences have been extensively studied because of their applications in spread spectrum communications [84], channel estimation and fast start-up equalization [65], pulse compression radars [25, 48], sonar systems [108], and system identication [102].

Many different types of perfect sequences have been reported. Perfect unimodular (PSK) sequences are studied in [22] [23]. Golomb and Lüke proposed synthesized perfect real-valued sequences in [28, 56]. We know that $(1, 1, 1, -1)$ is the only known perfect binary sequence. By allowing 0, constructions of perfect $0, \pm 1$ sequences are presented in [39, 82]. Polyphase sequences allowing one or some zeros are also studied, which are called almost-polyphase sequences. Constructions of perfect almost-polyphase sequences are reported in [46, 47, 50, 57]. Polyphase sequences are special PSK sequences with constant magnitude. We limit our discussion to perfect polyphase sequences in the thesis.

We first give some transformations which preserve the ideal AC property. Let $\mathbf{s} = \{s(t)\}_{t=0}^{N-1}$ be a perfect sequence of period N. Then the variants of the sequence $\mathbf{s}$ under the following transformations are still perfect sequences [14].

i) Scaling: $s(t) \rightarrow cs(t)$ for any nonzero complex number c;

ii) Cyclic shift: $s(t) \rightarrow s(t + \tau)$ for any integer τ;

iii) Decimation: $s(t) \rightarrow s(dt)$ for any integer d satisfying $\gcd(d, N) = 1$;

iv) Conjugation: $s(t) \rightarrow s^*(t)$;

v) Linear-frequency modulation: $s(t) \rightarrow s(t)\zeta^t$, where ζ is any complex n-th root of unity.

Beside these perfectness-preserving transformations, the product of two perfect sequences with relatively prime periods is also perfect [56]. Two perfect sequences of

the same period are said to be *equivalent* if one can be obtained from the other via the successive application of the above transformations.

In the following, we give a list of all known constructions of perfect polyphase sequences. Two well-known families are Zadoff-Chu sequences and Frank-Zadoff (a.k.a. Frank-Zadoff-Heimiller) sequences, and many other constructions are based on these two families. There are also several constructions from one-dimensional generalised bent functions. A unified construction that includes all these families is also presented.

Based on Zadoff-Chu sequences

- Zadoff-Chu sequences [10] [18] 1972

$$s(t) = \begin{cases} \omega_N^{\frac{1}{2}t^2+ct} & t = 0, 1, \cdots, N-1, \ for\ N\ even, \\ \omega_N^{t(t+1)/2+ct} & t = 0, 1, \cdots, N-1, \ for\ N\ odd, \end{cases}$$

  where c is any integer.

- Ipatov sequences [42] 1979

$$s(t) = \omega_N^{t^2+ct}, \ t = 0, 1, \cdots, N-1, \ N \text{ odd}, c \text{ is any integer},$$

  In 1985, Kumar, Scholtz and Welch investigated this class of sequences from the perspective of generalised bent functions [49, Th. 2]. It was explained in [73] that Ipatov sequences are equal to Zadoff-Chu sequences of odd period N.

- Milewski sequences [65] 1983

$$s(t) = a(t_2 \bmod m)\omega_{m^{h+1}}^{t_1 t_2}, \ t = 0, 1, \cdots, N-1,$$

  where $N = m^{2h+1}$, $m \geq 2$ is an integer, $t = t_1 + t_2 \cdot m^h$, $0 \leq t_1 < m^h$, $0 \leq t_2 < m^{h+1}$, and $\{a(i)\}$ is a Zadoff-Chu sequence of period m.

- Generalised chirp-like sequences by Popović [73] 1992

$$s(t) = a(t)b(t \bmod m), \ t = 0, 1, \cdots, N-1, \tag{1.2}$$

  where $\{a(t)\}$ is a Zadoff-Chu sequence of period $N = rm^2$, r and m are any positive integers, and $\{b(i)\}_{i=0}^{m-1}$ is any sequence of m complex number having magnitude 1.

We can see from above that generalised chirp-like sequences and Milewski sequences are based on Zadoff-Chu sequences. It is obvious that generalised chirp-like sequences include Zadoff-Chu sequences and Ipatov sequences as special cases. It was shown [66] that Milewski sequences in some case are special cases of generalised chirp-like sequences, but not completely included by them.

Based on Frank-Zadoff-Heimiller sequences

- Heimiller sequences [35] 1961

$$s(t) = \omega_p^{\pi(t_1)\cdot(t_2+\sigma(t_1))},$$

where $N = p^2$, p is prime, $t = t_1 + t_2 \cdot p$, $0 \le t_1, t_2 < p$, π is an arbitrary permutation of $\mathbb{Z}_p$ and σ is an arbitrary function from $\mathbb{Z}_p$ to $\mathbb{Z}_p$.

- Frank-Zadoff sequences [19] 1962

$$s(t) = \omega_m^{t_1\cdot t_2}, \tag{1.3}$$

where $N = m^2$, m is any positive integer, $t = t_1 + t_2 \cdot m$, $0 \le t_1, t_2 < m$.

- Generalised Frank sequences by Kumar, Scholtz and Welch [49] 1985

$$s(t) = \omega_N^{m\pi(t_1)\cdot t_2+\sigma(t_1)}, \tag{1.4}$$

where $N = m^2$, m is any positive integer, $t = t_1 + t_2 \cdot m$ and $0 \le t_1, t_2 < m$, π is an arbitrary permutation of $\mathbb{Z}_m$ and σ is an arbitrary function from $\mathbb{Z}_m$ to $\mathbb{Z}_N$.

- Modulatable orthogonal sequences by Suehiro and Hatori [89] 1988

$$s(t) = \omega_m^{t_1\cdot t_2} b(t_1), \tag{1.5}$$

where $N = m^2$, m is any positive integer, $t = t_1 + t_2 \cdot m$, $0 \le t_1, t_2 < m$, and $\{b(i)\}_{i=0}^{m-1}$ is any sequence of m complex number having magnitude 1.

In this class, generalised Frank sequences are the most general case and include all the other cases as special cases.

Based on bent functions

An m-dimensional (generalized) bent function $f : \mathbb{Z}_q^m \to \mathbb{Z}_q$ is defined as a function with the property that all the m-dimensional Fourier coefficients of $f(\cdot)$ defined by

$$F(\lambda) = \frac{1}{q^{m/2}} \sum_{x\in\mathbb{Z}_q^m} \omega_q^{f(x)-\lambda^T x}, \ \forall \lambda \in \mathbb{Z}_q^m$$

have unit magnitude. When $m = 1$, it is called one-dimensional bent function. It is known [21,66] that a one-dimensional function f is bent if and only if the corresponding sequence $\{s(t) = \omega_q^{f(t)}\}$ is perfect. In 1985, Kumar, Scholtz and Welch proposed three constructions of one-dimensional bent functions [49]. Two of them are included by generalised chirp-like sequences. The third one is well-known as generalised Frank sequences. We introduce two other families as follows.

- Generalised bent function by Chung and Kumar [11] 1989

  Let q be an integer with $q \not\equiv 2 \bmod 4$. A function $f : \mathbb{Z}_q \to \mathbb{Z}_q$ defined by

  $$f(t+1) = f(t) + a(t), \ \forall\, t \text{ and } f(0) \in \mathbb{Z}_q,$$

  where $\{a(t)\}$ satisfy

  $$\begin{cases} \sum_{t=0}^{r-1} a(t) = 0 (\bmod\, r); \\ a(t+mr) = a(t) + cmr, \forall t \in \mathbb{Z}_r, \forall m \in \mathbb{Z}_{q/r}, \end{cases}$$

  for some integer c with $\gcd(c, q) = 1$, and r is any integer satisfying $r \equiv q (\bmod\, 2)$ and $r^2 | q$, is bent. Later Mow gave a closed-form of this recursive construction, which is included as a special case in a unified construction of perfect polyphase sequences [66].

- Bent function by Gabidulin [21] 1995

  Let $q = p^{2h}$, where p is a prime and h is a positive integer. Let $t = t_1 + t_2 p^h$, where $0 \le t_1, t_2 \le p^h - 1$. Then a function $f : \mathbb{Z}_q \to \mathbb{Z}_q$ defined by

  $$f(t) = F(t_1) + x_2 G(x_1) p^h,$$

  where F is any function taking values in $\mathbb{Z}_q$ and G is a permutation over $\mathbb{Z}_{p^h}$, is bent. Note that this construction is a special case of generalised Frank sequences.

Based on known perfect sequences

The idea of constructing new perfect sequences based on known ones is not new. For example, Mileswki sequences and generalised chirp-like sequence are based on known perfect sequences, specifically, Zadoff-Chu sequences. However, the construction by Gabidulin is based on any perfect sequences of prime period.

- Gabidulin sequences [20] 1993

  $$s(t) = a(t_2) \omega_{p^h}^{t_1 t_3} \omega_{p^{h+1}}^{t_1 t_2}, \ t = 0, 1, \cdots, N-1,$$

  where $N = p^{2h+1}$, p is prime, $t = t_1 + t_2 \cdot p^h + t_3 \cdot p^{h+1}$, $0 \le t_1 < p^h$, $0 \le t_2 < p$, $0 \le t_3 < p^h$, and $\{a(t_2)\}$ is a perfect sequence of period p.

  It is pointed out by Fan and Darnell [16] that this is equivalent to Milewshi sequences if the perfect sequence $\{a(t_2)\}$ is a Zadoff-Chu sequence.

A unified construction of perfect sequences

- Mow's unified construction [67] 1996

  $$s(t) = \omega_{rm}^{mc(r)\alpha(l)k^2 + \beta(l)k + g(l)}, \tag{1.6}$$

where $N = rm^2$, r and m are positive integers, $t = km+l, 0 \leq k < rm, 0 \leq l < m$, $c(r)$ is 1 when r is odd and $\frac{1}{2}$ otherwise, $\alpha : \mathbb{Z}_m \to \mathbb{Z}_r$ is any function with $gcd(\alpha(l), r) = 1$, $\beta : \mathbb{Z}_m \to \mathbb{Z}_{rm}$ is any function such that $l \mapsto \beta(l) \bmod m$ is a permutation over $\mathbb{Z}_m$, and g is any function over the rational numbers.

This unified construction includes all the previously mentioned constructions as special cases. Moreover, it was proven that no more perfect sequences can be obtained by applying the perfectness-preserving transformations and the direct construction to the unified construction. It was also conjectured that this unified construction describes all the perfect sequences that exist [67].

Discussions

There are some related works on perfect polyphase sequences in recent years. Liu and Fan presented modified Chu sequences with smaller alphabet size [54]. For even period case, it is no longer a perfect sequence. For odd period case, it is the same as normal Chu sequences, which is included in the unified construction. Following the similar idea as in [54], Blake and Tirkel derived a construction of perfect polyphase sequences based on the generalised Frank sequences [5]. In 2009, Ma and Ng investigated non-existence of p-ary perfect sequences [61], where p is an odd prime. In 2014, Soltanalian and Stoica studied the existence of perfect polyphase sequences with a prime-size alphabet [85]. In 2016, Park, Song, Kim and Golomb proposed a construction of perfect polyphase sequences based on generators and array structures [70], which are essentially generalised Frank sequences of prime period. Later this result was extended to a general case in [86] and the generated sequences are equivalent to generalised Frank sequences.

1.2.2 Related works

In this subsection, we give an overview of sets of perfect polyphase sequences with optimal correlation, i.e., the maximum CC magnitude $\theta_c = \sqrt{N}$, where N is the period of the sequences. As we have discussed previously in Section 1.1.3, the size of such sequence set vanishes in the Sarwate bound. It is unclear how large the size can be. However, one would like the size to be as large as possible due to practical applications. In the following, we give a list of known constructions that are based on different perfect polyphase sequences.

- Based on Zadoff-Chu sequences by Sarwate [79] 1979

$$\mathcal{S} = \{s_j(t) = \omega_N^{M_j t^2},\ t = 0, 1, \cdots, N-1,\ N \text{ odd} \mid 1 \leq j \leq p-1\},$$

where p is the smallest prime divisor of odd N and M_j is the multiplicative inverse of j modulo N.

- Based on Zadoff-Chu sequences by Alltop [1] 1980

$$\mathcal{S} = \{s_j(t) = \omega_N^{jt^2},\ t = 0, 1, \cdots, N-1,\ N \text{ odd} \mid 1 \le j \le p-1\},$$

where p is the smallest prime divisor of odd N.

- Based on decimations of Frank-Zadoff-Heimiller sequences by Alltop [2] 1984

$$\mathcal{S} = \{s_j(t) = \omega_p^{jt_1 \cdot t_2} \mid \gcd(j, N) = 1 \text{ and } \gcd((j_1{}^{-1} j_2)^2 - 1, N) = 1\},$$

where $N = p^2$, p is prime, $t = t_1 + t_2 \cdot m$, $0 \le t_1, t_2 < m$, and j_1, j_2 are any two distinct integers that are coprime to N. The largest families meeting the Sarwate bound contain $(p-1)/2$ distinct sequences.

- Based on modulatable orthogonal sequences by Suehiro and Hatori [89] 1988

$$\mathcal{S} = \{s_j(t) = \omega_p^{jt_1 \cdot t_2} b(t_1) \mid 1 \le j \le p-1\},$$

where $N = p^2$, p is prime, $t = t_1 + t_2 \cdot p$, $0 \le t_1, t_2 < m$, and $\{b(i)\}_{i=1}^{m-1}$ is any sequence of m complex numbers having magnitude 1.

- Based on generalised chirp-like sequences by Popović [73] 1992

$$\mathcal{S} = \{\{s_j(t) = \omega_N^{jt(t+1)+ct} b(t \bmod m)\}_{t=0}^{N-1} \mid \gcd(j, N) = 1 \text{ and } \gcd(j_1 - j_2, N) = 1\},$$

where N is odd, $N = rm^2$ with r and m are any positive integers, $\{b(i)\}_{i=0}^{m-1}$ is any sequence of m complex numbers having magnitude 1, and j_1, j_2 are any two distinct integers that are coprime to N. When $1 \le j \le p-1$, the construction yields $p-1$ sequences with optimal correlation, where p is the smallest prime divisor of N.

- Based on Frank-Zadoff-Heimiller sequences by Gabidulin [20] 1993

$$\mathcal{S} = \{s_j(t) = \omega_p^{jt_1 \cdot t_2} b(t_1) \mid 1 \le j \le p-1\},$$

where $N = p^{2k}$, p is an odd prime, $t = t_1 + t_2 \cdot p$, $0 \le t_1, t_2 < p^k$, and $\{b(i)\}_{i=1}^{m-1}$ is any sequence of m complex numbers having magnitude 1.

Note that this is a special case of the construction by Suehiro and Hatori [89].

- Based on Gabidulin sequences [20] 1993

$$\mathcal{S} = \{s_j(t) = \omega_p^{jt_2^2} \omega_{p^h}^{t_1 t_3} \omega_{p^{h+1}}^{t_1 t_2} \mid 1 \le j \le p-1\},$$

where $N = p^{2h+1}$, p is an odd prime, $t = t_1 + t_2 \cdot p^h + t_3 \cdot p^{h+1}$, $0 \le t_1 < p^h$, $0 \le t_2 < p$, $0 \le t_3 < p^h$.

- Based on the unified construction by Mow [67] 1996

$$\mathcal{S} = \{s_j(t) = \omega_{rm}^{mc(r)jk^2+jlk+g(l)} \mid 1 \le j \le p-1\},$$

where $N = rm^2$, r and m are positive integers, $t = km+l$, $0 \le k < rm$, $0 \le l < m$, $c(r)$ is 1 when r is odd and $\frac{1}{2}$ otherwise, g is any function over the rational numbers and p is the smallest prime divisor of N.

- Based on generators and array structures by Park et al. [70] 2016

$$\mathcal{S} = \{s_j(t) = \omega_p^{j\pi(t_1)\cdot t_2+\sigma(t_1)} \mid 1 \le j \le p-1\},$$

where $N = p^2$, p is an odd prime, $t = t_1 + t_2 \cdot p$, $0 \le t_1, t_2 < m$, σ is an arbitrary function over $\mathbb{Z}_p$, and π is a permutation of $\mathbb{Z}_p$ such that $j_1\pi(t_1+\tau') = j_2\pi(t_1)$ has exactly one solution for all $\tau' = 0, 1, \cdots, p-1$ and $1 \le j_1 \ne j_2 \le p-1$.

Note that sequences in this construction are generalised Frank sequences of prime period. Later this construction was extended to the case of odd N in [86], which is essentially based on generalised Frank sequences of odd period.

We can see that the size of all above constructions is based on the smallest prime divisor p of the period N and the number of perfect polyphase sequences with optimal correlation is at most $p-1$. In addition, all of these constructions are defined only for odd period, and they are trivial when N is even.

Papers I and II build a connection between polyphase sequences and well-studied combinatorial objects, circular Florentine arrays. From this connection, perfect sequences with optimum cross-correlation properties are derived. Moreover, the size of the perfect sequences depends on the existence of circular Florentine arrays. As a result, the number of the perfect sequences with optimal correlation is improved for some cases, compared with the previous results.

1.2.3 Summaries of Paper I and a part of Paper II

Paper I concerns generalised Frank sequences. The connection between circular Florentine arrays and generalised Frank sequences allows us to derive $F_c(N)$ perfect sequences of period N^2 with optimal correlation, where $F_c(N)$ is the maximum number such that an $F_c(N) \times N$ circular Florentine array exists. The main construction is as follows.

Let N be a positive integer and C be an $M \times N$ circular Florentine array, where $M = F_c(N)$. A set of permutations from each row of C is denoted by Π, i.e., $\Pi = \{\pi_0, \pi_1, \cdots \pi_{M-1}\}$. A sequence set of period N^2 of size M is defined as

$$\mathcal{S} = \{\mathbf{s}_i \mid \mathbf{s}_i(t) = \omega_{N^2}^{N\cdot\pi_i(t_1)t_2+\sigma(t_1)}, 0 \le i \le M-1\},$$

where $t = t_1 + t_2 \cdot N$, $0 \le t_1, t_2 < N$, $\pi_i \in \Pi$ for $0 \le i \le M-1$, and σ is an arbitrary function from $\mathbb{Z}_N$ to $\mathbb{Z}_{N^2}$. Then $\mathcal{S}$ is a set of perfect sequences with optimal correlation.

The general lower bound on $F_c(N)$ is $p-1$, where p is the smallest prime divisor of N. But for non-prime N, the lower bound on $F_c(N)$ has been proved for many cases.

Then the number of perfect sequences with optimal cross-correlation is improved as a result. Unfortunately, $F_c(N) = 1$ when N is even. No optimal pair of perfect polyphase sequences can be derived.

Paper II extends the results in Paper I and adopts the unified construction of perfect polyphase sequences in (1.6) to obtain families of perfect sequences with optimal correlation.

Let $N = rm^2$, where r and m are positive integers. Let r^* denote the smallest prime divisor of r. Let C be an $F_c(m) \times m$ circular Florentine array over $\mathbb{Z}_m$, where $F_c(m)$ is the maximum number such that an $F_c(m) \times m$ circular Florentine array exists. We denote $P = \{\beta_1, \beta_2, \cdots \beta_{F_c(m)}\}$ a set of permutations over $\mathbb{Z}_m$ from each row of C. Let $M = \min(r^* - 1, F_c(m))$ be the minimum of $r^* - 1$ and $F_c(m)$. When $r \neq 1$, a set of perfect sequences of size M defined by

$$\mathcal{S} = \{\mathbf{s}_j | s_j(t) = \omega_{rm}^{mc(r)jt_1^2 + \beta_j(t_2)t_1 + g(t_2)}, 1 \leq j \leq M\},$$

meets the Sarwate bound, where $t = t_1 m + t_2$ for $0 \leq t_1 < rm$ and $0 \leq t_2 < m$, $\beta_j \in P$ for $1 \leq j \leq M$, and functions c and g are the same as defined in (1.6).

When $r = 1$, the construction in Paper II is the same as that in Paper I. When $r \neq 1$, the number of the perfect sequences with optimal correlation is determined by the minimum of $r^* - 1$ and $F_c(m)$, which improves the previous results for some cases due to the existence of circular Florentine arrays.

Paper II also presents a construction of multiple ZCZ sequence sets with low inter-set cross-correlation. To avoid repetition, more details are introduced in Section 1.3.3.

1.3 ZCZ sequence sets

In this section, we introduce the other research topic in this thesis: ZCZ sequences. The definition of ZCZ sequences and the theoretical bound, as well as their applications, are presented in Section 1.3.1. Section 1.3.2 gives an overview of known work and briefly mentions the contribution of this thesis. Section 1.3.3 summarizes the main results in Papers II-VI.

1.3.1 ZCZ sequences and their bound

In Quasi-Synchronous Code-Division Multiple-Access (QS-CDMA) communication systems [88], a time delay between the signals of different users within a few chips is allowed. To eliminate co-channel and multipath interference in such systems, a new type of spreading sequences called zero correlation zone (ZCZ) or low correlation zone (LCZ) sequences were proposed [17, 88]. Later Tang, Fan and Matsufuji [93] gave the corresponding bound on the correlation function of ZCZ(resp. LCZ) sequence set. Since then, many researchers have been devoted to constructing optimal ZCZ(resp. LCZ) sequence sets with respect to the bound. Meanwhile, the concept of zero correla-

tion zone has been extended to two-dimensional sequence sets [30] and complementary sequence sets [15], respectively. However, these two topics are beyond the scope of our discussion in this thesis.

ZCZ sequences with desirable properties have also applications in multi-antenna [77], underwater acoustic [76], ultrawideband [106], free-space optical communications [63] and inverse synthetic aperture radar imaging [60]. In telecommunication industry, ZCZ sequences have been used as uplink random access channel preambles in the fourth-generation cellular standard LTE [81] and 5G physical random access channel [71].

Definition

Let $\mathcal{S} = \{\mathbf{s}_0, \mathbf{s}_1, \cdots, \mathbf{s}_{M-1}\}$ be a sequence set of size M of period N. The set $\mathcal{S}$ is called an (N, M, Z)-ZCZ sequence set if

$$R_{\mathbf{s}_i}(\tau) = 0 \ \text{ for } (0 < |\tau| < z_a)$$

and

$$R_{\mathbf{s}_i,\mathbf{s}_j}(\tau) = 0 \ \text{ for } (0 \le |\tau| < z_c \text{ and } i \ne j),$$

where $Z = \min(z_a, z_c)$ is called the length of the zero correlation zone.

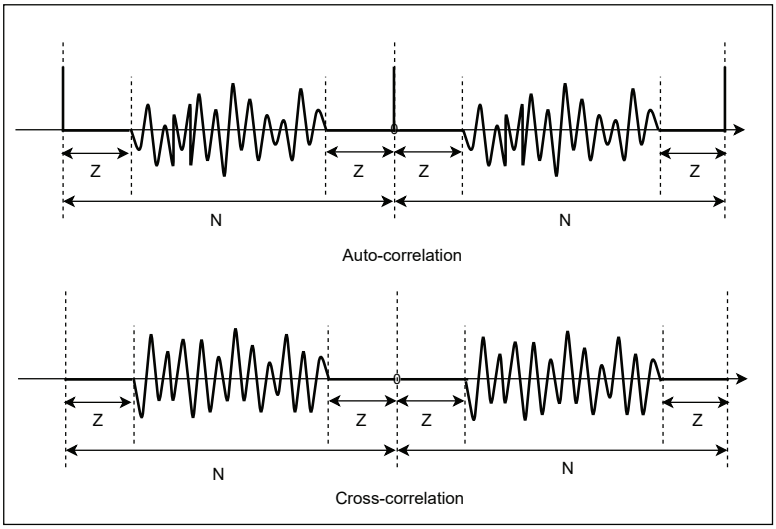


Figure 1.1: ZCZ sequences

ZCZ sequences are a class of spreading sequences with ideal correlation within a zone around the origin (see Figure 1.1). They are also referred to as interference free window (IFW) sequences (codes) in [87]. A ZCZ sequence set is generally characterized by the sequence period, the size of the set, the length of the ZCZ and the number of phases of the sequence elements. Given a sequence set of size M of period N, the following bound gives an upper bound on the ZCZ length.

Tang-Fan-Matsufuji Bound

Given an (N, M, Z)-ZCZ sequence set, the parameters are restricted by

$$MZ \leq N, \tag{1.7}$$

i.e., the ZCZ length Z is upper bounded by the period of sequences N divided by the size M [93]. A ZCZ sequence set meeting this bound is said to be *optimal*.

ZCZ sequences have zero out-of-phase auto-correlation and cross-correlation simultaneously in a zone around the origin. When the correlation of sequences in the zone is not zero but very small, they are called *sequences with low correlation zone* or *LCZ sequences*. The bound (1.7) and a lower bound on correlation of LCZ sequences, were derived from the Welch bound [93].

As we can see from (1.7), it has no restrictions on the behaviour of the correlation functions outside the zero correlation zone. Thus, trivial constructions of ZCZ sequence set can be derived based on perfect sequences as follows. Let $\mathbf{s}$ be a perfect sequences of period $N = MZ$, where M and Z are positive integers. Then $\mathbf{s}$ and its cyclic shifts form a set, defined by

$$\mathcal{S} = \{s_j(t) = s(t + jZ) \mid 0 \leq j \leq M - 1\},$$

which is an optimal (N, M, Z)-ZCZ sequence set. However, the CC function values of two sequences at shift $|\tau| = Z$ can be equal to N. This can be a defect in practice when a time delay is longer than expected. Therefore, it is important to construct ZCZ sequence sets in which all the sequences are cyclically distinct.

Two families of ZCZ sequences

Before presenting more related work on the design of ZCZ sequences, we introduce two special classes of ZCZ sequences with additional favorable properties as follows.

- Uncorrelated ZCZ sequence sets are a family of ZCZ sequences which have zero CC values across all shifts. When AC functions of each sequence have non-zero values only at subperiodic shifts, such uncorrelated ZCZ sequence sets are also referred to as Interference-Free Zero-Autocorrelation Zone (IF-ZAZ) sequence sets [74].

- A ZCZ sequence set is composed of perfect sequences. Instead of ideal CC properties, each sequence in such a set has ideal AC property, i.e., each sequence is a perfect sequence.

Since the theoretical bounds imply that it is impossible to have ideal AC and CC properties simultaneously within an entire period, these two families of ZCZ sequences illustrate the trade-offs between AC and CC properties, and have ideal CC and AC properties, respectively (see Figure 1.2).

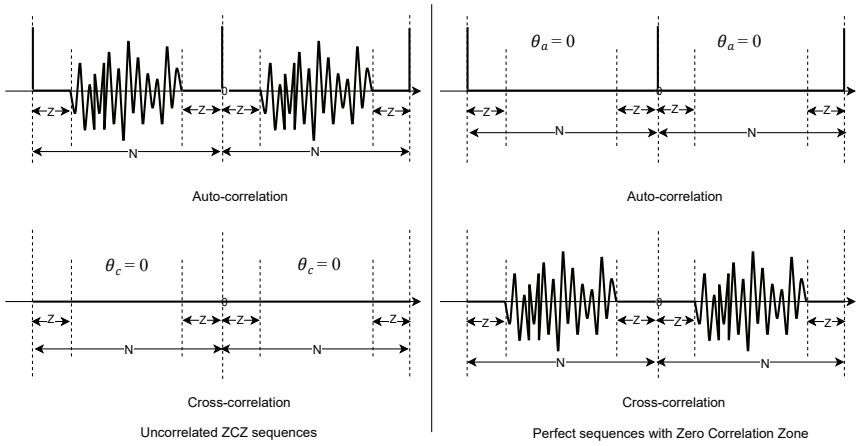


Figure 1.2

1.3.2 Related works

ZCZ sequences are a family of sequences that exhibits an ideal correlation zone among their members, which have been extensively studied because of their wide applications. Numerous constructions of ZCZ sequence sets based on different methods have been proposed. Moreover, to minimize the inter-cell interference in multi-user communication environments, constructions of multiple ZCZ sequence sets with favorable inter-set cross-correlation properties have also attracted lots of attention. In the following, we give a brief introduction to known constructions of ZCZ sequence sets and multiple ZCZ sequence sets, respectively. The contribution of this thesis and some related works are also included.

ZCZ sequence sets

A number of studies on constructing ZCZ sequence sets have been reported. Constructions presented in [3, 12, 90, 91] are based on complementary sequence sets. In this thesis, we mainly focus on constructions based on based on perfect sequences.

There are several methods to generate ZCZ sequences from perfect sequences. Constructions derived by using the transform domain method are proposed in [6, 55, 101]. Interleaving techniques were proven to be effective in [40, 92, 110]. Some other constructions by manipulating perfect sequences in different ways are reported in [32, 62, 72, 74, 97–99]. Among these, constructions in [32, 62, 97] can be reinterpreted from an interleaving perspective. We further discuss some related works in the following.

A: Transform domain method

Given a sequence $\mathbf{s}$ of period N, its discrete Fourier transform (DFT) generates a discrete periodic spectrum $\{F_k\}$, where $F_k = \sum_{t=0}^{N-1} s(t)e^{-i\frac{2\pi tk}{N}}$, $0 \le k \le N-1$. The relationship

between the AC function of $\mathbf{s}$ and its DFT is

$$F_k^* F_k = |F_k|^2 = \sum_{\tau=0}^{N-1} R_{\mathbf{s}}(\tau) e^{i\frac{2\pi\tau k}{N}}.$$

When $R_{\mathbf{s}}(\tau) = 0$ for $\forall \tau \not\equiv 0 \bmod N$, then $|F_k|^2 = R_{\mathbf{s}}(0)$ for all $0 \le k \le N-1$. It follows that $\mathbf{s}$ is a perfect sequence if and only if all components of $\{F_k\}$ have the same magnitude $|F_k| = \sqrt{R_{\mathbf{s}}(0)}$. Similarly, for two sequences $\mathbf{s}_1$ and $\mathbf{s}_2$ of period N, they are uncorrelated, i.e., $R_{\mathbf{s}_1,\mathbf{s}_2}(\tau) = 0$ for $\forall \tau$, if and only if $F_{1,k} F_{2,k}^* = 0$ for $\forall k$, where $\{F_{1,k}\}$ and $\{F_{2,k}\}$ are discrete Fourier transforms of $\mathbf{s}_1$ and $\mathbf{s}_2$, respectively.

Basically, the transform domain method transforms the correlation requirements into transform domain identities. With desirable properties of the spectral representations, sequences can be recovered by employing inverse discrete Fourier transforms. For example, IF-ZAZ (uncorrelated ZCZ) sequences were derived in [101] by using a set of orthogonal tones, i.e., the spectral representations of any two sequences are orthogonal. Instead of good CC properties, Liu, Chen and Su [55] made use of the fact that the spectrum of perfect sequences have constant magnitude and presented ZCZ sequences with ideal AC property. Instead of DFT, Brodzik used finite Zak transform (FZT) and derived several Zak space constructions of ZCZ sequences, including constructions of IF-ZAZ sequences [6, 7].

B: IF-ZAZ sequence sets

Several constructions of IF-ZAZ sequences based on transform domain method are mentioned above. We introduce two other constructions in the following.

We introduced a unified construction of perfect popyphase sequences in Section 1.2.1 [67]. This construction can be viewed as interleaving an uncorrelated and complementary set of sequences defined as follows. Let $\mathcal{U} = \{\mathbf{u}_0, \mathbf{u}_1, \cdots, \mathbf{u}_m\}$ be a set of m sequences. For $0 \le l < m$, each sequence $\mathbf{u}_l$ of period rm is defined by

$$u_l(k) = \omega_{rm}^{mc(r)\alpha(l)k^2+\beta(l)k+g(l)}, \ 0 \le k < rm, \tag{1.8}$$

where r and m are positive integers, functions c, α, β and g are the same as defined in (1.6). Apart from the uncorrelated and complementary properties of $\mathcal{U}$ given in [67], Paper III shows that all sequences in $\mathcal{U}$ possess a common zero correlation zone r. In other words, $\mathcal{U}$ is an (rm, m, r) IF-ZAZ sequence set.

Since g is any function over the rational numbers, let $g = mg'$, where g' is any function over the rational numbers. Then each sequence $\mathbf{u}_l$ above can be written as

$$u_l(k) = \omega_r^{c(r)\alpha(l)k^2+g'(l)} \omega_{rm}^{\beta(l)k},$$

where $\omega_r^{c(r)\alpha(l)k^2+g'(l)}$ is a Zadoff-Chu sequence of period r. This is generalised to any perfect sequences of period r by Popović [74] as follows. Let $\mathcal{U}' = \{\mathbf{u}'_0, \mathbf{u}'_1, \cdots, \mathbf{u}'_m\}$

be a set of m sequences. For $0 \leq l < m$, each sequence $\mathbf{u}'_l$ of period rm is defined by

$$u'_l(k) = a_l(k \bmod r)\omega_{rm}^{lk},\ 0 \leq k < rm,$$

where $\mathbf{a}_l$ is any perfect sequence of period r. Then the set $\mathcal{U}'$ is an (rm, m, r) IF-ZAZ sequence set and has exactly the same properties as $\mathcal{U}$.

These two constructions of IF-ZAZ sequence sets employ a short perfect sequence, and the period of the generated ZCZ sequences is a multiple of that of the perfect sequences.

C: Based on modulatable perfect sequences

In the following, we introduce several constructions based on modulatable perfect sequences. The generated ZCZ sequences have the same period as the employed perfect sequence.

Let $\mathbf{c}$ be a perfect sequence of period N. Then $\mathbf{c}$ is called modulatable if the corresponding modulated sequence defined by

$$s(t) = c(t) \cdot b(t \bmod m) \tag{1.9}$$

is also perfect, where $m|N$, $\mathbf{c}$ is called a carrier sequence, and $\mathbf{b}$ is any complex sequence of period m and is called a modulation sequence. The terminology of modulatable orthogonal (perfect) sequences was used in [89], where $\mathbf{c}$ is a Frank-Zadoff sequences (see (1.5)). More generally, the generalised Frank sequences (1.4) are also examples of modulatable perfect sequences. Later Popović [73] chose $\mathbf{c}$ to be Zadoff-Chu sequences and the corresponding modulated sequences are known as generalized chirp-like sequences (see (1.2)). To construct ZCZ sequences based on modulatable perfect sequences, it is common to use the same carrier sequence and adopt different modulation sequences such that the constructed sequences possess good CC properties.

Constructions of ZCZ sequence sets based on different modulatable perfect sequences have been proposed. Popović [72] derived optimal ZCZ sequences based on generalized chirp-like sequences. There are also several constructions based on generalised Frank sequences. Since generalised Frank sequences are related to bent functions and discrete Fourier transform (DFT) matrix, constructions of multiple ZCZ sequence sets based on functions in Papers V and VI and DFT matrix in [98, 99] are essentially based on generalised Frank sequences.

Inspired by the work mentioned above, it is natural to consider other perfect sequences. Mow gave a unified construction of perfect polyphase sequences in (1.6), which includes generalised Frank function and generalized chirp-like sequences. In addition to the construction of IF-ZAZ sequences in (1.8), Paper III also gives a construction of optimal ZCZ sequence sets with the expression (1.9) based on the unified construction. Moreover, each generated ZCZ sequence is also a perfect sequence.

D: Interleaving technique

Interleaving technique has been an important tool for sequence design, which allows us to generate sequences with long periods and desirable properties based on short sequences with good correlation.

Let $\mathbf{a} = (a(0), a(1), \cdots, a(N-1))$ be a perfect sequence of period N. Let $\mathbf{e} = (e_0, e_1, \cdots, e_{M-1})$ be a sequence of length M defined over $\mathbb{Z}_N$. Let L be the left cyclic shift operator such that $L^{e_i}(\mathbf{a})$ denotes the e_i-element left cyclically shifted version of $\mathbf{a}$. Then one can obtain an $N \times M$ matrix

$$L^{\mathbf{e}}(\mathbf{a}) = \begin{bmatrix} a_{e_0} & a_{e_1} & \cdots & a_{e_{M-1}} \\ a_{e_0+1} & a_{e_1+1} & \cdots & a_{e_{M-1}+1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{e_0+N-1} & a_{e_1+N-1} & \cdots & a_{e_{M-1}+N-1} \end{bmatrix},$$

denoted by $L^{\mathbf{e}}(\mathbf{a}) = [L^{e_0}(\mathbf{a}) \sim L^{e_1}(\mathbf{a}) \sim \cdots \sim L^{e_{M-1}}(\mathbf{a})]$ for convenience. By concatenating the successive rows of the matrix $L^{\mathbf{e}}(\mathbf{a})$, one obtains an interleaved sequence $\overline{\mathbf{a}}$ of length NM, where $\mathbf{a}$ and $\mathbf{e}$ are called the *component* and *shift* sequences of $\overline{\mathbf{a}}$, respectively. Mathematically, the interleaved sequence $\overline{\mathbf{a}}$ of period NM can be expressed by

$$\overline{a}(t) = \overline{a}(i + jM) = a(j + e_i),$$

where $0 \le j \le N-1, 0 \le i \le M-1$. A sequence set of size M based on the interleaved sequence can be defined by

$$\mathcal{S} = \{s_k(t) = \overline{a}(t) \cdot b_k(i) = a(j + e_i) \cdot b_k(i) \mid 1 \le k \le M\},$$

where $t = i + jM$, $0 \le j \le N-1$, $0 \le i \le M-1$, and $\mathbf{b}_k = \{b_k(i)\}$ is the k-th row of an $M \times M$ orthogonal matrix B.

The key of interleaving technique is to construct an appropriate shift sequence such that the sequence set $\mathcal{S}$ has desirable properties. ZCZ sequence sets are derived for the following cases:

- $e_t = M^{-1}t \pmod N$, when $gcd(N, M) = 1$ [62],
- $e_t = \frac{N}{M}t \pmod N$, when $M|N$ [97],
- $e_t = t \pmod N$, when $N|M$ [97].

Later Tang and Mow [92] presented a general construction of shift sequences, which includes the three cases above. We omit the expression here due to space constraints.

Instead of using a single shift sequence, a set of shift sequences can be used to increase the size of ZCZ sequences as follows. Let $\mathcal{E} = \{\mathbf{e}^0, \mathbf{e}^1, \cdots, \mathbf{e}^{L-1}\}$ be a set of shift sequences of length M. A sequence set of size ML of period NM can be defined by

$$\mathcal{S} = \{s_k^l(t) = a(j + e_i^l) \cdot b_k(i) \mid 1 \le k \le M,\ 0 \le l \le L\},$$

where $t = i + jM$, $0 \le j \le N-1$, $0 \le i \le M-1$, and $\mathbf{b}_k = \{b_k(i)\}$ is the k-th row of an $M \times M$ orthogonal matrix B.

Several constructions of ZCZ sequence sets with the expression above have been proposed. In [31], Hayashi employed a set of $L = 2n' + 1$ shift sequences of length $M = 2$, where n' is an odd integer. Later this result was extended to the case $M = 4$ in [32], where perfect ternary sequences were employed. Zhou, Tang and Gong gave a construction of shift sequence sets with $M = 2$ [110]. Later, more general M was considered by Hu and Gong [40]. A set of shift sequences, called a phase-shift vector set, was also proposed by Hayashi and Matsufuji [34].

All these constructions of shift sequence sets have strong constraints on the parameters under which the constructed ZCZ sequence set is optimal, as well as complex expressions. It is a challenge to construct sets of shift sequences with simple expressions and few constrains on the parameters.

In Paper IV, instead of trying to construct multiple shift sequences, we use multiple component sequences to increase the size of ZCZ sequences. Let $\mathcal{U} = \{\mathbf{u}_0, \mathbf{u}_1, \cdots, \mathbf{u}_{m-1}\}$ be a set of m sequences of period n, where $N = nm$. Let $\mathbf{e}$ be a sequence of length M defined over $\mathbb{Z}_N$. A sequence set of size mM of period NM can be defined by

$$\mathcal{S} = \{s_k(t) = u_{i \bmod m}(j + e_{\lfloor \frac{i}{m} \rfloor}) \cdot b_k(i) \mid 1 \le k \le mM\}, \tag{1.10}$$

where $t = i + jmM$, $0 \le j \le n-1$, $0 \le i \le mM-1$, and $\mathbf{b}_k = \{b_k(i)\}$ is the k-th row of an $mM \times mM$ orthogonal matrix B. With a set $\mathcal{U}$ and a shift sequence $\mathbf{e}$ properly chosen, optimal ZCZ sequences can be derived.

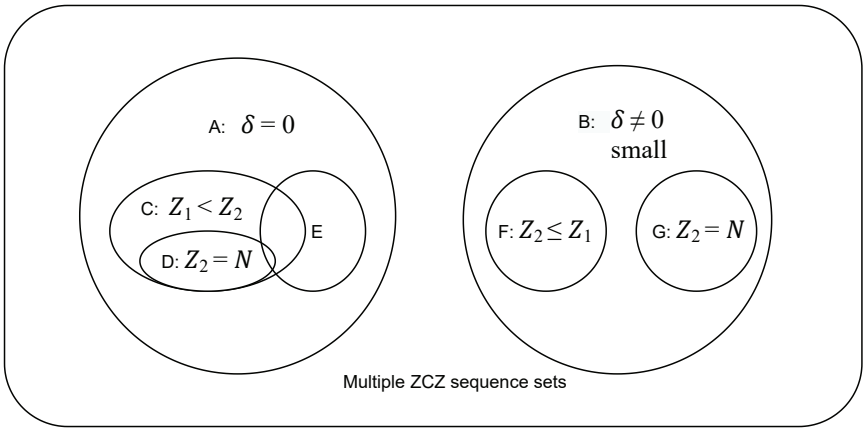
Multiple ZCZ sequence sets

In a cellular network, a ZCZ sequence set can be used to eliminate MAI and MPI in a single cell. However, sequences transmitted in different cells may also interfere with each other in multi-user environments. To minimize inter-cell interference, one promising solution is to construct multiple ZCZ sequence sets with favorable inter-set cross correlation.

Let $\mathbb{S} = \{\mathcal{S}^k \mid 0 \le k \le M_2\}$ be a set of M_2 sequence sets. For each $0 \le k \le M_2$, $\mathcal{S}^k = \{\mathbf{s}_0^k, \mathbf{s}_1^k, \cdots, \mathbf{s}_{M_1-1}^k\}$ is a set of M_1 sequences of period N. It is preferable to construct the set $\mathbb{S}$ with the following properties:

$$\begin{cases} R_{\mathbf{s}_i^k}(\tau) = 0 \ \text{ for } (0 < |\tau| < z_a \text{ and } \forall k), \\ R_{\mathbf{s}_i^k, \mathbf{s}_j^k}(\tau) = 0 \ \text{ for } (0 \le |\tau| < z_c, i \ne j \text{ and } \forall k), \\ |R_{\mathbf{s}_i^k, \mathbf{s}_j^l}(\tau)| \le \delta \ \text{ for } (0 \le |\tau| < Z_2, k \ne l \text{ and } \forall i, j), \end{cases}$$

where $Z_1 = \min(z_a, z_c)$ is called intra-set ZCZ length. Note that each set $\mathcal{S}^k$ is an (N, M_1, Z_1)-ZCZ sequence set and the maximum magnitude of the inter-set cross-correlation values within a zone is upper bounded by a constant δ. We discuss the



A: Mutually orthogonal ZCZ (MOZCZ) sequence sets
B: Multiple ZCZ sequence sets with low inter-set cross-correlation
C: Asymmetric ZCZ sequence sets
D: Asymmetric ZCZ sequence sets with inter-set uncorrelated sequences
E: Each ZCZ sequence set is optimal. All the sets together is also an optimal ZCZ sequence set.
F: Multiple ZCZ sequence sets with low inter-set cross-correlation within a small zone
G: Multiple ZCZ sequence sets with low inter-set cross-correlation within an entire period

parameter δ in the following two cases, after which some related works are given, respectively.

When $\delta = 0$, multiple ZCZ sequence sets possess a common zero correlation zone $Z = \min(Z_1, Z_2)$, where Z_2 is called the inter-set ZCZ length. Thus, the set $\mathbb{S}$ (all ZCZ sequences together) is an (N, M_1M_2, Z)-ZCZ sequence set.

When $\delta \neq 0$ and δ is a small value compared with the period of the sequences, we say such multiple ZCZ sets have low inter-set cross-correlation.

A: Multiple ZCZ sequence sets with a common zero correlation zone

When $\delta = 0$ and $Z_2 = 1$, such multiple ZCZ sequence are called mutually orthogonal ZCZ (MOZCZ) sequence sets, i.e., any two sequences that belong to different ZCZ sequence sets are orthogonal. Many constructions of MOZCZ sequence sets have been proposed. Based on mutually orthogonal complementary sequence sets (MOCSS), MOZCZ sequence sets were proposed in [3]. Based on interleaving technique, MOZCZ sequence sets from perfect sequences and orthogonal codes were derived in [100]. For more constructions of MOZCZ sequence sets, the readers are referred to [53, 109] and the references therein.

When $\delta = 0$ and $Z_1 < Z_2$, such multiple ZCZ sequence are known as asymmetric ZCZ sequence sets. Asymmetric ZCZ sequence sets emphasize the property that the inter-set ZCZ length is larger than the intra-set ZCZ length. A number of studies have been proposed [33, 90, 91, 94–96, 103]. A special case is when $\delta = 0$ and $Z_2 = N$, which implies that any two sequences from different sequence sets are uncorrelated. Asymmetric ZCZ sequence sets with inter-set uncorrelated sequences have been presented in [95, 103].

It was proposed as an open problem in [90] to construct multiple ZCZ sets satisfying two requirements: 1) each set is an optimal ZCZ set and 2) these sets possess a common zero correlation zone such that all sequences together from an optimal ZCZ set. Most of the previous results only satisfy one of these two requirements. In [91] [90], each set can be optimal but all these sets together can not generate an optimal ZCZ set. There are also many other constructions where all sets together can be optimal or almost optimal, but the optimality does not hold for a single set [33, 94–96, 103]. Multiple ZCZ polyphase sequence sets proposed in [53, 99] meet both requirements. Two arbitrary sequences that belongs to different ZCZ sequence sets are orthogonal in [53], i.e. $Z = 1$. The construction in [99] is derived from DFT matrices and orthogonal codes.

B: Multiple ZCZ sequence sets with low inter-set cross-correlation

Some constructions consider the inter-set cross-correlation property within the same zone as intra-set ZCZ zone, i.e., $Z_2 \leq Z_1$. Two families of multiple ZCZ binary sequence sets with low inter-set cross-correlation within the zone $Z_2 = Z_1$ were derived by constructing specific mutually orthogonal complementary sequence sets in [90, Th. 4, Th. 5]. Based on Zadoff-Chu sequences, Li et al. [52] obtained quaternary multiple ZCZ sequence sets with low inter-set cross-correlation within the zone $Z_2 = Z_1 = 4$.

Multiple ZCZ sequence sets having low inter-set cross-correlation within an entire period, i.e., $Z_2 = N$, are of particular interest in this thesis. In the following, we introduce some known constructions and our contributions.

Based on Zadoff-Chu sequences, $N - 1$ ZCZ sequence sets with parameters $(N, \lfloor \frac{N}{Z} \rfloor, Z)$ are used in 4G LTE systems as physical random access channel (PRACH) sequences, where N is a prime [71, 81]. Moreover, all employed sequences are perfect and the maximum inter-set cross-correlation is equal to $\sqrt{N}$, which meets the Sarwate bound. Therefore, such multiple ZCZ sequence sets possess optimal inter-set cross-correlation property.

Popović proposed ZCZ sequence sets based on generalised chirp-like sequences [72]. Together with a construction of the generalised chirp-like sequences with optimal cross-correlation property in [73], $p - 1$ ZCZ sequence sets with optimal inter-set cross-correlation are derived as a result, where p is the smallest prime divisor of the period of the sequences.

Paper V presents a construction of $N - 1$ ZCZ sequence sets of period N^2 based on a class of functions, of which the inter-set cross-correlation is equal to N for any shift τ, where N is prime. The generated sequences are essentially generalised Frank sequences of prime period, and thus each ZCZ sequence is perfect. Moreover, each set is an optimal (N^2, N, N)-ZCZ sequence set.

Later the results are generalised to odd case N in Paper VI and $p - 1$ ZCZ sequence sets are obtained, where p is the smallest prime divisor of N. The key to the optimal inter-set cross-correlation property is to construct a set of permutations satisfying certain properties. Paper VI presents a construction of permutation sets such that each ZCZ sequence set is optimal and sequences from different sets possess the optimal inter-set

cross-correlation property.

As we can see above, the number of the ZCZ sequence sets having optimal inter-set cross-correlation is $p-1$ in all the previous constructions, where p is the smallest prime divisor of the period of the sequences. Paper II proposes a construction of multiple ZCZ sequence sets based on circular Florentine arrays, which improves the number of the ZCZ sequence sets with optimal inter-set cross-correlation due to the existence of circular Florentine arrays.

1.3.3 Summaries of Papers III-VI and a part of Paper II

Paper III presents two constructions of ZCZ sequence set based on a unified construction of perfect sequences. The first construction defined by

$$\mathcal{S} = \left\{\mathbf{s}_i, 0 \le i < m \mid s_i(t) = \omega_{rm}^{mc(r)\alpha(l)k^2+\beta(l)k+irg(l)}\right\}$$

generates optimal ZCZ sequence sets with parameters (rm^2, m, rm), where $t = km + l$, $0 \le k < rm$, $0 \le l < m$, functions c, α, and β are defined in (1.6), function g is any permutation over $\mathbb{Z}_m$ such that there exist no c_1 and c_2 in $\mathbb{Z}_m^*$ with

$$c_1 \cdot (\beta(l) \bmod m) + c_2 \cdot g(l) = 0,$$

where $\mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{0\}$. The condition on functions β and g ensures that all the sequences are cyclically distinct. In addition, each ZCZ sequence is also perfect by (1.6). The second construction defined by (1.8) produces IF-ZAZ sequences with parameters (rm, m, r). The first construction have the optimal AC property in the sense that each sequence is perfect, while the second construction exhibits the optimal CC property, because any two different sequences are uncorrelated.

Paper IV proposes a new interleaving approach to constructing ZCZ sequence sets. Instead of constructing new shift sequences, we employ multiple component sequences with certain properties and derive ZCZ sequence sets with flexible parameters. The main results are as follows. With a proper single shift sequence of length M, the constructed set $\mathcal{S}$ defined by (1.10) is an (NM, mM, mz)-ZCZ sequence set when the initial set $\mathcal{U}$ is an (n, m, z) IF-ZAZ sequence set, where $N = nm$. The new construction has a smaller alphabet compared with an initial IF-ZAZ sequence set with the same parameters. Furthermore, the construction (1.10) is related to constructions based on perfect sequences when $\mathcal{U}$ is properly chosen. Compared with known related constructions, our construction has a less restrictive condition under which the constructed ZCZ sequence set is optimal. New optimal ZCZ sequence sets are obtained as a result.

Note that when $M = 1$, the construction(1.10) becomes

$$\mathcal{S} = \{s_k(t) = u_i(j) \cdot b_k(i) \mid 1 \le k \le m\},$$

where $t = i + jm$, $0 \le j \le n-1$, $0 \le i \le m-1$, and $\mathbf{b}_k = \{b_k(i)\}$ is the k-th row of an

$m \times m$ orthogonal matrix B. This generates an (nm, m, mz)-ZCZ sequence set based on any given initial (n, m, z) IF-ZAZ sequence set, which includes the construction in Paper III as a special case.

Papers V and VI address multiple ZCZ sequence sets with low inter-set cross-correlation. The generated multiple ZCZ sequence sets have following properties: 1) each sequence in each set is perfect; 2) each set is an optimal ZCZ sequence set; 3) multiple sets possess optimal inter-set cross-correlation property. The number of the ZCZ sequence sets in both papers is one less than the smallest prime divisor of the period of the sequences.

Paper V generates multiple ZCZ sequence sets based on perfect non-linear functions which are known as Frank-Zadoff sequences of prime periods. The construction is as follows.

Let p be an odd prime integer. For each $1 \leq m < p$, define a sequence set $\mathcal{S}^m$ of period p^2 and size p as

$$\mathcal{S}^m = \{\mathbf{s}_u^m \ : \ \mathbf{s}_u^m \triangleq \{s_u^m(t)\}_{t=0}^{p^2-1}, 0 \leq u < p\}.$$

Herein, for each $0 \leq t < p^2$,

$$s_u^m(t) = \omega_p^{m\pi(t_1)\cdot t_2 + u\sigma(t_1)}, \tag{1.11}$$

where $t = t_1 + t_2 \cdot p$ and $0 \leq t_1, t_2 < p$, π and δ satisfy conditions

- π is a permutation of $\mathbb{Z}_p$ such that the equation $\pi(x + a) \equiv c\pi(x) \pmod p$ has exactly one solution for any given $a \in \mathbb{Z}_p$;
- σ is a permutation of $\mathbb{Z}_p$ satisfying $\sigma \neq k\pi + l$ for any $k, l \in \mathbb{Z}_p$.

The contribution of Paper V is that we give explicit constraints on permutations π and σ that ensure desired properties. The constraint on π ensures the optimal inter-set cross-correlation property, while the constraint on the relationship between π and σ assures that all the sequences are cyclically inequivalent. In addition, we present a construction of such permutations meeting these requirements.

Paper VI generalises the results in Paper V to the case that p is odd. Let N be an odd integer and $\mathcal{M}$ be an index set. We denote $\Pi = \{\pi_m \mid \pi_m \text{ is a permutation over } \mathbb{Z}_N \text{ for } m \in \mathcal{M}\}$ a set of permutations. For each $m \in \mathcal{M}$, we define a sequence set as

$$\mathcal{S}^m = \{\mathbf{s}_n^m \mid \mathbf{s}_n^m(t) = \omega_N^{\pi_m(t_1)\cdot t_2 + n\cdot\sigma(t_1)}, 0 \leq n < N\},$$

where $t = t_1 + t_2 \cdot N$, $0 \leq t_1, t_2 < N$, $\pi_m \in \Pi$ and σ is a permutation over $\mathbb{Z}_N$. We show that each set is an optimal (N^2, N, N)-ZCZ sequence set.

We further prove that these $|\mathcal{M}|$ ZCZ sequence sets possess optimal cross-correlation if and only if the following conditions are satisfied:

- $\pi_{m_1}(t_1 + \tau_1) \equiv \pi_{m_2}(t_1) \pmod N$ has only one solution for $\tau_1 \in \mathbb{Z}_N$ and $m_1 \neq m_2 \in \mathcal{M}$,

- σ is a permutation over $\mathbb{Z}_N$ such that there exist no c_1 and c_2 in $\mathbb{Z}_N^*$ satisfying $c_1 \cdot \pi_m(t_1) + c_2 \cdot \sigma(t_1) = 0$ for each $m \in \mathcal{M}$,

where $|\mathcal{M}|$ is the cardinality of the set $\mathcal{M}$.

The contribution of Paper VI is to extend the constraints in Paper V to a general representation and propose a construction of permutation sets Π that meets the requirements. Moreover, the requirement for the permutation set Π inspired us to employ combinatorial objects to generate sequences with optimal correlation in Papers I and II.

The rest of Paper II presents a construction of multiple optimal ZCZ sequence sets based on the connection between circular Florentine arrays and the unified construction of perfect polyphase sequences. Let $N = rm^2$, where r and m are positive integers. Let

$$M = \begin{cases} F_c(m) & \text{when } r = 1, \\ \min(r^* - 1, F_c(m)) & \text{when } r \neq 1. \end{cases}$$

where r^* is the smallest prime divisor of r and $F_c(m)$ is the maximum number such that an $F_c(m) \times m$ circular Florentine array C over $\mathbb{Z}_m$ exists. Let $P = \{\beta_1, \beta_2, \cdots \beta_{F_c(m)}\}$ be a set of permutations from each row of C. Then M sequence sets can be defined as follows.

For each $1 \leq j \leq M$, a sequence set of size m of period N is defined as

$$\mathcal{S}^j = \{\mathbf{s}_i^j | s_i^j(t) = \omega_{rm}^{mc(r)jt_1^2 + \beta_j(t_2)t_1 + irg(t_2)}, 0 \leq i < m\},$$

where $t = t_1 m + t_2$, $0 \leq t_1 < rm$, $0 \leq t_2 < m$, function c is the same as defined in (1.6), $\beta_j \in P$ for $1 \leq j \leq M$, and g is a permutation over $\mathbb{Z}_m$ satisfying certain properties.

Each sequence is perfect and each set is an optimal (N, m, rm)-ZCZ sequence set. The maximum inter-set CC magnitude is $\sqrt{N}$, which achieves the Sarwate bound. When $r \neq 1$, the number of the ZCZ sequence sets depends on the minimum between $r^* - 1$ and $F_c(m)$. When $r = 1$ and m is non-prime, $M \geq q - 1$, which improves the results in Paper V and VI.

Chapter 2

Discussion and future work

This thesis concerns perfect polyphase sequences with low cross-correlation and ZCZ sequences based on perfect sequences. These two topics are connected, because perfect polyphase sequences with low cross-correlation can induce multiple ZCZ sequences with low inter-set cross-correlation, and the number of perfect sequences with low cross-correlation affects the number of the ZCZ sequence sets with optimal inter-set cross-correlation.

Since it is difficult to find new perfect polyphase sequences, most constructions of perfect polyphase sequences with low cross-correlation are based on the known perfect polyphase sequences. The goal is to find as many as possible perfect polyphase sequences of the same period with optimal cross-correlation. As we have discussed, the number of such sequences is limited by the smallest prime divisor of the period of the sequences or the existence of circular Florentine arrays of some order. Instead of restricting to the optimal cross-correlation property, it will be of great interest in the future to construct sequence sets with a larger size having almost optimal cross-correlation. Meanwhile, it will be interesting is to find new perfect polyphase sequences despite of the difficulty.

Based on different expressions, we classify some known constructions of ZCZ sequences of period NM into the following three representations:

1) $s_1(i + jM) = a_1(j + e_i) \cdot b_1(i),\ 0 \le j \le N-1, 0 \le i \le M-1$

2) $s_2(i + jM) = a_2(i + jM) \cdot b_2(i),\ 0 \le j \le N-1, 0 \le i \le M-1$

3) $s_3(i + jM) = a_3(j) \cdot b_3(i + jM),\ 0 \le j \le N-1, 0 \le i \le M-1$

where $\mathbf{a}_1$, $\mathbf{a}_2$ and $\mathbf{a}_3$ are perfect sequence of period N, NM, and N, respectively; $\mathbf{b}_1$, $\mathbf{b}_2$ and $\mathbf{b}_3$ are complex sequences of period M, M, and NM, respectively; and $\mathbf{e}$ is a sequence of length M defined over $\mathbb{Z}_N$. Here we call $\mathbf{a}_1$, $\mathbf{a}_2$ and $\mathbf{a}_3$ are carrier sequences and $\mathbf{b}_1$, $\mathbf{b}_2$ and $\mathbf{b}_3$ are modulation sequences. ZCZ sequence sets are derived by applying different modulation sequences on the same or different carrier sequences. Modulation sequences are used to preserve the orthogonality between ZCZ sequences.

Construction based on interleaving technique in [92] has the expression of Case 1). The main difficulty for this case is to find appropriate constructions of shift sequences

such that the generated sequences have desirable properties. Constructions in [40, 110] used multiple shift sequences $\mathbf{e}$ to increase the number of sequences, while Paper IV adopts multiple component sequence $\mathbf{a}_1$ to achieve flexible parameters.

For the expression of Case 2), [72] chooses $\mathbf{a}_2$ to be Zadoff-Chu sequences, while Papers V and VI adopt generalised Frank sequences. Paper III shows that the unified construction of perfect polyphase sequence is also applicable.

Case 3) generates IF-ZAZ sequences. In [67], $\mathbf{a}_3$ is chosen to be Zadoff-Chu sequences. It was shown in [74] that $\mathbf{a}_3$ can be any perfect sequences (not necessary to be perfect polyphase sequences). One disadvantage of these constructions is that the alphabet is always equal to or larger than the period of sequences.

For future work on the design of ZCZ sequences, the following research questions are interesting to explore.

- Construction of ZCZ sequences based on the transform domain method proposed in [55] consists of equivalent sequences. It will be interesting to find constraints in transform domain such that all the generated ZCZ sequences are cyclically distinct.

- For the design of multiple ZCZ sequence sets, it will be interesting to construct multiple optimal ZCZ sequence sets with new parameters for which all the sequences together also form an optimal ZCZ sequence set.

- The Tang-Fan-Matsufuji Bound shows that the number of the ZCZ sequences M is upper bounded by the period of sequences N divided by the zero correlation zone Z. This implies that the number of ZCZ sequences is always smaller than the period, which is too small to accommodate all users in a cell [71]. It will be interesting to design sequences with good correlation and a large family size.

Bibliography

[1] W. Alltop. Complex sequences with low periodic correlations (corresp.). *IEEE Transactions on Information Theory*, 26(3):350–354, May 1980.

[2] W. Alltop. Decimations of the Frank-Heimiller sequences. *IEEE Transactions on Communications*, 32(7):851–853, July 1984.

[3] R. Appuswamy and A. K. Chaturvedi. A new framework for constructing mutually orthogonal complementary sets and ZCZ sequences. *IEEE Transactions on Information theory*, 52(8):3817–3826, 2006.

[4] K. T. Arasu. Sequences and arrays with desirable correlation properties. In *In D. Crnković and V. Tonchev, editors, Information Security, Coding Theory and Related Combinatorics, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur.*, volume 29, pages 136–171, 2011.

[5] S. T. Blake and A. Z. Tirkel. A construction for perfect periodic autocorrelation sequences. In K.-U. Schmidt and A. Winterhof, editors, *Sequences and Their Applications - SETA 2014*, pages 104–108, Cham, 2014. Springer International Publishing.

[6] A. K. Brodzik. New polyphase sequence sets with all-zero cross-correlation. In *2012 IEEE International Symposium on Information Theory Proceedings*, pages 1421–1424, July 2012.

[7] A. K. Brodzik. On certain sets of polyphase sequences with sparse and highly structured Zak and Fourier transforms. *IEEE Transactions on Information Theory*, 59(10):6907–6916, 2013.

[8] Y. Cai and C. Ding. Binary sequences with optimal autocorrelation. *Theoretical Computer Science*, 410(24):2316 – 2322, 2009.

[9] T.-S. Chen, Y.-S. Chen, C.-Y. Chang, and C.-L. Wang. Green technologies for wireless communications and mobile computing. *Communications, IET*, 5:2595–2597, 12 2011.

[10] D. Chu. Polyphase codes with good periodic correlation properties (corresp.). *IEEE Transactions on information theory*, 18(4):531–532, 1972.

[11] H. Chung and P. V. Kumar. A new general construction for generalized bent functions. *IEEE Transactions on Information Theory*, 35(1):206–209, Jan 1989.

[12] X. Deng and P. Fan. Spreading sequence sets with zero correlation zone. *Electronics Letters*, 36(11):1, 2000.

[13] J. F. Dillon. New p-ary perfect sequences and difference sets with Singer parameters. In T. Helleseth, P. V. Kumar, and K. Yang, editors, *Sequences and their Applications*, pages 23–33, London, 2002. Springer London.

[14] P. Fan and M. Darnell . Sequence design for communications applications. *Communications Systems, Techniques, and Applications Series. J. Wiley, New York*, 1996.

[15] P. Fan, W. Yuan, and Y. Tu. Z-complementary binary sequences. *IEEE Signal Processing Letters*, 14(8):509–512, 2007.

[16] P. Z. Fan and M. Darnell. The synthesis of perfect sequences. In C. Boyd, editor, *Cryptography and Coding*, pages 63–73, Berlin, Heidelberg, 1995. Springer Berlin Heidelberg.

[17] P. Z. Fan, N. Suehiro, N. Kuroyanagi, and X. M. Deng. A class of binary sequences with zero correlation zone. *IEE Electtron. Lett.*, 35(10):777–779, 1999.

[18] R. Frank. Comments on "polyphase codes with good periodic correlation properties" by Chu, David C. *IEEE Transactions on Information Theory*, 19(2):244–244, 1973.

[19] R. Frank and S. Zadoff. Phase shift pulse codes with good periodic correlation properties (corresp.). *IRE Transactions on Information Theory*, 8(6):381–382, 1962.

[20] E. M. Gabidulin. Non-binary sequences with the perfect periodic auto-correlation and with optimal periodic cross-correlation. In *Proceedings. IEEE International Symposium on Information Theory*, pages 412–412, 1993.

[21] E. M. Gabidulin. Partial classification of sequences with perfect autocorrelation and bent functions. In *Proc. IEEE International Symposium on Information Theory (ISIT), Whistler*, page 467, 1995.

[22] E. M. Gabidulin and V. V. Shorin. New sequences with zero autocorrelation. *Probl. Inf. Transm.*, 38(4):255–267, Oct. 2002.

[23] E. M. Gabidulin and V. V. Shorin. Unimodular perfect sequences of length p^s. *IEEE Transactions on Information Theory*, 51(3):1163–1166, 2005.

[24] G. Garg, T. Helleseth, and P. V. Kumar. *Recent Advances in Low-Correlation Sequences*, pages 63–92. Springer US, Boston, MA, 2009.

[25] B. Getz and N. Levanon. Weight effects on the periodic ambiguity function. *IEEE Transactions on Aerospace and Electronic Systems*, 31(1):182–193, 1995.

[26] R. Gold. Optimal binary sequences for spread spectrum multiplexing (corresp.). *IEEE Transactions on Information Theory*, 13(4):619–621, 1967.

[27] S. Golomb and G. Gong. *Signal Design for Good Correlation: for Wireless Communication, Cryptography, and Radar*. Cambridge University Press, 2005.

[28] S. W. Golomb. Two-valued sequences with perfect periodic autocorrelation. *IEEE Transactions on Aerospace and Electronic Systems*, 28(2):383–386, 1992.

[29] B. Gordon, W. H. Mills, and L. R. Welch. Some new difference sets. *Canidian Journal of Mathematics*, 14(4):614–625, 1962.

[30] T. Hayashi. A class of two-dimensional binary sequences with zero-correlation zone. *IEEE Signal Processing Letters*, 9(7):217–221, 2002.

[31] T. Hayashi. Optimal zero-correlation zone sequence set constructed from a perfect sequence. In *7th IEEE International Conference on Computer and Information Technology (CIT 2007)*, pages 475–479, 2007.

[32] T. Hayashi. A class of zero-correlation zone sequence set using a perfect sequence. *IEEE Signal Processing Letters*, 16(4):331–334, April 2009.

[33] T. Hayashi, T. Maeda, S. Kanemoto, and S. Matsufuji. A novel construction of zero-correlation zone sequence set with wide inter-subset zero-correlation zone. In *Proceedings of the Fifth International Workshop on Signal Design and Its Applications in Communications*, pages 25–28, Oct 2011.

[34] T. Hayashi and S. Matsufuji. A generalized construction of optimal zero-correlation zone sequence set from a perfect sequence. In *2009 Fourth International Workshop on Signal Design and its Applications in Communications*, pages 24–27, 2009.

[35] R. Heimiller. Phase shift pulse codes with good periodic correlation properties. *IRE Transactions on Information Theory*, 7(4):254–257, 1961.

[36] T. Helleseth. Some results about the cross-correlation function between two maximal linear sequences. *Discrete Mathematics*, 16(3):209 – 232, 1976.

[37] T. Helleseth and Guang Gong. New nonbinary sequences with ideal two-level autocorrelation. *IEEE Transactions on Information Theory*, 48(11):2868–2872, 2002.

[38] T. Helleseth and P. V. Kumar. Sequences with low correlation. *In V. S. Pless and W. C. Huffman, editors, Handbook of Coding Theory, Vol. I, II, chapter 21*, page 1765–1853, 1998.

[39] T. Hoholdt and J. Justesen. Ternary sequences with perfect periodic autocorrelation (corresp.). *IEEE Transactions on Information Theory*, 29(4):597–600, 1983.

[40] H. Hu and G. Gong. New sets of zero or low correlation zone sequences via interleaving techniques. *IEEE Transactions on Information Theory*, 56(4):1702–1713, April 2010.

[41] W. Huffman, J.-L. Kim, and P. Solé. *Concise Encyclopedia of Coding Theory*. Chapman and Hall/CRC, 2021.

[42] V. P. Ipatov. Multiphase sequences spectrums. *Izvestiya VUZ. Radioelektronika (Radioelectronics and Communications systems)*, 22:80–82, 1979.

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

[44] T. Kasami. Weight distribution formula for some class of cyclic codes. *Technical Report No. R-285, Coordinated Science Laboratory, University of Illinois at Urbana- Champaign*, 1996.

[45] D. Kedia, M. Duhan, and S. L. Maskara. Evaluation of correlation properties of orthogonal spreading codes for CDMA wireless mobile communication. In *2010 IEEE 2nd International Advance Computing Conference (IACC)*, pages 325–330, 2010.

[46] E. Krengel. New polyphase perfect sequences with small alpabet. *Electron. Lett.*, 44(17):1013–1014, 2008.

[47] E. I. Krengel. Some constructions of almost-perfect, odd-perfect and perfect polyphase and almost-polyphase sequences. In C. Carlet and A. Pott, editors, *Sequences and Their Applications – SETA 2010*, pages 387–398, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[48] F. F. Kretschmer and K. Gerlach. Low sidelobe radar waveforms derived from orthogonal matrices. *IEEE Transactions on Aerospace and Electronic Systems*, 27(1):92–102, 1991.

[49] P. V. Kumar, R. A. Scholtz, and L. R. Welch. Generalized bent functions and their properties. *Journal of Combinatorial Theory, Series A*, 40(1):90–107, 1985.

[50] C. Lee. Perfect q-ary sequences from multiplicative charactes over GF(p). *Electron. Lett.*, 3628(9):833–835, 1992.

[51] B. Leonard D. *Cyclic Difference Sets*. Springer-Verlag Berlin Heidelberg, 1971.

[52] J. Li, J. Fan, and X. Tang. A generic construction of generalized chirp-like sequence sets with optimal zero correlation property. *IEEE Communications Letters*, 17(3):549–552, 2013.

[53] Y. B. Li, C. Q. Xu, and K. Liu. Construction of mutually orthogonal zero correlation zone polyphase sequence sets. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E94-A(4):1159–1164, 2011.

[54] Y. Liu and P. Fan. Modified Chu sequences with smaller alphabet size. *Electron. Lett.*, 40(10):598–599, 2004.

[55] Y.-C. Liu, C.-W. Chen, and Y. T. Su. New constructions of zero-correlation zone sequences. *IEEE Transactions on Information Theory*, 59(8):4994–5007, 2013.

[56] H. D. Lüke. Sequences and arrays with perfect periodic correlation. *IEEE Transactions on Aerospace and Electronic Systems*, 24(3):287–294, 1988.

[57] H. D. Lüke. BTP transform and perfect sequences with small phase alphabet. *IEEE Transactions on Aerospace and Electronic Systems*, 32(1):497–499, 1996.

[58] H. D. Lüke, H. D. Schotten, and H. Hadinejad-Mahram. Generalised sidelnikov sequences with optimal autocorrelation properties. *Electron. Lett.*, 36(6):525–527, 2000.

[59] H. D. Lüke, H. D. Schotten, and H. Hadinejad-Mahram. Binary and quadriphase sequences with optimal autocorrelation properties: a survey. *IEEE Trans. Inform. Theory*, 49(12):3271–3282, 2003.

[60] C. Ma, T. S. Yeo, C. S. Tan, and Z. Liu. Three-dimensional imaging of targets using colocated mimo radar. *IEEE Transactions on Geoscience and Remote Sensing*, 49(8):3009–3021, 2011.

[61] S. L. Ma and W. S. Ng. On non-existence of perfect and nearly perfect sequences. *Int. J. Inf. Coding Theory*, 1(1):15–38, Mar. 2009.

[62] S. Matsufuji, N. Kuroyanagi, N. Suehiro, and P. Fan. Two types of polyphase sequence sets for approximately synchronized CDMA systems. *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, E86A:229–234, 01 2003.

[63] T. Matsumoto, Y. Suwaki, and S. Matsufuji. Experimental evaluation of parallel transmission using optical ZCZ-CDMA system. In *2009 Fourth International Workshop on Signal Design and its Applications in Communications*, pages 118–121, 2009.

[64] T. McGree. Signal sets with optimal correlation properties. *IEEE Transactions on Communications*, 31(9):1109–1112, 1983.

[65] A. Milewski. Periodic sequences with optimal properties for channel estimation and fast start-up equalization. *IBM Journal of Research and Development*, 27(5):426–431, Sep. 1983.

[66] W. H. Mow. *Sequence Design for Spread Spectrum*. The Chinese University Press (Chinese University of Hong Kong, Shatin, Hong Kong), 1995.

[67] W. H. Mow. A new unified construction of perfect root-of-unity sequences. In *Proceedings of ISSSTA'95 International Symposium on Spread Spectrum Techniques and Applications*, volume 3, pages 955–959, 1996.

[68] Y. Niho. Multi-valued cross-correlation functions between two maximal linear recursive sequences. *PhD Thesis, University of California*, 1972.

[69] J. Olsen, R. Scholtz, and L. Welch. Bent-function sequences. *IEEE Transactions on Information Theory*, 28(6):858–864, 1982.

[70] K. Park, H. Song, D. S. Kim, and S. W. Golomb. Optimal families of perfect polyphase sequences from the array structure of fermat-quotient sequences. *IEEE Transactions on Information Theory*, 62(2):1076–1086, Feb 2016.

[71] R. A. Pitaval, B. M. Popović, P. Wang, and F. Berggren. Overcoming 5G PRACH capacity shortfall: Supersets of Zadoff–Chu sequences with low-correlation zone. *IEEE Transactions on Communications*, 68(9):5673–5688, 2020.

[72] B. M. Popovic and O. Mauritz. Generalized chirp-like sequences with zero correlation zone. *IEEE Transactions on Information Theory*, 56(6):2957–2960, 2010.

[73] B. M. Popović. Generalized chirp-like polyphase sequences with optimum correlation properties. *IEEE Transactions on Information Theory*, 38(4):1406–1409, July 1992.

[74] B. M. Popović. Optimum sets of interference-free sequences with zero autocorrelation zones. *IEEE Transactions on Information Theory*, 64(4):2876–2882, April 2018.

[75] A. Pott and S. P. Bradley. Existence and nonexistence of almost-perfect autocorrelation sequences. *IEEE Transactions on Information Theory*, 41(1):301–304, 1995.

[76] F. Qu, L. Yang, and T. C. Yang. High reliability direct-sequence spread spectrum for underwater acoustic communications. In *OCEANS 2009*, pages 1–6, 2009.

[77] K. Rajawat and A. K. Chaturvedi. Near optimal training sequences for low complexity symbol timing estimation in mimo systems. *IEEE Transactions on Communications*, 58(1):281–288, 2010.

[78] T. S. Rappaport. Wireless communications - principles and practice. 1996.

[79] D. Sarwate. Bounds on crosscorrelation and autocorrelation of sequences (corresp.). *IEEE Transactions on Information Theory*, 25(6):720–724, 1979.

[80] R. A. Scholtz and L. Welch. Group characters: sequences with good correlation properties. *IEEE Transactions on Information theory*, IT-24:79–84, 1978.

[81] S. Sesia, I. Toufik, and M. Baker. *LTE - The UMTS Long Term Evolution: From Theory to Practice: Second Edition*. 2011.

[82] D. Shedd and D. V. Sarwate. Construction of sequences with good correlation properties (corresp.). *IEEE Transactions on Information Theory*, 25(1):94–97, 1979.

[83] V. M. Sidelnikov. On mutual correlation of sequences. *Soviet Math. Dokl*, 12:197–201, 1971.

[84] M. K. Simon, J. k. Omura, R. A. Scholtz, and B. K. Levitt. *Spread Spectrum Communications Handbook*. McGraw-Hill, New York, NY, USA: McGraw-Hill, 2002.

[85] M. Soltanalian and P. Stoica. On prime root-of-unity sequences with perfect periodic correlation. *IEEE Transactions on Signal Processing*, 62(20):5458–5470, 2014.

[86] M. K. Song and H. Song. A construction of odd length generators for optimal families of perfect sequences. *IEEE Transactions on Information Theory*, 64(4):2901–2909, April 2018.

[87] S. Stanczak, H. Boche, and M. Haardt. Are LAS-codes a miracle ? In *GLOBECOM'01. IEEE Global Telecommunications Conference (Cat. No.01CH37270)*, volume 1, pages 589–593 vol.1, 2001.

[88] N. Suehiro. A signal design without co-channel interference for approximately synchronized CDMA systems. *IEEE Journal on Selected Areas in Communications*, 12(5):837–841, 1994.

[89] N. Suehiro and M. Hatori. Modulatable orthogonal sequences and their application to SSMA systems. *IEEE Transactions on Information Theory*, 34(1):93–100, Jan 1988.

[90] X. Tang, P. Fan, and J. Lindner. Multiple binary ZCZ sequence sets with good cross-correlation property based on complementary sequence sets. *IEEE Transactions on Information Theory*, 56(8):4038–4045, 2010.

[91] X. Tang and W. H. Mow. Design of spreading codes for quasi-synchronous CDMA with intercell interference. *IEEE Journal on Selected Areas in Communications*, 24(1):84–93, 2006.

[92] X. Tang and W. H. Mow. A new systematic construction of zero correlation zone sequences based on interleaved perfect sequences. *IEEE Transactions on Information Theory*, 54(12):5729–5734, Dec 2008.

[93] X. H. Tang, P. Z. Fan, and S. Matsufuji. Lower bounds on correlation of spreading sequence set with low or zero correlation zone. *Electronics Letters*, 36(6):551–552, 2000.

[94] H. Torii, T. Matsumoto, and M. Nakamura. A new method for constructing asymmetric ZCZ sequence sets. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 95(9):1577–1586, 2012.

[95] H. Torii, T. Matsumoto, and M. Nakamura. Optimal polyphase asymmetric ZCZ sequence sets including uncorrelated sequences. *Journal of Signal Processing*, 16(6):487–494, 2012.

[96] H. Torii, T. Matsumoto, and M. Nakamura. Extension of methods for constructing polyphase asymmetric ZCZ sequence sets. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E96.A:2244–2252, November 2013.

[97] H. Torii, M. Nakamura, and N. Suehiro. A new class of zero-correlation zone sequences. *IEEE Transactions on Information Theory*, 50(3):559–565, 2004.

[98] H. Torii, M. Nakamura, and N. Suehiro. A new class of polyphase sequence sets with optimal zero-correlation zones. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E88-A(7):1987–1994, 2005.

[99] H. Torii, M. Satoh, T. Matsumoto, and M. Nakamura. New generalised mutually orthogonal ZCZ sequence sets constructed from DFT matrix. In *Recent advances in communications circuits and technological innovation: proceedings of the 3rd European conference of circuits technology and devices (ECCTD '12)*, pages 262–267, 2012.

[100] H. Torii, M. Satoh, T. Matsumoto, and M. Nakamura. Generalized mutually orthogonal ZCZ sequence sets based on perfect sequences and orthogonal codes. In *2013 15th International Conference on Advanced Communications Technology (ICACT)*, pages 894–899, 2013.

[101] L.-S. Tsai and Y. T. Su. Transform domain approach for sequence design and its applications. *IEEE Journal on Selected Areas in Communications*, 24(1):75–83, Jan 2006.

[102] R. Van Schyndel. Using phase-modulated probe signals to recover delays from higher order non-linear systems. In *Biomedical Research in 2001 IEEE Engineering in Medicine and Biology*, pages 94–97, 2001.

[103] L. Wang, X. Zeng, and H. Wen. Asymmetric ZCZ sequence sets with inter-subset uncorrelated sequences via interleaved technique. *IEICE Transactions on*

Fundamentals of Electronics, Communications and Computer Sciences, (2):751–756, 2017.

[104] L. Welch. Lower bounds on the maximum cross correlation of signals (corresp.). *IEEE Transactions on Information Theory*, 20(3):397–399, 1974.

[105] J. Wolfmann. Almost perfect autocorrelation sequences. *IEEE Transactions on Information Theory*, 38(4):1412–1418, 1992.

[106] D. Wu, P. Spasojevic, and I. Seskar. Orthogonal variable spreading factor codes with zero-correlation zone for TS-UWB. In *IEEE Wireless Communications and Networking Conference, 2005*, volume 2, pages 807–812 Vol. 2, 2005.

[107] Y. Xia, C. Li, X. Zeng, and T. Helleseth. Some results on cross-correlation distribution between a p-ary m-sequence and its decimated sequences. *IEEE Transactions on Information Theory*, 60(11):7368–7381, 2014.

[108] L. Xu, Q. Liang, X. Wu, and B. Zhang. Phase coded waveform design for sonar sensor network. In *2011 6th International ICST Conference on Communications and Networking in China (CHINACOM)*, pages 251–256, 2011.

[109] Z. Zhang, F. Zeng, and G. Xuan. Mutually orthogonal sets of complementary sequences for multi-carrier CDMA systems. 09 2010.

[110] Z. Zhou, X. Tang, and G. Gong. A new class of sequences with zero or low correlation zone based on interleaving technique. *IEEE Transactions on Information Theory*, 54(9):4267–4273, Sep. 2008.

Chapter 3

Scientific results

Paper I

3.1 New optimal sets of perfect polyphase sequences based on circular Florentine arrays

Dan Zhang and Tor Helleseth
IEEE International Symposium on Information Theory (ISIT), Los Angeles, CA, USA, pp. 2921-2925 (2020)

New Optimal Sets of Perfect Polyphase Sequences Based on Circular Florentine Arrays

Dan Zhang
email: dan.zhang@uib.no

Tor Helleseth
email: tor.helleseth@uib.no

Abstract

Families of periodic sequences with some desirable auto-correlation and crosscorrelation properties have applications in communications and radar systems for identification, synchronization, ranging, or interference mitigation. A sequence is said to be *a polyphase sequence* if all the coordinates are n-th roots of unity. In this paper, we develop a connection between generalised Frank sequences and well-studied combinatorial objects: circular Florentine arrays. From this connection, we can derive an optimal set of perfect polyphase sequences with respect to the Sarvate bound. Furthermore, the size of the optimal set is determined by the existence of circular Florentine arrays. As a result, the size of an optimal set of perfect sequences is increased, compared with the previous results, where the size depends on the smallest prime divisor of the period.

1 Introduction

The periodic *cross-correlation* value of two complex sequences $\mathbf{u} = \{u(t)\}_{t=0}^{N-1}$ and $\mathbf{v} = \{v(t)\}_{t=0}^{N-1}$ of period N at shift τ is defined as

$$R_{\mathbf{u},\mathbf{v}}(\tau) = \sum_{t=0}^{N-1} u(t+\tau)v^*(t), \quad 0 \le \tau < N,$$

where $t+\tau$ is taken modulo N and $v^*(t)$ is the complex conjugate of the complex number $v(t)$. When two sequences $\mathbf{u}$ and $\mathbf{v}$ are identical, the periodic cross-correlation function is called *auto-correlation* function, and is denoted by $R_{\mathbf{u}}(\tau)$. Sequences with good periodic auto-correlation have been widely used in digital communication systems and pulse compression radars [1, 2]. In many cases, sequences having small (preferably zero) out-of-phase auto-correlation magnitude are required. In particular, a sequence is said to be *perfect* if all the out-of-phase periodic auto-correlation coefficients are zero, i.e., $R_{\mathbf{u}}(\tau) = 0$ for $\tau \not\equiv 0 \mod N$. There is so far only one example of a binary perfect sequence of period four [1].

Spread spectrum multiple access systems also demand minimum possible cross-correlation between the sequences within a set of sequences having good auto-correlation properties. Let $\mathcal{S}$ be a set of M sequences of period N. The maximum out-of-phase periodic auto-correlation magnitude is denoted by R_a and defined by $R_a = \max\{|R_{\mathbf{s}_i}(\tau)| : \mathbf{s}_i \in \mathcal{S}, 0 < \tau < N\}$. The maximum periodic cross-correlation magnitude is denoted by R_c and defined by $R_c = \max\{|R_{\mathbf{s}_i,\mathbf{s}_j}(\tau)| : \mathbf{s}_i \neq \mathbf{s}_j \in \mathcal{S}, 0 \le \tau < N\}$. Sarwate [3] showed that R_a and R_c are related through the inequality

$$\frac{R_c^2}{N} + \frac{N-1}{N(M-1)}\frac{R_a^2}{N} \ge 1,$$

Table 1: Optimal sets of perfect polyphase sequences

References	[3] [4]	[5]	[6]	[7]	[8]	[9]	this paper	[10]
Class of perfect sequences	Generalized chirp-like sequences		Generalised Frank sequences					Unified
Period of perfect sequences	N	sm^2	N^2	$N = Q^2$	$N = Q^2$	N^2	N^2	sm^2
Size of optimal set	$p-1$	$p-1$	$(p-1)/2$	$Q-1$	$Q-1$	$p-1$	$F_c(N)$	$p-1$

N is an odd integer; p is the smallest prime divisor of the period; Q is an odd prime; s is a square-free integer; m is a positive integer; $F_c(N)$ is the maximum number such that an $F_c(N) \times N$ circular Florentine array exists.

which provides a lower bound on one of the maxima if the value of the other is specified. When R_a is zero, i.e., all the sequences in $\mathcal{S}$ are perfect, the lower bound on R_c is equal to $\sqrt{N}$. A set of perfect sequences meeting this bound is called *an optimal set of perfect sequences*. We can see that M vanishes if R_a is zero, thus, the inequality no longer depends on M. Therefore, there are no bounds on the size of an optimal set of perfect sequences. In this paper, we are interested in how large the size of an optimal set of perfect sequences can be. Many constructions of optimal sets based on the known perfect sequences have been investigated.

In [4] and [3], Frank-Zadoff-Chu sequences of odd period were employed to get an optimal set of $p-1$ perfect sequences, where p is the smallest prime divisor of the period. Popović [5] presented an optimal set of $p-1$ generalized chirp-like sequences. Alltop [6] obtained optimal sets from $(p-1)/2$ decimations of the Frank-Heimiller sequences of period N^2, where N is an odd integer. Suehiro and Hatori [7] proposed an optimal set of $N-1$ modulatable orthogonal sequences of period N^2, where N is a prime number. Mow [10] classified all the known perfect polyphase sequences into four classes: I) Generalised Frank sequences [11], II) Generalized chirp-like polyphase sequences [5], III) Milewski sequences [12], and IV) perfect polyphase sequences associated with the general construction of generalised bent function [13]. Furthermore, Mow [10] proposed a unified construction of perfect polyphase sequences, which included all the perfect sequences mentioned above as special cases. Thus, an optimal set of size $p-1$ from the unified construction was derived.

Park et al. recently presented perfect polyphase sequences based on generators and array structures [8], which are essentially special cases of generalised Frank sequences. When a generator of length N is a permutation over $\mathbb{Z}_N$, the associated family is a set of perfect sequences of period N^2, where N is an odd prime. This is equivalent to the requirements in Theorem 3 [11] that π is a permutation over $\mathbb{Z}_N$ and g is any function on $\mathbb{Z}_N$. Each optimal generator can induce an optimal set of $N-1$ perfect sequences. This result was later extended to the case of odd N and an optimal set of $p-1$ perfect sequences of period N^2 were derived [9].

We can see that the sizes of the optimal sets are all based on the smallest prime divisor of the period according to all papers mentioned above. The size of an optimal set is at most $p-1$, where p is the smallest prime divisor of the period (see table I). In this paper, we present a construction of optimal sets based on generalised Frank sequences and cyclic Florentine arrays, where the size of an optimal set is determined by the existence of cyclic Florentine arrays. As a result, the size of an optimal set is improved compared with the known results.

The rest of the paper is organised as follows. Section II gives an introduction to cyclic Florentine arrays. We build a connection between circular Florentine arrays and generalised Frank sequences in Section III. A construction of optimal sets of perfect sequences is derived consequently. Section IV concludes this paper.

2 Preliminaries

An $m \times n$ *Tuscan-k array* has m rows and n columns such that 1) each row is a permutation of n symbols and 2) for any two symbols a and b, and for each t from 1 to k, there is at most one row in which b is the t-th symbol to the right of a. In particular, a Tuscan-$(n-1)$ array is referred to as a Florentine array. If it is also a Latin square, we may call it a Vatican square. We call an $n \times n$ square a *Latin square* if its rows and columns are all permutations of n symbols.

An $m \times n$ *circular Florentine array* is an array of n distinct symbols in m circular rows such that each row contains every symbol exactly once and that for any pair of distinct symbols and for each t from 1 to $n-1$ there is at most one row in which b occurs t steps (circularly) to the right of a. By definition, an $m \times n$ circular Florentine array is an array in which the Tuscan-$(n-1)$ property holds when the rows are taken to be circular. See Table II for an example of a 4×15 circular Florentine array. For each positive integer $n \geq 2$, we denote $F_c(n)$ the maximum number such that an $F_c(n) \times n$ circular Florentine array exists.

Lemma 1. *(1)* $F_c(n) = 1$ *when n is even [14], and*

(2) $p - 1 \leq F_c(n) \leq n - 1$, *where p is the smallest prime factor of n [15], and*

(3) $F_c(n) = n - 1$ *when n is a prime [15], and*

(4) $F_c(n) \leq n - 3$ *when* $n \equiv 15 \mod 18$ *[15].*

Circular Florentine arrays are connected to other combinatorial objects. For example, an $m \times n$ circular Florentine array is equivalent to an $(n, m+1; 1)$ difference matrix [16]. Moreover, circular Florentine arrays are also related with a set of Mutually Orthogonal Latin Squares (MOLS) having an additional property.

Lemma 2. *[15] There exists a circular Florentine array of size* $m \times n$ *if and only if there exists a set of m mutually orthogonal Latin squares of order n such that the rows of any squares are cyclic shifts of each other and that every square is obtainable from any other only by permuting the rows.*

Table 2: A 4×15 circular Florentine array

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	7	1	8	2	12	3	11	9	4	13	5	14	6	10
0	4	11	7	10	1	13	9	5	8	3	6	2	14	12
0	13	7	2	11	6	14	10	3	5	12	9	1	4	8

Table 3: Possible values of $F_c(n)$ for odd composite n [15]

n	$F_c(n)$	n	$F_c(n)$	n	$F_c(n)$
9	2	35	$4, \cdots, 33$	57	$7, \cdots, 55$
15	4	39	$3, \cdots, 38$	63	$6, \cdots, 62$
21	$5, \cdots, 19$	45	$2, \cdots, 43$	65	$4, \cdots, 63$
25	$4, \cdots, 24$	49	$6, \cdots, 48$	69	$2, \cdots, 66$
27	$4, \cdots, 26$	51	$2, \cdots, 48$	75	$2, \cdots, 73$
33	$3, \cdots, 30$	55	$4, \cdots, 54$	77	$6, \cdots, 75$

The basic lower bound on $F_c(n)$ is $p-1$, where p is the smallest prime factor of n, which can be improved by Lemma 2 and known constructions of MOLS with the desirable property in [17–19] (see Table III). For example, $F_c(21) \geq 5$, $F_c(33) \geq 3$, $F_c(39) \geq 3$, $F_c(57) \geq 7$, and $F_c(63) \geq 6$. In this paper, we are interested in the bounds on $F_c(n)$, because they determine how large an optimal set of perfect sequences can be in the next section. The following lemma will help to build a connection between a circular Florentine array and an optimal set of perfect sequences.

Let A be an $m \times n$ circular Florentine array on $\mathbb{Z}_n$. In matrix notation, the rows are indexed as 0 to $m-1$ while the columns are indexed as 0 to $n-1$ mod n. According to the definition, each row, denoted by π_i for $0 \leq i \leq m-1$, is a permutation of $\mathbb{Z}_n$. And for each l from 1 to $n-1$, $(A(i,j), A(i,j+l)) \neq (A(r,k), A(r,k+l))$ unless $i = r$ and $j = k$, where $0 \leq i, r \leq m-1$ and $0 \leq j, k \leq n-1$. In other words, for each $l \not\equiv 0 \bmod n$, $(\pi_i(j), \pi_i(j+l)) = (\pi_r(k), \pi_r(k+l))$ if and only if $i = r$ and $j = k$.

Lemma 3. *For $0 \leq i \neq r \leq m-1$, $\pi_i(t) = \pi_r(t+l')$ only has one solution for each $0 \leq l' \leq n-1$.*

Proof. Assume that on the contrary, there exists l' such that $\pi_i(t) = \pi_r(t+l')$ has two or more than two solutions. Let t_1 and t_2 be two of the solutions. Then we have $\pi_i(t_1) = \pi_r(t_1 + l')$ and $\pi_i(t_2) = \pi_r(t_2 + l')$. As a consequence, $(\pi_i(t_1), \pi_i(t_2)) = (\pi_r(t_1 + l'), \pi_r(t_2 + l'))$, which contradicts the definition of the circular Florentine array. Hence, $\pi_i(t) = \pi_r(t + l')$ only has one solution for each $0 \leq l' \leq n-1$ for $0 \leq i \neq r \leq m-1$. □

3 Optimal set of perfect sequences

In this section, we develop a connection between generalised Frank sequences and circular Florentine arrays. From this connection, we can generate an optimal set of $F_c(N)$ perfect sequences of period N^2, where N is any positive integer and $F_c(N)$ is the maximum number such that an $F_c(N) \times N$ circular Florentine array exists. We first give a brief introduction to generalised Frank sequences before giving the main construction.

Generalized Frank sequences constitute a class of perfect polyphase sequences which are from one-dimensional bent function and were proposed by Kumar, Scholtz and Welch in [11].

Lemma 4. *[11] Let N be a positive integer and ω_N be a primitive N-th root of unity. Let*

(i) π be a permutation of elements in $\mathbb{Z}_N$ and let

(ii) σ be an arbitrary function from $\mathbb{Z}_N$ to $\mathbb{Z}_{N^2}$.

Then $s(t) = \omega_{N^2}^{N \cdot t_2 \pi(t_1) + \sigma(t_1)}$ where $t = t_1 + N \cdot t_2$, $0 \leq t_1, t_2 < N$, is a perfect sequence of period N^2.

The sequences in Lemma 4 were first discovered by Frank and Zadoff [20] in the case $\sigma = 0$ and π being the identity permutation. Heimiller [21] found the sequences $\omega_{N^2}^{N \cdot \pi(t_1)(t_2 + h(t_1))}$ for the case of prime N, where h is also an arbitrary function on $\mathbb{Z}_N$. Lemma 4 is a more general construction.

By Lemma 4, there are in total $N!N^{2m}$ perfect sequences of period N^2. In order to generate an optimal set from these sequences, the maximum cross-correlation magnitude of any two distinct sequences should be N. In the following, we give a construction of optimal sets and prove that the cross-correlation functions between any two distinct sequences have constant magnitude N.

Let N be a positive integer. Let A be an $m \times N$ circular Florentine array. For convenience, the set of permutations from the rows of A is denoted by Π, i.e., $\Pi = \{\pi_0, \pi_1, \cdots \pi_{m-1}\}$. A set of sequences of period N^2 is defined as

$$\mathcal{S} = \{\mathbf{s}_i \mid \mathbf{s}_i(t) = \omega_{N^2}^{N\cdot\pi_i(t_1)t_2+\sigma(t_1)}, 0 \le i \le m-1\},$$

where $t = t_1 + t_2 \cdot N$, $0 \le t_1, t_2 < N$, $\pi_i \in \Pi$ for $0 \le i \le m-1$, and σ is an arbitrary function from $\mathbb{Z}_N$ to $\mathbb{Z}_{N^2}$.

Theorem 1. *The set $\mathcal{S}$ is an optimal set of perfect sequences.*

Proof. Since each $\pi_i(t_1)$ is a permutation over $\mathbb{Z}_N$, each sequence in $\mathcal{S}$ is perfect by Lemma 4. For any shift $0 \le \tau < N^2$, we rewrite $\tau = \tau_1 + \tau_2 \cdot N$, where $0 \le \tau_1, \tau_2 < N$, and define

$$\delta_{t_1,\tau_1} = \begin{cases} 0 & \text{if } t_1 + \tau_1 < N, \\ 1 & \text{if } t_1 + \tau_1 \ge N. \end{cases}$$

Let $\mathbf{s}_i$ and $\mathbf{s}_r$ be two sequences in $\mathcal{S}$, where $0 \le i \ne r \le m-1$. Then the cross-correlation between $\mathbf{s}_i$ and $\mathbf{s}_r$ is given by

$$\begin{aligned} R_{\mathbf{s}_i,\mathbf{s}_r}(\tau) &= \sum_{t=0}^{N^2-1} s_i(t+\tau){s_r}^*(t) \\ &= \sum_{t_2=0}^{N-1}\sum_{t_1=0}^{N-1} \omega_{N^2}^{N\cdot\pi_i(t_1+\tau_1)(t_2+\tau_2+\delta_{t_1,\tau_1})+\sigma(t_1+\tau_1)} \cdot \omega_{N^2}^{-(N\cdot\pi_r(t_1)t_2+\sigma(t_1))} \\ &= \sum_{t_1=0}^{N-1} \omega_{N^2}^{N\cdot\pi_i(t_1+\tau_1)(\tau_2+\delta_{t_1,\tau_1})+\sigma(t_1+\tau_1)-\sigma(t_1)} \cdot \sum_{t_2=0}^{N-1} \omega_N^{(\pi_i(t_1+\tau_1)-\pi_r(t_1))t_2}. \end{aligned} \tag{1}$$

The inner sum of the last identity above is zero unless

$$\pi_i(t_1 + \tau_1) \equiv \pi_r(t_1) \mod N.$$

By Lemma 3, the above equation has a unique solution for any shift $\tau_1 \in \mathbb{Z}_N$ and $i \ne r$. Therefore, we have $|R_{\mathbf{s}_i,\mathbf{s}_r}(\tau)| = N$ for all $0 \le \tau < N^2 - 1$. □

We give an example to illustrate Theorem 1 before some remarks to conclude this section.

Example 1. *Let $N = 15$ and a 4×15 circular Florentine array is provided in Table II. The permutation set from the rows of the circular Florentine array is denoted by $\Pi = \{\pi_0, \pi_1, \pi_2, \pi_3\}$. For simplicity, let $\sigma = 0$. Then a set of sequences of period 225 is defined as*

$$\mathcal{S} = \{\mathbf{s}_i \mid \mathbf{s}_i(t) = \omega_{15}^{\pi_i(t_1)t_2}, 0 \le i \le 3\},$$

where $t = t_1 + t_2 \cdot 15$, $0 \le t_1, t_2 < 15$, $\pi_i \in \Pi$ for $0 \le i \le 3$. It is verifiable that

- *each sequence is perfect; and*
- *$|R_{\mathbf{s}_i,\mathbf{s}_r}(\tau)| = 15$ for any $0 \le \tau \le 224$, $0 \le i \ne r \le 3$,*

which are consistent with Theorem 1.

Given an $m \times N$ circular Florentine array, we can get an optimal set of size m from generalised Frank sequences of period N^2 by Theorem 1. As mentioned in the introduction, the size of all the previous optimal sets is at most $p - 1$, where p is the smallest divisor of the period of the sequences. Table IV gives a comparison between the smallest divisor of some N and $F_c(N)$, where $F_c(N)$ is the maximum number such that an $F_c(N) \times n$ circular Florentine array exists. Thus, we can see that the size of an optimal set is increased by the construction in this paper.

Table 4: Comparison of $F_c(N)$ and $p-1$

N	$F_c(N)$	$p-1$	N	$F_c(N)$	$p-1$
15	4	2	21	$5, \cdots, 19$	2
27	$4, \cdots, 26$	2	33	$3, \cdots, 30$	2
39	$3, \cdots, 38$	2	57	$7, \cdots, 55$	2
63	$6, \cdots, 62$	2	$\cdots$		

4 Conclusion

In this paper, we built a connection between the generalised Frank sequences and circular Florentine arrays. We derived optimal sets of $F_c(N)$ perfect sequences of period N^2, where $F_c(N)$ is the maximum number such that an $F_c(N) \times N$ circular Florentine array exists. The general lower bound on $F_c(N)$ is $p-1$, where p is the smallest prime divisor of N. But in many cases, the lower bound on $F_c(N)$ is improved by Lemma 2 (see Table IV). Therefore, we improved the size of an optimal set of perfect polyphase sequences, compared with previous research papers, where the size is at most $p-1$.

Acknowledgment

Tor Helleseth was in part supported by the Research Council of Norway under Grant 247742/O70.

References

[1] P. Fan, "Sequence design for communications applications," Taunton, 1996.

[2] S. W. Golomb and G. Gong, *Signal Designs With Good Correlation: For Wireless Communications, Cryptography and Radar Applications*. Cambridge University Press, 2005.

[3] D. Sarwate, "Bounds on crosscorrelation and autocorrelation of sequences (corresp.)," *IEEE Transactions on Information Theory*, vol. 25, no. 6, pp. 720–724, November 1979.

[4] W. Alltop, "Complex sequences with low periodic correlations (corresp.)," *IEEE Transactions on Information Theory*, vol. 26, no. 3, pp. 350–354, May 1980.

[5] B. M. Popović, "Generalized chirp-like polyphase sequences with optimum correlation properties," *IEEE Transactions on Information Theory*, vol. 38, no. 4, pp. 1406–1409, July 1992.

[6] W. Alltop, "Decimations of the Frank-Heimiller sequences," *IEEE Transactions on Communications*, vol. 32, no. 7, pp. 851–853, July 1984.

[7] N. Suehiro and M. Hatori, "Modulatable orthogonal sequences and their application to SSMA systems," *IEEE Transactions on Information Theory*, vol. 34, no. 1, pp. 93–100, Jan 1988.

[8] K. Park, H. Song, D. S. Kim, and S. W. Golomb, "Optimal families of perfect polyphase sequences from the array structure of Fermat-Quotient sequences," *IEEE Transactions on Information Theory*, vol. 62, no. 2, pp. 1076–1086, Feb 2016.

[9] M. K. Song and H. Song, "A construction of odd length generators for optimal families of perfect sequences," *IEEE Transactions on Information Theory*, vol. 64, no. 4, pp. 2901–2909, April 2018.

[10] W. H. Mow, "A new unified construction of perfect root-of-unity sequences," in *Proceedings of ISSSTA'95 International Symposium on Spread Spectrum Techniques and Applications*, vol. 3, 1996, pp. 955–959.

[11] P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized bent functions and their properties," *Journal of Combinatorial Theory, Series A*, vol. 40, no. 1, pp. 90–107, 1985.

[12] A. Milewski, "Periodic sequences with optimal properties for channel estimation and fast start-up equalization," *IBM Journal of Research and Development*, vol. 27, no. 5, pp. 426–431, Sep. 1983.

[13] H. Chung and P. V. Kumar, "A new general construction for generalized bent functions," *IEEE Transactions on Information Theory*, vol. 35, no. 1, pp. 206–209, Jan 1989.

[14] S. Golomb, T. Etzion, and H. Taylor, "Polygonal path constructions for tuscan-k squares," *Ars Combinatoria*, vol. 30, pp. 97–140, 1990.

[15] H.-Y. Song, "The existence of circular florentine arrays," *Computers & Mathematics with Applications*, vol. 39, no. 11, pp. 31 – 35, 2000.

[16] H. Y. Song, "On aspects of tuscan squres," *PhD thesis, University of Southern California*, 1991.

[17] P. J. Schellenberg, G. J. Van Rees, and S. A. Vanstone, "Four pairwise orthogonal latin squares of order 15," *Ars Combinatoria*, vol. 6, pp. 141–150, 1978.

[18] D. Jungnickel, "On difference matrices and regular latin squares," 1980.

[19] A. Nazarok, "Five pairwise orthogonal latin squares of order 21," *Issled. oper. i ASU*, vol. 54, 1991.

[20] R. L. Frank and S. Zadoff, "Phase shift pulse codes with good periodic correlation properties," *IRE Trans. Inform. Theory*, vol. 8, no. 6, pp. 381–382, 1962.

[21] R. Heimiller, "Phase shift pulse codes with good periodic correlation properties," *IRE Transactions on Information Theory*, vol. 7, no. 4, pp. 254–257, 1961.

Paper II

3.2 Sequences with good correlations based on circular Florentine arrays

Dan Zhang and Tor Helleseth
IEEE Transactions on Information Theory, (submitted, 2020)

Paper III

3.3 Zero correlation zone sequences from a unified construction of perfect polyphase sequences

Dan Zhang
IEEE International Symposium on Information Theory (ISIT), Paris, France, pp. 2269-2273 (2019)

Zero Correlation Zone Sequences from a Unified Construction of Perfect Polyphase Sequences

Dan Zhang
email: dan.zhang@uib.no

Abstract

Sequence families with Zero Correlation Zone (ZCZ) can be used in quasi-synchronous code-division multiple-access (QS-CDMA) communication systems. This paper proposes two methods for constructing polyphase ZCZ sequence sets by using a unified construction of perfect polyphase sequences. The first method generates sets of perfect sequences with zero cross-correlation zone, i.e., sets such that the out-of-phase autocorrelation of each sequence is zero and the cross-correlation of any two sequences in a set is zero in some zone around the origin. The second method produces sets of so-called interference-free sequences with zero autocorrelation zone, i.e., sets such that the cross-correlation of any two sequences in a set is zero at any shift and the autocorrelation of each sequence is zero in some zone around the origin. Moreover, each generated ZCZ sequence set is optimal with respect to the Tang-Fan-Matsufuji bound.

1 Introduction

Families of periodic sequences with some desirable autocorrelation (AC) and cross-correlation (CC) properties have applications in communications and radar systems for identification, synchronization, ranging, or interference mitigation. For example, to minimize multiple access interference and self-interference in a multiuser and multipath environment, one would like to have an *ideal sequence set*, where the out-of-phase AC of each sequence is zero and the CC of any pair of sequences at any shift is zero. Unfortunately, no such ideal sequence set exists according to the Sawarte bound [17]. It is therefore impossible to have sequences which have simultaneously impulse-like AC and zero CC during an entire period. However, sets of sequences satisfying both of these properties simultaneously in some smaller zone around the origin (called the zero-correlation zone, or ZCZ) do exist. Sequences with such properties are known as ZCZ sequences. They have been extensively studied in recent years due to their important applications in QS-CDMA systems, where a time delay between the signals of different users within a few chips is allowed. ZCZ sequences can eliminate both multiple access interference and multipath interference in such a system [4] [5]. A ZCZ sequence set is generally characterized by the sequence period, the size of the set, the length of the ZCZ and the number of phases of the sequence elements. The Tang-Fan-Matsufuji bound [18] shows there is a tradeoff between the set size and the ZCZ length for any given sequence period. ZCZ sequence sets are said to be optimal if they meet this bound.

A number of studies on constructing ZCZ sequence sets have been reported. The methods presented in [1, 4, 19, 21] are based on complementary sequence sets, while interleaving techniques were proven to be effective in [7, 20, 23, 28]. There were also several constructions

derived by manipulating perfect sequences [8, 11, 16, 23]. ZCZ sequence sets were obtained in [2, 10, 22] using the transform domain method. One special class of ZCZ sequence sets having nonzero AC only at subperiodic correlation shifts and zero CC across all shifts are referred to as interference-free ZCZ sequence sets [2, 13, 16, 22]. Some ZCZ sequence sets can be partitioned into smaller subsets so that the ZCZ length between any two sequences from different subsets is larger than that between sequences from the same subsets. These are referred to as asymmetric ZCZ (A-ZCZ) sequence sets [19, 21, 24, 25].

In this paper, we propose two constructions of polyphase ZCZ sequence sets based on a unified construction of perfect polyphase sequences. The first construction generates sets of perfect sequences with zero cross-correlation zone. The second construction produces sets of interference-free sequences with zero autocorrelation zone. We give some conditions under which all the ZCZ sequences generated by our constructions are cyclically distinct (meaning that one sequence cannot be obtained by taking a cyclic shift of another). Moreover, each generated ZCZ sequence set is optimal with respect to the Tang-Fan-Matsufuji bound. Our construction includes some previous results as special cases [14, 29].

2 Preliminaries

We denote the ring of integers modulo N by $\mathbb{Z}_N$, where N is a positive integer. Let $\mathbf{u} = \{u(t)\}_{t=0}^{N-1}$ and $\mathbf{v} = \{v(t)\}_{t=0}^{N-1}$ be two complex sequences of period N. The (periodic) *cross-correlation* (CC) of $\mathbf{u}$ and $\mathbf{v}$ at shift τ is defined as

$$R_{\mathbf{u},\mathbf{v}}(\tau) = \sum_{t=0}^{N-1} u(t+\tau)v^*(t), \quad 0 \le \tau < N,$$

where $t + \tau$ is reduced modulo N and x^* is the complex conjugate of the complex number x. When $\mathbf{u} = \mathbf{v}$, then $R_{\mathbf{u},\mathbf{u}}(\tau)$ is called the *auto-correlation* (AC) of $\mathbf{u}$. In this case, we write $R_{\mathbf{u}}(\tau) = R_{\mathbf{u},\mathbf{u}}(\tau)$ for short. A sequence $\mathbf{u}$ is said to be *perfect* if $R_{\mathbf{u}}(\tau) = 0$ for all $0 < \tau < N$.

Consider a sequence set $\mathcal{S}$ of size M of period N. The set $\mathcal{S}$ is called *periodically uncorrelated* if the correlation between any two distinct sequences in $\mathcal{S}$ at any shift is zero, i.e.,

$$R_{\mathbf{u},\mathbf{v}}(\tau) = 0, \forall \tau \in \mathbb{Z}_N, \forall \mathbf{u}, \mathbf{v} \in \mathcal{S} \text{ with } \mathbf{u} \neq \mathbf{v}.$$

The set $\mathcal{S}$ is called *periodically complementary* if the sum of all ACs of sequences in $\mathcal{S}$ at the same nonzero shift is zero, specifically,

$$\sum_{\mathbf{u}\in\mathcal{S}} R_{\mathbf{u}}(\tau) = 0, \forall \tau \in \mathbb{Z}_N \text{ with } \tau \neq 0.$$

Definition 1. *Let $\mathcal{S} = \{\mathbf{s}_m = \{s_m(t)\}_{t=0}^{N-1},\ 0 \le m < M\}$ be a set of M sequences of period N. The set $\mathcal{S}$ is called an (N, M, Z_{cz})-ZCZ sequence set if*

$$R_{\mathbf{s}_i,\mathbf{s}_j}(\tau) = 0 \text{ for } (0 < |\tau| < Z_{cz})$$

and

$$R_{\mathbf{s}_i,\mathbf{s}_j}(\tau) = 0 \text{ for } (\tau = 0 \text{ and } i \neq j),$$

where Z_{cz} is called the length of the zero correlation zone.

The following lemma shows that Z_{cz} is bounded from above by a value depending on the sequence period and the size of the sequence set. Any sequence set meeting this bound is an *optimal ZCZ set*.

Lemma 1. *[18] Let $\mathcal{S}$ be an (N, M, Z_{cz})-ZCZ sequence set. Then*

$$MZ_{cz} \leq N.$$

A *polyphase sequence* is a sequence whose elements are are all complex roots of unity of the form $exp(i2\pi x)$ where x is a rational number and $i = \sqrt{-1}$. A sequence is perfect if its out-of-phase periodic autocorrelation is always equal to zero. Perfect polyphase sequences have attracted a lot of attention from engineers and researchers for decades due to their applications in spread spectrum systems such as pulse compression radars, DS/SSMA, FH/SSMA, etc. Mow [26] classified all known perfect polyphase sequences into four classes: generalised Frank sequences [9], generalised chirp-like sequences [15], Milewski sequences [12], and perfect polyphase sequences associated with generalised bent functions [3]. Mow also proposed a unified construction of perfect polyphase sequences, which includes all of the four special cases above. Moreover, Mow conjectured that the unified construction describes all the perfect polyphase sequences that exist.

Lemma 2. *[26] For any positive integers r and m with r a square-free integer, let a polyphase sequence* **s** *of period rm^2 be defined by*

$$s(km + l) = \exp(i2\pi f(km + l)/rm)$$

for any $l \in \mathbb{Z}_m$ and any $k \in \mathbb{Z}_{rm}$, with

$$f(km + l) = mc(r)\alpha(l)k^2 + \beta(l)k + g(l), \tag{1}$$

where

$$c(r) = \begin{cases} 1 & \text{for } r \text{ odd}, \\ \frac{1}{2} & \text{for } r \text{ even}, \end{cases}$$

α is any function over $\mathbb{Z}_r$ with $gcd(\alpha(l), r) = 1$ for all $l \in \mathbb{Z}_m$, $\beta : \mathbb{Z}_m \to \mathbb{Z}_{rm}$ is any function such that $l \mapsto \beta(l) \pmod m$ is a permutation over $\mathbb{Z}_m$, and g is any function over the rational numbers. Then s is a perfect sequence.

The next lemma on exponential sums will be used to prove the ZCZ property of the main construction in the next section.

Lemma 3. *[26] For any positive integer q and $a, b \in \mathbb{Z}_{2q}$ with $aq + b$ even, we have*

$$\left|\sum_{u=0}^{q-1} \exp(i\pi(au^2 + bu)/q)\right|^2 = \begin{cases} dq & b \equiv a(q/d) \pmod{2d} \\ 0 & b \not\equiv a(q/d) \pmod{2d}, \end{cases}$$

where $d = gcd(a, q)$.

In the following section, we use the unified construction of perfect sequences in Lemma 2 to construct two types of ZCZ sequence sets. The first type has sequences with zero AC across all out-of-phase shifts and nonzero CC only at sub-periodic correlation shifts. For convenience, we call such sets *ZCCZ sets*. The second type has nonzero AC only at subperiodic correlation shifts and zero CC across all shifts, i.e. interference-free sequences with zero autocorrelation zones; for short, we call these *ZACZ sets*.

3 Optimal ZCZ sequence sets

3.1 Construction of ZCCZ sets

In this section, we employ Mow's unified construction to construct ZCCZ sets which consist of perfect sequences with zero cross-correlation zone. With additional restrictions on the functions g and β in Lemma 2, we can derive ZCZ sequence sets with desirable properties.

Construction 1. *Let r and m be integers with r square-free. Let ω_{rm} be a primitive rm-th root of unity. A sequence set of size m of period $N = rm^2$ is denoted by*

$$\mathcal{S} = \{\mathbf{s}_n = \{s_n(t)\}_{t=0}^{N-1}, 0 \le n < m\}.$$

For each n, the sequence $\mathbf{s}_n$ is defined as

$$s_n(km + l) = \omega_{rm}^{f_n(km+l)}, 0 \le l < m, 0 \le k < rm,$$

with

$$f_n(km + l) = mc(r)\alpha(l)k^2 + \beta(l)k + nrg(l),$$

where

$$c(r) = \begin{cases} 1 & \text{for } r \text{ odd}, \\ \frac{1}{2} & \text{for } r \text{ even}, \end{cases}$$

α is any function over $\mathbb{Z}_r$ with $gcd(\alpha(l), r) = 1$ for all $l \in \mathbb{Z}_m$, $\beta : \mathbb{Z}_m \to \mathbb{Z}_{rm}$ is any function such that $l \mapsto \beta(l) \pmod m$ is a permutation over $\mathbb{Z}_m$, and g is any permutation over $\mathbb{Z}_m$ such that there exist no c_1 and c_2 in $\mathbb{Z}_m^*$ with $c_1 \cdot (\beta(l) \bmod m) + c_2 \cdot g(l) = 0$, where $\mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{0\}$.

Note that cyclically equivalent sequences are not desirable in practical applications [6], since they are not treated as essentially different sequences. The next lemma ensures that all the sequences in the constructed set are cyclically distinct.

Lemma 4. *All the sequences in $\mathcal{S}$, given by Construction 1, are cyclically distinct.*

We leave out the proof due to space constraints.

Theorem 1. *The sequence set $\mathcal{S}$, given by Construction 1, is a (rm^2, m, rm)-ZCZ sequence set.*

Proof. Since each sequence is obtained from Mow's unified construction in Lemma 2, all the sequences in $\mathcal{S}$ are perfect.

For any shift $0 \le \tau < rm^2$, we write $\tau = \tau_1 \cdot m + \tau_2$, where $0 \le \tau_1 < rm$ and $0 \le \tau_2 < m$. The cross-correlation of $s_{n_1}(t)$ and $s_{n_2}(t)$ for $n_1 \ne n_2$ at shift τ is

$$\begin{aligned} R_{\mathbf{s}_{n_1},\mathbf{s}_{n_2}}(\tau) &= \sum_{t=0}^{N-1} s_{n_1}(t+\tau)s_{n_2}^*(t) \\ &= \sum_{l=0}^{m-1} \omega_{rm}^{mc(r)\alpha(l+\tau_2)\tau_1^2+\beta(l+\tau_2)\tau_1+n_1rg(l+\tau_2)-n_2rg(l)} \\ &\sum_{k=0}^{rm-1} \omega_{rm}^{mc(r)(\alpha(l+\tau_2)-\alpha(l))k^2+(2mc(r)\alpha(l+\tau_2)\tau_1+\beta(l+\tau_2)-\beta(l))k}. \end{aligned}$$

We now consider the inner sum from equation above and examine two cases.

Case i) $\tau_2 \neq 0$: to apply Lemma 3, let $q = rm$, $a = 2[mc(r)(\alpha(l+\tau_2) - \alpha(l))]$ and $b = 2[2mc(r)\alpha(l+\tau_2)\tau_1 + \beta(l+\tau_2) - \beta(l)]$. Note that $aq + b$ is even. Since $gcd(\alpha(l), r) = 1$ for all $l \in \mathbb{Z}_m$, $\alpha(l+\tau_2) - \alpha(l)$ is even. Therefore $c(r)(\alpha(l+\tau_2) - \alpha(l))$ is always an integer and m divides d. So the condition $b \equiv a(q/d) \bmod 2d$ in Lemma 3 implies that $b \equiv a(q/d) \bmod 2m$. Plugging in the values of a, b, we have $\beta(l+\tau_2) \equiv \beta(l) \bmod m$, which is impossible for $\tau_2 \neq 0$. It follows from Lemma 3 that the inner sum is zero for $\tau_2 \neq 0$. Therefore, $R_{\mathbf{s}_{n_1}, \mathbf{s}_{n_2}}(\tau) = 0$ for $\tau_2 \neq 0$.

Case ii) $\tau_2 = 0$: then the inner sum becomes $\sum_{k=0}^{rm-1} \omega_r^{2c(r)\alpha(l)\tau_1 k} = m \sum_{k=0}^{r-1} \omega_r^{2c(r)\alpha(l)\tau_1 k}$. Since $gcd(\alpha(l), r) = 1$ for all $l \in \mathbb{Z}_m$, then $2c(r)\alpha(l)\tau_1 \not\equiv 0 \bmod r$ if $\tau_1 \not\equiv 0 \bmod r$, which means the inner sum is zero. Therefore $R_{\mathbf{s}_{n_1}, \mathbf{s}_{n_2}}(\tau) = 0$ for $\tau_2 = 0$ and $\tau_1 \not\equiv 0 \bmod r$.

When $\tau_1 = \tau_2 = 0$, we have

$$R_{\mathbf{s}_{n_1}, \mathbf{s}_{n_2}}(\tau) = rm \sum_{l=0}^{m-1} \omega_m^{(n_1 - n_2)g(l)},$$

which is zero because $n_1 \neq n_2$ and g is a permutation over $\mathbb{Z}_m$.

Combining the above cases, $\mathcal{S}$ is a sequence set with ZCZ length rm, which is optimal by Lemma 1. □

Note that we can also interpret Construction 1 from the perspective of a "modulation" sequence as in [14]. A sequence of period N with a divisor m is defined as $s(t) = a(t)b(t \bmod m)$ where $a(t)$ is a "carrier" sequence and $b(t \bmod m)$ is a "modulation" sequence of m arbitrary root of unities. A sequence set can be obtained by using the same carrier sequence with different modulation sequences. This can be a ZCZ sequence set if the carrier sequence is well chosen and the different modulation sequences are orthogonal. Moreover, the number of different orthogonal modulation sequences determines the size of the sequence set. It is also important to ensure that all sequences in the set are cyclically distinct. In our case, $s_n(t)$ in Construction 1 can be rewritten as $s_n(t) = a(t)b_n(t \bmod m)$, where $a(t) = a(km + l) = \omega_{rm}^{mc(r)\alpha(l)k^2 + \beta(l)k}$ and $b_n(t \bmod m) = \omega_m^{ng(l)}$. We proved that all the sequences in the set are cyclically distinct and the constructed set is an optimal ZCZ set with respect to the Tang-Fan-Matsufuji bound.

In [14], the Zadoff-Chu sequence was employed as a carrier sequence, which is a special case of the unified construction. The authors proposed two types of orthogonal modulation sequences: discrete Fourier transform (DFT) sequences and binary Hadamard sequences. As pointed out in [29], orthogonal modulation sequences obtained from the discrete Fourier transform (DFT) may lead to equivalent sequences in the set. Additionally, it is easy to check that the ZCZ sequence sets obtained by the binary Hadamard sequences given in [14] always lead to equivalent sequences. In our work, instead of discrete Fourier transform (DFT) sequences, we employ the generalised DFT sequences $b_n(t \bmod m) = \omega_m^{ng(l)}$. The condition on the functions g and β in the carrier sequence ensures that the resulting sequences are inequivalent.

In [29], the authors derived optimal (p^2, p, p)-ZCZ sequence sets from perfect nonlinear functions for an odd prime p. The construction can also be viewed as a carrier sequence from a special case of generalised Frank sequences with modulation sequences from generalised DFT sequences, which is a special case of our construction.

Construction 1 includes both [14] and [29] as special cases. The parameters in this paper are more flexible than those in [29]. The parameters in [14] can be flexible, but this comes at a cost to the autocorrelation property. The corresponding sequence could be perfect if the parameters are carefully chosen. Moreover, as mentioned before, the constructions in [14] may

produce equivalent sequences, while we derive the conditions under which all the sequences in the set are cyclically inequivalent.

3.2 Construction of ZACZ sets

In this subsection, we examine the structure of one perfect sequence from the unified construction and decompose it in a special way. Then we get a sequence set with some desirable properties. The cross-correlation between any two different sequences is zero for all shifts, i.e., the set is uncorrelated. Each sequence has a zero autocorrelation zone. Thus, we obtain a set of interference-free sequences with zero autocorrelation zone.

We can rewrite the sequence of period $N = rm^2$ in Lemma 2 in the form of an $rm \times m$ matrix such that the sequence can be reproduced by concatenating successive rows of the matrix. Every column can then be regarded as a new sequence. Thus, we derive a sequence set of size m as follows.

Construction 2. *Let r and m be integers. Let ω_{rm} be a primitive rm-th root of unity. A sequence set of size m of period rm is denoted by*

$$\mathcal{U} = \{\mathbf{u}_l = \{u_l(k)\}_{k=0}^{rm-1}, 0 \le l < m\}.$$

For each l, the sequence $\mathbf{u}_l$ is defined as

$$u_l(k) = \omega_{rm}^{f_l(k)} = \omega_{rm}^{mc(r)\alpha(l)k^2+\beta(l)k}, 0 \le k < rm,$$

where

$$c(r) = \begin{cases} 1 & \text{for } r \text{ odd}, \\ \frac{1}{2} & \text{for } r \text{ even}, \end{cases}$$

α is any function over $\mathbb{Z}_r$ with $gcd(\alpha(l), r) = 1$ for all $l \in \mathbb{Z}_m$ and $\beta : \mathbb{Z}_m \to \mathbb{Z}_{rm}$ is any function such that $l \mapsto \beta(l) \pmod m$ is a permutation over $\mathbb{Z}_m$.

Lemma 5. *[26] The set $\mathcal{U}$ is periodically uncorrelated and complementary.*

Using the property of the set $\mathcal{U}$ being periodically uncorrelated, it is easy to prove that $\mathcal{U}$ is an optimal ZACZ set.

Theorem 2. *The set $\mathcal{U}$ in Construction 2 is an optimal (rm, m, r)-ZCZ sequence set.*

Proof. Lemma 5 shows that $\mathcal{U}$ is periodically uncorrelated. To prove the ZCZ property of this set, we only need to consider the autocorrelation property of the sequences in the set.

The autocorrelation of $\mathbf{u}_l$ at shift τ is

$$\begin{aligned} R_{\mathbf{u}_l}(\tau) &= \sum_{k=0}^{rm-1} u_l(k+\tau)u_l^*(k) \\ &= \sum_{k=0}^{rm-1} \omega_{rm}^{mc(r)\alpha(l)(k+\tau)^2+\beta(l)(k+\tau)-mc(r)\alpha(l)k^2-\beta(l)k} \\ &= m\omega_{rm}^{mc(r)\alpha(l)\tau^2+\beta(l)\tau} \sum_{k=0}^{r-1} \omega_r^{2c(r)\alpha(l)\tau k}. \end{aligned}$$

Since $gcd(\alpha(l), r) = 1$ for all $l \in \mathbb{Z}_m$, $2c(r)\alpha(l)\tau \not\equiv 0 \bmod r$ provided that $\tau \not\equiv 0 \bmod r$, which means the sum above is zero for $\tau \not\equiv 0 \bmod r$. So $R_{\mathbf{u}_l}(\tau) = 0$ for $\tau \not\equiv 0 \bmod r$.

Thus, the constructed set $\mathcal{U}$ is an optimal (rm, m, r)-ZCZ sequence set with respect to the Tang-Fan-Matsufuji bound. □

Note that it is not necessary for r to be square-free in Construction 2. Since the set $\mathcal{U}$ is uncorrelated, it is obvious that all the sequences in $\mathcal{U}$ are cyclically distinct.

We can rewrite $u_l(k)$ in Construction 2 as $\omega_r^{c(r)\alpha(l)k^2}\omega_{rm}^{\beta(l)k}$. When r is odd, $\omega_r^{mc(r)\alpha(l)k^2}$ corresponds to an Ipatov sequence of period r, which is also a Zadoff-Chu seqeunce of odd length. When r is even, $\omega_r^{c(r)\alpha(l)k^2}$ is a Zadoff-Chu seqeunce of even length. If $\beta(l) = l$, then the set $\mathcal{U}$ is a special case of the construction in [16]. However, β in our construction is any function over $\mathbb{Z}_{rm}$ such that $l \mapsto \beta(l) \pmod{m}$ is a permutation on $\mathbb{Z}_m$, which means that our construction is more general in this specific case.

4 Conclusion

We introduced two constructions of ZCZ sequence sets based on the unified construction of perfect polyphase sequences. We showed that each ZCZ set obtained using these constructions is optimal with respect to the Tang-Fan-Matsufuji bound.

References

[1] R. Appuswamy and A. K. Chaturvedi, "A new framework for constructing mutually orthogonal complementary sets and ZCZ sequences," *IEEE Trans. Inform. Theory*, vol. 52, no. 8, pp. 3817-3826, 2006.

[2] A. K. Brodzik, "New polyphase sequence sets with all-zero cross-correlation," in *Proc. IEEE Int. Symp. Inf. Theory*, Boston, MA, USA, pp. 1421–1424, Jul. 2012.

[3] H. Chung and P. V. Kumar, "A new general construction for generalized bent functions," *IEEE Trans. Inform. Theory,* vol. IT-35, pp. 206-209, 1989.

[4] X. M. Deng and P. Z. Fan, "Spreading sequence sets with zero correlation zone," *Electron. Letters,* vol. 36, no. 11, pp. 993-994, 2000.

[5] P. Z. Fan and L. Hao, "Generalized orthogonal sequences and their applications in synchronous CDMA systems," *IEICE Trans. Fundam.*, vol. 83, no. 11, pp. 2054-2069, Nov. 2000.

[6] S. W. Golomb and G. Gong, "Signal Designs With Good Correlation: For Wireless Communications, Cryptography and Radar Applications," Cambridge, U.K.: Cambridge University Press, 2005.

[7] H. Hu and G. Gong, "New sets of zero or low correlation zone sequences via interleaving techniques," *IEEE Trans. Inform. Theory*, vol. 56, no. 4, pp. 1702-1713, Apr. 2010.

[8] T. Hayashi, "A class of zero-correlation zone sequence sets using a perfect sequence,"*IEEE Signal Process. Lett.*, vol. 16, no. 4, pp. 331-334, Apr. 2009.

[9] P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized bent functions and their properties," *J. Combin. Theory Ser. A,* vol. 40, no. 1, pp. 90-107, Sept. 1985.

[10] Y. C. Liu, C. W. Chen, and Y. T. Su, "New constructions of zero-correlation zone sequences," *IEEE Trans. Inform. Theory*, vol. 59, no. 8, pp. 4994-5007, 2013.

[11] S. Matsufuji, N. Kuroyanagi, N. Suehiro, and P. Z. Fan, "Two types of polyphase sequence sets for approximately synchronized CDMA systems," *IEICE Trans. Fundamentals,* vol. E86-A, no. 1, pp. 229-234, 2003.

[12] A. Milewski, "Periodic sequences with optimal properties for channel estimation and fast start-up equalization," *IBM J. Res. Develop.,* vol. 27, no. 5, pp. 426-431, 1983.

[13] S. I. Park, S. R. Park, I. Song, and N. Suehiro, "Multiple-access interference reduction for QS-CDMA systems with a novel class of polyphase sequences," *IEEE Trans. Inform. Theory,* vol. 46, no. 4, pp. 1448-1458, July 2000.

[14] B. M. Popovic and O. Mauritz, "Generalized chirp-like sequences with zero correlation zone," *IEEE Trans. Inform. Theory,* vol. 56, no. 6, pp. 2957-2960, June 2010.

[15] B. M. Popovic, "Generalized chirp-like polyphase sequences with optimum correlation properties," *IEEE Trans. Inform. Theory,* vol. 38, no. 4, pp. 1406-1409, July 1992.

[16] B. M. Popovic, "Optimum sets of interference-free sequences with zero autocorrelation zones," *IEEE Trans. Inform. Theory,* vol. 64, no. 4, pp. 2876-2882, April 2018.

[17] D. Sarwate, "Bounds on cross-correlation and autocorrelation of sequences," *IEEE Trans. Inform. Theory*, vol. IT-25, no. 6, pp. 720 - 724, Nov. 1979.

[18] X. H. Tang, P. Z. Fan, and S. Matsufuji, "Lower bounds on correlation of spreading sequence set with low or zero correlation zone," *Electron. Lett,* vol. 36, pp. 551-552, Mar. 2000.

[19] X. H. Tang, and W. H. Mow, "Design of spreading codes for quasi-synchronous CDMA with intercell interference," *IEEE J. Sel. Areas Commun.,* vol. 24, no. 1, pp. 84-93, 2006.

[20] X. H. Tang, and W. H. Mow, "A new systematic construction of zero correlation zone sequences based on interleaved perfect sequences," *IEEE Trans. Inform. Theory,* vol. 54, no. 12, pp. 5279-5734, Dec. 2008.

[21] X. H. Tang, P. Z. Fan, and J. Lindner, "Multiple binary ZCZ sequence sets with good cross-correlation property based on complementary sequence sets," *IEEE Trans. Inform. Theory,* vol. 56, no. 8, pp. 4038-4045, Aug. 2010.

[22] L. S. Tsai, and Y. T. Su, "Transform domain approach for sequence design and its applications," *IEEE J. Sel. Areas Commun.,* vol. 24, no. 1, pp. 75-83, Jan. 2006.

[23] H. Torii, M. Nakamura, and N. Suehiro, "A new class of zero-correlation zone sequences," *IEEE Trans. Inform. Theory,* vol. 50, no. 3, pp. 559-565, Mar. 2004.

[24] H. Torii, T. Matsumoto, and M. Nakamura, "A new method for constructing asymmetric ZCZ sequence sets," *IEICE Trans. Fundamentals,* vol. E95-A, no. 9, pp. 1577-1586, Sept. 2012.

[25] L. Wang, X. Zeng, and H. Wen, "Asymmetric ZCZ sequence sets with inter-subset uncorrelated sequences via interleaved technique," *IEICE Trans. Fundamentals,* vol. E100-A, no. 2, pp. 751-756, Feb. 2017.

[26] W. H. Mow, "A new unified construction of perfect root-of-unity sequences," in *Proc. IEEE 4th Int. Symp. Spread Spectr. Techn. Appl. (ISSSTA),* pp. 955-959, Sep. 1996.

[27] J. D. Yang, X. Jin, K. Y. Song, J. S. No, and D. J. Shin, "Multicode MIMO systems with quaternary LCZ and ZCZ sequences," *IEEE Trans. Vehicular Technology*, vol. 57, no. 4, pp. 2334-2341, 2008.

[28] Z. C. Zhou, X. H. Tang, and G. Gong, "A new class of sequences with zero or low correlation zone based on interleaving technique," *IEEE Trans. Inform. Theory,* vol. 54, no. 9, pp. 4267-4273, 2008.

[29] Z. C. Zhou, D. Zhang, T. Helleseth and J. M. Wen, "A construction of multiple optimal ZCZ sequence sets with good cross correlation," *IEEE Trans. Inform. Theory,* vol. 64, no. 2, pp. 1340 - 1346, 2018.

Paper IV

3.4 New optimal zero-correlation zone sequences based on IF-ZAZ sequences and interleaving technique

Dan Zhang, Chunlei Li and Matthew Geoffrey Parker
partly presented at the conference SETA (2020) (to be submitted)

Paper V

3.5 A construction of multiple optimal ZCZ sequences with good cross correlation

Zhengchun Zhou, Dan Zhang, Tor Helleseth, and Jinming Wen
IEEE Transactions on Information Theory, vol. 64, no. 2, pp. 1340-1346 (2018)

A Construction of Multiple Optimal ZCZ Sequence Sets with Good Cross-Correlation

Zhengchun Zhou
email: zczhou@126.com

Dan Zhang
email: dan.zhang@uib.no

Tor Helleseth
email: tor.helleseth@uib.no

Jinming Wen
email: jinming.wen@utoronto.ca

Abstract

Zero correlation zone (ZCZ) sequences are a class of spreading sequences having ideal auto-correlation and cross-correlation in a zone around the origin. They have been extensively studied in recent years due to their important applications in quasi-synchronous code division multiple access (QS-CDMA) systems. In this paper, a construction of ZCZ sequence sets is proposed based on perfect nonlinear functions. It generates multiple ZCZ sequence sets with the properties: (1) each sequence is perfect in the sense that its out-of-phase auto-correlation is always zero; (2) each ZCZ sequence set is optimal with respect to the Tang-Fan-Matsufuji bound in which all the sequences are pairwise cyclically distinct; and (3) the maximum inter-set cross-correlation of multiple sequence sets achieves the well-known Sarwate bound.

***Index terms*—** Spreading sequence, zero correlation zone (ZCZ), inter-set cross-correlation, quasi-synchronous code division multiple access (QS-CDMA), Tang-Fan-Matsufuji bound.

1 Introduction

Code-division multiple-access (CDMA) has been widely applied in digital cellular systems. For quasi-synchronous CDMA (QS-CDMA) systems, a time delay between the signals of different users within a few chips is allowed, which provides more flexibility in designing communication systems. In order to utilize this advantage, a new class of spreading sequences, called zero correlation zone (ZCZ) sequences [8], were employed in QS-CDMA systems, which can eliminate both multiple access interference and multipath interference in such a system [9]. In addition to this application, ZCZ sequences also have good performance in MIMO [30], ranging systems [5], and OFDM [15].

A set of ZCZ sequences consists of equal-length sequences whose out-of-phase auto-correlation and cross-correlation are all equal to zero over the range of delays $|\tau| < Z_{cz}$, where τ is a time shift and Z_{cz} is called the length of ZCZ. Let $\mathcal{S}$ be a ZCZ sequence set of period N with set size M and ZCZ length Z_{cz}. In order to accommodate a large number of users and to ease the synchronization requirement, it is usually desirable that M and Z_{cz} are both as large as possible for a given sequence length in the design of ZCZ sequence sets. However, the Tang-Fan-Matsufuji bound [23] implies that the parameters of a ZCZ sequence set have to satisfy $MZ_{cz} \leq N$. That is, for any given sequence period N, there is a tradeoff between the set

size M and ZCZ length Z_{cz}. A ZCZ sequence set meeting the theoretical bound with equality is said to be optimal. Searching optimal ZCZ sequence sets has been an interesting research topic in recent years. Many classes of optimal ZCZ sequence sets have been reported in the literature (see [9, 10, 18, 20, 24, 25, 27, 31], and references therein).

There is a similar scenario in the conventional spreading sequence design for asynchronous CDMA (A-CDMA) systems, which is also limited by some theoretical bounds such as the Welch bound [28]. In [12], Gong introduced a concept of intraference among sequences, which is referred to as the inter-set cross-correlation of multiple sequence sets (i.e., cross-correlation between any two sequences from distinct sets), and then proposed some constructions for yielding multiple sequence sets with low correlation. To the best of our knowledge, the analogous inter-set cross-correlation of spreading sequences in synchronous CDMA (S-CDMA) systems was proposed by Yang and Kumar [29]. Based on the so-called bent functions and semi-bent functions, they obtained several classes of orthogonal sequence sets with low inter-set cross-correlation [29].

Table 1: The parameters of some multiple ZCZ sequence sets

Period	Phase	Set size	Z_{cz}	The number of sets	inter-set cross-correlation zone Z	Maximal inter-set cross-correlation in zone Z	References
2^n	2	2^n	1	2^{n-1}	2^n	$2^{\frac{n}{2}}$	[29]
$2^{n+2}(Q-1)$	2	2^{n+1}	Q	2^{n-1}	Q	$2^{\frac{n+4}{2}}(Q-1)$	[26] †
$2^{n+2}(Q-1)$	2	2^{n+1}	Q	2^n	Q	$2^{\frac{n+5}{2}}(Q-1)$	[26] ‡
$2^{n+1}Q+2Q-2$	3	2^{n+1}	Q	2^{n-1}	Q	$2^{\frac{n+2}{2}}Q$	[24]†
$2^{n+1}Q+2Q-2$	3	2^{n+1}	Q	2^n	Q	$2^{\frac{n+3}{2}}Q$	[24]‡
2^{n+2}	4	2^n	4	2^n	4	$2^{\frac{n+4}{2}}$	[17]
$N=ML$	N	M	L	$\nu(N)$	N	$\sqrt{N}$	[20]§
p^2	p	p	p	$p-1$	p^2	p	This paper *

† n is even ‡ n is odd * p is any odd prime Q is a positive integer with certain property. § $\nu(N)=|I|$, where I is a subset of $\{i : 1 \le i < N, \gcd(i,N)=1\}$ such that $\gcd(i_1-i_2,N)=1$ for all $i_1 \ne i_2 \in I$.

Facing this challenge of ZCZ sequence design, one similarly promising solution is to construct multiple ZCZ sequence sets with favorable inter-set cross correlation. Specifically, it is desirable to obtain K ZCZ sequence sets $\mathcal{S}^m$, $0 \le m < K$, with the following properties

1. each $\mathcal{S}^m$ is an optimal ZCZ sequence set with respect to the Tang-Fan-Matsufuji bound; and

2. the K sequence sets have low inter-set cross correlation within a certain zone with length Z, i.e., the maximal inter-set cross-correlation value is less than or equal to a constant δ, which is small compared with the length N.

It is worthwhile to point out that multiple ZCZ sequence sets can be used in multiuser environments to enlarge the application of ZCZ sequences [24]. As mentioned above, a vast amount of knowledge exists for the design of single ZCZ sequence set, but relatively little is known about the multiple ones. In recent years, some progress on the constructions of multiple ZCZ sequence sets has been made. In [1], Appuswamy and Chaturvedi constructed mutually orthogonal binary ZCZ sequence sets from mutually orthogonal complementary sequence sets (MOCSS) and orthogonal matrices, i.e. $Z = 0$ and $\delta = 0$. Tang and Mow presented a systematic construction of many new families of generalized loosely synchronized codes with low intercode cross-correlation properties within a certain window [24]. Later in [26], Tang,

Fan, and Lindner generated multiple ZCZ sequence sets with good inter-set cross-correlation from some specific families of MOCSS. Recently in [17], Li, Tan, and Tang obtained quaternary multiple sets with good correlation property based on Zadoff-Chu sequences [4]. The parameters of these known multiple ZCZ sequence sets are listed in Table I. As pointed out by one of the anonymous reviews, the construction of ZCZ sequence sets in [20] based on Zadoff-Chu sequences can be extended to obtain multiple ZCZ sequence sets whose maximum inter-set cross-correlation achieves the Sarwate bound (see Remark 3 in Section 3 for more details). The parameters of this class of multiple ZCZ sequence sets are also listed in Table I. It will be seen later that some ZCZ sequences generated by the construction in [20] may be cyclically equivalent. Note that cyclically equivalent sequences are not desirable in practically applications [13], since they are not treated as essentially different sequences.

Perfect nonlinear functions (PNFs) are a class of functions with optimal nonlinearity which have important applications in cryptography, sequences and coding theory. In cryptography, PNFs can be used to construct keystream generators for stream ciphers, S-boxes for block ciphers, building blocks for hash algorithms, and authentication codes [19], [7]. In coding theory, they permit to construct good error correcting codes [2]. In sequences, they are used to obtain frequency-hopping sequences with good Hamming correlation for FH-CDMA communication systems [6].

The objective of this paper is to present a construction of multiple ZCZ sequence sets using perfect nonlinear functions over a cyclic group. Like the construction in [20], this construction also generates multiple ZCZ sets with properties: (1) each sequence is perfect in the sense that its out-of-phase auto-correlation is always zero; (2) each ZCZ sequence set is optimal with respect to the Tang-Fan-Matsufuji bound; and (3) the maximum inter-set cross-correlation of multiple sequence sets achieves the well-known Sarwate bound. Most notably, we can mathematically prove that all the generated ZCZ sequences are cyclically distinct. The key of our construction is to find suitable permutations with certain properties. As a comparison with the known ones, the parameters of our multiple ZCZ sequence sets are also listed in Table I.

2 PRELIMINARIES

Let $\mathcal{S}$ be a family of M complex roots of unity sequences of period N, which can be written as

$$\begin{aligned} \mathcal{S} &= \{\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{M-1}\}, \\ \mathbf{s}_i &= (s_i(0), s_i(1), \cdots, s_i(N-1)) = \{s_i(t)\}_{t=0}^{N-1}, \end{aligned}$$

where each $s_i(t)$ is a complex number with modulus 1. For two sequences, say $\mathbf{u} = \{u(t)\}_{t=0}^{N-1}$ and $\mathbf{v} = \{v(t)\}_{t=0}^{N-1}$ in $\mathcal{S}$, their (periodic) cross-correlation function at a shift of τ is defined by

$$R_{\mathbf{u},\mathbf{v}}(\tau) = \sum_{t=0}^{N-1} u(t+\tau)v^*(t), \quad 0 \le \tau < N,$$

where $t + \tau$ is reduced modulo N and x^* is the complex conjugate of the complex number x. When $\mathbf{u} = \mathbf{v}$, $R_{\mathbf{u},\mathbf{u}}(\tau)$ is called the auto-correlation function of $\mathbf{u}$. In this case, we write $R_{\mathbf{u},\mathbf{u}}(\tau) = R_{\mathbf{u}}(\tau)$ for short. A sequence $\mathbf{u}$ is said to be perfect if $R_{\mathbf{u}}(\tau) = 0$ for all $0 < \tau < N$. Two sequences $\mathbf{u}$ and $\mathbf{v}$ are said to be cyclically equivalent if there exists some $0 \le \tau < N$ and a constant complex number c with $|c| = 1$ such that $v(t) = cu(t + \tau)$ for all $0 \le t < N$ (i.e., $|R_{\mathbf{u},\mathbf{v}}(\tau)| = N$). Otherwise they are said to be cyclically distinct. In practical applications, all

employed sequences are preferred to be cyclically distinct since cyclically equivalent sequences are not treated as essentially different sequences [12], [13].

For the sequence set $\mathcal{S}$, the maximum out-of-phase periodic auto-correlation magnitude R_a and the maximum periodic cross-correlation magnitude R_c are respectively defined by

$$R_a = \max\{|R_{\mathbf{u}}(\tau)| : \mathbf{u} \in \mathcal{S}, 0 < \tau < N\},$$

and

$$R_c = \max\{|R_{\mathbf{u},\mathbf{v}}(\tau)| : \mathbf{u}, \mathbf{v} \in \mathcal{S}, \mathbf{u} \neq \mathbf{v}, 0 \leq \tau < N\}.$$

The following is the well-known Sarwate bound on R_a and R_c.

Lemma 1. *([22]) For any sequence set $\mathcal{S}$ with M sequences of period N,*

$$\frac{R_c^2}{N} + \frac{N-1}{N(M-1)}\frac{R_a^2}{N} \geq 1. \tag{1}$$

Lemma 1 tells us that it is impossible to get a sequence set with both R_a and R_c being zero. This implies that the cross-correlation and nontrivial auto-correlation can not be zero for all τ. However, this can be achieved when the time shift τ is located at some zone around the origin, which motivated the notion and development of the so-called zero correlation zone sequences [8].

Definition 1. *Let $\mathcal{S}$ be a set of M sequences of period N, then the zero correlation zone Z_{cz} is defined as*

$$Z_{cz} = max\{T : R_{\mathbf{u},\mathbf{v}}(\tau) = 0 \ for \ (0 < |\tau| < T) \ or \ (\tau = 0 \ and \ \mathbf{u} \neq \mathbf{v}), \forall\, \mathbf{u}, \mathbf{v} \in \mathcal{S}\}.$$

Moreover, $\mathcal{S}$ is called an (N, M, Z_{cz})-ZCZ sequence set.

Since $|R_{\mathbf{u},\mathbf{v}}(-\tau)| = |R_{\mathbf{v},\mathbf{u}}(\tau)|$, it suffices to compute the correlation function of sequences in $\mathcal{S}$ with $0 \leq \tau < N$, i.e.,

$$Z_{cz} = \max\{T : R_{\mathbf{u},\mathbf{v}}(\tau) = 0 \ \text{ for } (0 < \tau < T) \text{ or } (\tau = 0 \text{ and } \mathbf{u} \neq \mathbf{v}), \forall\, \mathbf{u}, \mathbf{v} \in \mathcal{S}\}.$$

The following bound implies that there is a tradeoff among the parameters of any ZCZ sequence set.

Lemma 2. *(Tang-Fan-Matsufuji bound [23]) Let $\mathcal{S}$ be a set of M sequences of period N with ZCZ length Z_{cz}, then*

$$MZ_{cz} \leq N.$$

A ZCZ sequence set meeting the Tang-Fan-Matsufuji bound with equality is said to be optimal.

In this paper, we will construct multiple optimal ZCZ sequence sets whose maximal inter-set cross-correlation achieves the Sarwate bound in Lemma 1. Our construction is based on perfect nonlinear functions (PNFs) which have important applications in cryptography and coding theory. In what follows, we shall give a brief introduction to PNFs. For more details on PNFs and their applications, the reader is referred to [3].

Let f be a function from a finite abelian group $(A,+)$ to another finite abelian group $(B,+)$. We say that f is linear if and only if $f(x+y) = f(x) + f(y)$ for all $x, y \in A$. A measure of nonlinearity of f is defined as

$$P_f = \max_{0 \neq a \in A} \max_{b \in B} \frac{|\{x \in A : f(x+a) - f(x) = b\}|}{|A|},$$

where $|A|$ denotes the cardinality of the set A. It is easily seen that $P_f \geq \frac{1}{|B|}$ [3]. Then f is called a PNF if $P_f = \frac{1}{|B|}$. It is easily verified that f is a PNF if and only if

$$|\{x \in A : f(x+a) - f(x) = b\}| = \frac{|A|}{|B|} \tag{2}$$

for any nonzero $a \in A$ and any $b \in B$. Thus PNF exists only when $|B|$ is a divisor of $|A|$.

Let $\mathbb{Z}_n$ denote the ring of integers modulo n, where n is a positive integer. The following is a known class of PNFs from $\mathbb{Z}_{p^2}$ to $\mathbb{Z}_p$. Herein and hereafter p is an odd prime.

Lemma 3. *[3] Let g be a function from $\mathbb{Z}_{p^2}$ to $\mathbb{Z}_p$ defined by*

$$g(t) = t_1 \cdot t_2 \mod p, \quad 0 \leq t < p^2,$$

where $t = t_1 + t_2 \cdot p$ and $0 \leq t_1, t_2 < p$. Then g is a PNF from $\mathbb{Z}_{p^2}$ to $\mathbb{Z}_p$.

Using the PNF in Lemma 3, we can obtain a complex sequence $\mathbf{s} = \{s(t)\}_{t=0}^{p^2-1}$ of period p^2 over the p-th root of unity, where $s(t) = \omega_p^{g(t)}$ for each $0 \leq t < p^2$ and ω_p is a primitive p-th root of unity. Based on (2), it is clear that $\mathbf{s}$ is a perfect sequence. In fact, this sequence is the well-known Frank-Zadoff sequence [11, 14]. PNFs can also be used to construct frequency-hopping sequences with optimal auto-correlation (see [6] for more details).

The following construction of PNFs is a generalization of Lemma 3. It is closely related with the Maiorana-McFarland construction of bent functions from $\mathbb{F}_p \times \mathbb{F}_p$ to $\mathbb{F}_p$ [16].

Lemma 4. *Let π be an arbitrary permutation of $\mathbb{Z}_p$ and σ be an arbitrary function from $\mathbb{Z}_p$ to $\mathbb{Z}_p$. Define a function from $\mathbb{Z}_{p^2}$ to $\mathbb{Z}_p$ as*

$$f(t) = \pi(t_1) \cdot t_2 + \sigma(t_1) \mod p, \quad 0 \leq t < p^2,$$

where $t = t_1 + t_2 \cdot p$ and $0 \leq t_1, t_2 < p$. Then f is a PNF from $\mathbb{Z}_{p^2}$ to $\mathbb{Z}_p$.

Proof. The conclusion follows directly from Theorem 16 in [3]. □

The following result shows that one can obtain a family of PNFs from one PNF in Lemma 4, which will be used to construct the desirable multiple ZCZ sequence sets in the sequel.

Lemma 5. *Let π be an arbitrary given permutation of $\mathbb{Z}_p$ and σ be an arbitrary given function from $\mathbb{Z}_p$ to $\mathbb{Z}_p$. Let $\mathcal{F} = \{f_{m,u} : 1 \leq m < p\ , 0 \leq u < p\ \}$ be a family of functions from $\mathbb{Z}_{p^2}$ to $\mathbb{Z}_p$, where*

$$f_{m,u}(t) = m\pi(t_1) \cdot t_2 + u\sigma(t_1) \mod p \tag{3}$$

for each $0 \leq t < p^2$ with $t = t_1 + t_2 \cdot p$ and $0 \leq t_1, t_2 < p$. Then each function in $\mathcal{F}$ is a PNF.

Proof. The conclusion follows from the fact that $m\pi(t_1)$ is a permutation for any $1 \leq m < p$ and Lemma 4. □

3 Multiple ZCZ sequence sets from perfect nonlinear functions

In this section, we present a simple construction of multiple ZCZ sequence sets with good properties from a subclass of PNFs in Lemma 5. Before doing this, we first fix some notations.

Let $\mathbb{Z}_p$ denote the ring of integers modulo p and ω_p be a primitive p-th root of unity, where p is an odd prime. We also need $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ and $\mathbb{Z}_p^{**} = \mathbb{Z}_p \setminus \{0, 1\}$.

Construction 1. *Let π be a permutation of $\mathbb{Z}_p$ such that the equation $\pi(x+a) \equiv c\pi(x) \pmod p$ has only one solution for any given $a \in \mathbb{Z}_p$ and $c \in \mathbb{Z}_p^{**}$. Let σ be a permutation of $\mathbb{Z}_p$ satisfying $\sigma \neq k\pi + l$ for any $k, l \in \mathbb{Z}_p$. For each $1 \leq m < p$, define a sequence set $\mathcal{S}^m$ as*

$$\mathcal{S}^m = \{\mathbf{s}_u^m \ : \ \mathbf{s}_u^m \triangleq \{s_u^m(t)\}_{t=0}^{p^2-1}, 0 \leq u < p\}.$$

Herein, for each $0 \leq t < p^2$,

$$s_u^m(t) = \omega_p^{f_{m,u}(t)}, \tag{4}$$

where $f_{m,u}(t)$ is the function from $\mathbb{Z}_{p^2}$ to $\mathbb{Z}_p$ given by (3).

For the sake of convenience, we fix some notations that will be used frequently to prove our main results in the sequel. Denote $\tau = \tau_1 + \tau_2 \cdot p$ for any time shift $0 \leq \tau < p^2$, where $0 \leq \tau_1, \tau_2 < p$. We also denote $t = t_1 + t_2 \cdot p$ for any integer $0 \leq t < p^2$, where $0 \leq t_1, t_2 < p$. Define

$$\delta_{t_1,\tau_1} = \begin{cases} 0 & \text{if } t_1 + \tau_1 < p, \\ 1 & \text{if } t_1 + \tau_1 > p. \end{cases}$$

The following lemma gives the set size of each sequence set generated by Construction 1.

Lemma 6. *For each $1 \leq m < p$, all sequences in $\mathcal{S}^m$ are cyclically shift distinct. Thus the set size of each $\mathcal{S}^m$ is p.*

Proof. Let $\mathbf{s}_u^m$ and $\mathbf{s}_v^m$ be any two sequences in $\mathcal{S}^m$, where $0 \leq u \neq v < p$. Assume on the contrary that they are cyclically shift equivalent, then there exist some integers τ and r such that

$$s_u^m(t) = s_v^m(t + \tau) \cdot \omega_p^r$$

for all $0 \leq t < p^2$. According to (3), we must have

$$\begin{aligned} m\pi(t_1) \cdot t_2 + u\sigma(t_1) \equiv\ & m\pi(t_1 + \tau_1) \cdot (t_2 + \tau_2 + \delta_{t_1,\tau_1}) + \\ & v\sigma(t_1 + \tau_1) + r \pmod p \end{aligned} \tag{5}$$

for all $0 \leq t_1, t_2 < p$. We distinguish between the following two cases to prove that this is impossible.

When $\tau_1 = 0$, $\delta_{t_1,\tau_1} = 0$ for all $0 \leq t_1 < p$, it is easy to verify that Equation (5) holds for all $0 \leq t_1, t_2 < p$ if and only if

$$\sigma(t_1) \equiv \frac{m\tau_2}{u - v} \cdot \pi(t_1) + \frac{r}{u - v} \pmod p$$

holds for all $0 \leq t_1 < p$. This is impossible for any $0 \leq \tau_2 < p$ since $\sigma \neq k\pi + l$ for any $k, l \in \mathbb{Z}_p$.

When $\tau_1 \neq 0$, on the other hand, we can deduce from (5) that

$$\begin{aligned} &m(\pi(t_1+\tau_1)-\pi(t_1))\cdot t_2 + m\pi(t_1+\tau_1)\cdot(\tau_2+\delta_{t_1,\tau_1})+ \\ &v\sigma(t_1+\tau_1)-u\sigma(t_1) \equiv r \pmod{p}. \end{aligned} \tag{6}$$

Note that π is a permutation and $\tau_1 \neq 0$. Thus $\pi(t_1+\tau_1)-\pi(t_1) \neq 0$ for any $0 \leq t_1 < p$. It follows that, for any given $0 \leq t_1 < p$, there exists at least one t_2 with $0 \leq t_2 < p$ such that (6) does not hold.

The analysis above shows that $\mathbf{s}_u^m$ and $\mathbf{s}_v^m$ are cyclically shift distinct. This finishes the proof of the lemma. □

The following is the main result of this paper.

Theorem 1. *Let $\mathcal{S}^m, 1 \leq m < p$, be the multiple sequence sets generated by Construction 1. Then,*

1. *Each sequence in $\mathcal{S}^m$ is perfect;*
2. *Each $\mathcal{S}^m$ is an optimal (p^2, p, p)-ZCZ sequence set.*
3. *$|R_{\mathbf{s}_u^m,\mathbf{s}_v^n}(\tau)| = p$ for all $0 \leq \tau < p^2$, $1 \leq m \neq n < p$, and $0 \leq u, v < p$.*

Proof. According to Lemma 5, each $f_{m,u}(t)$ is a PNF from $\mathbb{Z}_{p^2}$ to $\mathbb{Z}_p$, which means that the corresponding sequence $\mathbf{s}_u^m$ in $\mathcal{S}^m$ defined by (4) is perfect. This completes the proof of Part 1).

We now prove Part 2). Let $\mathbf{s}_u^m$ and $\mathbf{s}_v^m$ be two sequences in $\mathcal{S}^m$, where $0 \leq u \neq v < p$ and $1 \leq m < p$. We distinguish between the following two cases to calculate the correlation of $\mathbf{s}_u^m$ and $\mathbf{s}_v^m$:

$$R_{\mathbf{s}_u^m,\mathbf{s}_v^m}(\tau) = \sum_{t=0}^{p^2-1} \omega_p^{s_u^m(t+\tau)-s_v^m(t)}.$$

Case i), when $\tau = 0$: In this case, $\tau_1 = \tau_2 = 0$. It then follows from (4) and (3) that

$$\begin{aligned} R_{\mathbf{s}_u^m,\mathbf{s}_v^m}(\tau) &= \sum_{t_2=0}^{p-1}\sum_{t_1=0}^{p-1} \omega_p^{(u-v)\sigma(t_1)} \\ &= 0, \end{aligned}$$

where the second identity followed from the fact that $(u-v)\sigma$ is a permutation of $\mathbb{Z}_p$ for any $u \neq v$.

Case ii), when $0 < \tau < p$: In this case, $\tau_2 = 0$ and $0 < \tau_1 < p$. By (4) and (3), we have

$$\begin{aligned} &R_{\mathbf{s}_u^m,\mathbf{s}_v^m}(\tau) \\ &= \sum_{t_2=0}^{p-1}\sum_{t_1=0}^{p-1} \omega_p^{m\pi(t_1+\tau_1)\cdot(t_2+\delta_{t_1,\tau_1})+u\sigma(t_1+\tau_1)-(m\pi(t_1)\cdot t_2+v\sigma(t_1))} \\ &= \sum_{t_1=0}^{p-1} \omega_p^{m\pi(t_1+\tau_1)\cdot\delta_{t_1,\tau_1}+u\sigma(t_1+\tau_1)-v\sigma(t_1)} \sum_{t_2=0}^{p-1} \omega_p^{m(\pi(t_1+\tau_1)-\pi(t_1))t_2} \\ &= 0, \end{aligned}$$

where the last identity was due to $m(\pi(t_1+\tau_1)-\pi(t_1)) \not\equiv 0 \pmod{p}$ for any $0 < \tau_1 < p$, since $1 \leq m < p$ and π is a permutation of $\mathbb{Z}_p$.

The discussion in the two cases above together with Lemma 6 means that each $\mathcal{S}^m$ is a (p^2, p, Z_{cz})-ZCZ set with $Z_{cz} \geq p$. On the other hand, according to the Tang-Fan-Matsufuji bound of (2), we have $Z_{cz} \leq p$. Therefore each $\mathcal{S}^m$ is a (p^2, p, p)-ZCZ set and is optimal with respect to the Tang-Fan-Matsufuji bound.

Finally, we prove Part 3). Let $\mathbf{s}_u^m$ and $\mathbf{s}_v^n$ be two sequences in $\mathcal{S}^m$ and $\mathcal{S}^n$, respectively, where $1 \leq m \neq n < p$, and $0 \leq u, v < p$. Then the inter-set cross-correlation between $\mathbf{s}_u^m$ and $\mathbf{s}_v^n$ is given by

$$\begin{aligned} R_{\mathbf{s}_u^m, \mathbf{s}_v^n}(\tau) &= \sum_{t=0}^{p^2-1} \omega_p^{s_u^m(t+\tau) - s_v^n(t)} \\ &= \sum_{t_2=0}^{p-1} \sum_{t_1=0}^{p-1} \omega_p^{m\pi(t_1+\tau_1)(t_2+\tau_2+\delta_{t_1,\tau_1}) + u\sigma(t_1+\tau_1) - (n\pi(t_1)t_2 + v\sigma(t_1))} \\ &= \sum_{t_1=0}^{p-1} \omega_p^{m\pi(t_1+\tau_1)(\tau_2+\delta_{t_1,\tau_1}) + u\sigma(t_1+\tau_1) - v\sigma(t_1)} \\ &\quad \sum_{t_2=0}^{p-1} \omega_p^{(m\pi(t_1+\tau_1) - n\pi(t_1))t_2}. \end{aligned}$$

The inner sum is zero unless

$$m\pi(t_1 + \tau_1) \equiv n\pi(t_1) \pmod{p}. \tag{7}$$

Note that we have assumed that $\pi(x+a) \equiv c\pi(x) \pmod{p}$ has a unique solution x in $\mathbb{Z}_p$ for all $a \in \mathbb{Z}_p$ and $c \in \mathbb{Z}_p^{**}$. This means that (7) has only one solution of t_1 in $\mathbb{Z}_p$ for any $0 \leq \tau_1 < p$ and any $1 \leq m \neq n < p$. Therefore, $|R_{\mathbf{s}_u^m, \mathbf{s}_v^n}(\tau)| = p$ for all $1 \leq m \neq n < p$ and $0 \leq u, v < p$. This completes the proof of this theorem. □

Remark 1. *The conclusions in 1) and 3) of Theorem 1 imply that any pair of two sequences from two different ZCZ sequence sets $\mathcal{S}^m$ and $\mathcal{S}^n$ is optimal with respect to the Sarwate bound of (1). If we select any one sequence from each $\mathcal{S}^m$, then we derive a set of sequences of period p^2 with set size $p-1$ which is optimal with respect to the Sarwate bound. This means that the maximum inter-set cross-correlation of these ZCZ sequence sets achieves the Sarwate bound.*

The following lemma presents a class of permutations satisfying the condition of π in Construction 1.

Lemma 7. *Let $\pi(x) = x^e$, where e is a positive integer with $\gcd(p-1, e) = 1$. Then $\pi(x)$ is a permutation of $\mathbb{Z}_p$ such that the equation $\pi(x+a) \equiv c\pi(x) \pmod{p}$ has only one solution in $\mathbb{Z}_p$ for any $a \in \mathbb{Z}_p$ and any $c \in \mathbb{Z}_p^{**}$.*

Proof. Since p is an odd prime and $\gcd(p-1, e) = 1$, it is clear that $\pi(x)$ is a permutation of $\mathbb{Z}_p$, and $\pi(x) = 0$ (resp. $\pi(x) = 1$) if and only if $x = 0$ (resp. $x = 1$). When $a = 0$, the equation $\pi(x+a) \equiv c\pi(x) \pmod{p}$ becomes

$$(c-1)\pi(x) \equiv 0 \pmod{p}$$

which has a unique solution $x = 0$ in $\mathbb{Z}_p$ for any $c \in \mathbb{Z}_p^{**}$. On the other hand, when $a \in \mathbb{Z}_p^*$, $x = 0$ can never be a solution of the equation $\pi(x+a) \equiv c\pi(x) \pmod{p}$. Then $\pi(x+a) \equiv c\pi(x) \pmod{p}$ has the same solutions as the equation

$$\pi\left(\frac{a}{x} + 1\right) \equiv c \pmod{p}$$

which has a unique solution $x = \frac{a}{\pi^{-1}(c)-1}$ for any $a \in \mathbb{Z}_p^*$ and $c \in \mathbb{Z}_p^{**}$, where π^{-1} is the inverse mapping of $\pi(x)$. This completes the proof of the lemma. □

The following result follows directly from Lemma 7 and Theorem 1.

Corollary 1. *Let $\pi(x) = x^e$, where e is a positive integer with $\gcd(p-1, e) = 1$. Let σ be any permutation of $\mathbb{Z}_p$ satisfying $\sigma \neq k\pi + l$ for any $k, l \in \mathbb{Z}_p$. Then the sequence sets $\mathcal{S}^m, 1 \leq m < p$, generated by Construction 1 have the following properties*

1. *Each sequence in $\mathcal{S}^m$ is perfect;*
2. *Each $\mathcal{S}^m$ is an optimal (p^2, p, p)-ZCZ sequence set;*
3. *$|R_{\mathbf{s}_u^m, \mathbf{s}_v^n}(\tau)| = p$ for all $0 \leq \tau < p^2$, $1 \leq m \neq n < p$, and $0 \leq u, v < p$.*

Remark 2. *It might be possible to obtain more permutations π of $\mathbb{Z}_p$ satisfying the condition in Construction 1 other than the ones mentioned in Lemma 7. The reader is kindly invited to search such permutations.*

In the following, we use an example to illustrate Construction 1.

Example 1. *Let $p = 5$, $\pi(x) = x^3$ and $\sigma(x) = x$. By the construction above, then we can obtain 4 optimal ZCZ sequence sets of which the first two ones are*

$$\mathcal{S}^1 = \{\mathbf{s}_0^1, \mathbf{s}_1^1, \mathbf{s}_2^1, \mathbf{s}_3^1, \mathbf{s}_4^1\}, \quad \mathcal{S}^2 = \{\mathbf{s}_0^2, \mathbf{s}_1^2, \mathbf{s}_2^2, \mathbf{s}_3^2, \mathbf{s}_4^2\},$$

where

$$\begin{aligned}\mathbf{s}_0^1 = \{&1, \omega_5^2, 1, 1, \omega_5^3, 1, \omega_5^3, \omega_5^3, \omega_5^2, \omega_5^2, 1, \omega_5^4, \omega_5^1, \omega_5^4, \omega_5^1,\\ &1, 1, \omega_5^4, \omega_5^1, 1, 1, \omega_5^1, \omega_5^2, \omega_5^3, \omega_5^4\},\end{aligned}$$

$$\begin{aligned}\mathbf{s}_1^1 = \{&1, \omega_5^3, \omega_5^2, \omega_5^3, \omega_5^2, 1, \omega_5^4, 1, 1, \omega_5^1, 1, 1, \omega_5^3, \omega_5^2, 1, 1,\\ &\omega_5^1, \omega_5^1, \omega_5^4, \omega_5^4, 1, \omega_5^2, \omega_5^4, \omega_5^1, \omega_5^3\},\end{aligned}$$

$$\begin{aligned}\mathbf{s}_2^1 = \{&1, \omega_5^4, \omega_5^4, \omega_5^1, \omega_5^1, 1, 1, \omega_5^2, \omega_5^3, 1, 1, \omega_5^1, 1, 1, \omega_5^4, 1,\\ &\omega_5^2, \omega_5^3, \omega_5^2, \omega_5^3, 1, \omega_5^3, \omega_5^1, \omega_5^4, \omega_5^2\},\end{aligned}$$

$$\begin{aligned}\mathbf{s}_3^1 = \{&1, 1, \omega_5^1, \omega_5^4, 1, 1, \omega_5^1, \omega_5^4, \omega_5^1, \omega_5^4, 1, \omega_5^2, \omega_5^2, \omega_5^3, \omega_5^3,\\ &1, \omega_5^3, 1, 1, \omega_5^2, 1, \omega_5^4, \omega_5^3, \omega_5^2, \omega_5^1\},\end{aligned}$$

$$\begin{aligned}\mathbf{s}_4^1 = \{&1, \omega_5^1, \omega_5^3, \omega_5^2, \omega_5^4, 1, \omega_5^2, \omega_5^1, \omega_5^4, \omega_5^3, 1, \omega_5^3, \omega_5^4, \omega_5^1,\\ &\omega_5^2, 1, \omega_5^4, \omega_5^2, \omega_5^3, \omega_5^1, 1, 1, 1, 1, 1\},\end{aligned}$$

$$\begin{aligned}\mathbf{s}_0^2 = \{&1, \omega_5^3, \omega_5^3, \omega_5^2, \omega_5^2, 1, 1, \omega_5^4, \omega_5^1, 1, 1, \omega_5^2, 1, 1, \omega_5^3, 1,\\ &\omega_5^4, \omega_5^1, \omega_5^4, \omega_5^1, 1, \omega_5^1, \omega_5^2, \omega_5^3, \omega_5^4\},\end{aligned}$$

$$\mathbf{s}_1^2 = \{1, \omega_5^4, 1, 1, \omega_5^1, 1, \omega_5^1, \omega_5^1, \omega_5^4, \omega_5^4, 1, \omega_5^3, \omega_5^2, \omega_5^3, \omega_5^2,$$
$$1, 1, \omega_5^3, \omega_5^2, 1, 1, \omega_5^2, \omega_5^4, \omega_5^1, \omega_5^3\},$$

$$\mathbf{s}_2^2 = \{1, 1, \omega_5^2, \omega_5^3, 1, 1, \omega_5^2, \omega_5^3, \omega_5^2, \omega_5^3, 1, \omega_5^4, \omega_5^4, \omega_5^1, \omega_5^1,$$
$$1, \omega_5^1, 1, 1, \omega_5^4, 1, \omega_5^3, \omega_5^1, \omega_5^4, \omega_5^2\},$$

$$\mathbf{s}_3^2 = \{1, \omega_5^1, \omega_5^4, \omega_5^1, \omega_5^4, 1, \omega_5^3, 1, 1, \omega_5^2, 1, 1, \omega_5^1, \omega_5^4, 1, 1,$$
$$\omega_5^2, \omega_5^2, \omega_5^3, \omega_5^3, 1, \omega_5^4, \omega_5^3, \omega_5^2, \omega_5^1\},$$

$$\mathbf{s}_4^2 = \{1, \omega_5^2, \omega_5^1, \omega_5^4, \omega_5^3, 1, \omega_5^4, \omega_5^2, \omega_5^3, \omega_5^1, 1, \omega_5^1, \omega_5^3, \omega_5^2,$$
$$\omega_5^4, 1, \omega_5^3, \omega_5^4, \omega_5^1, \omega_5^2, 1, 1, 1, 1, 1\}.$$

It is easy to verify that

- *each sequence is perfect;*
- *each* $\mathcal{S}^m$ *is an optimal* $(25, 5, 5)$*-ZCZ sequence set, where* $1 \le m \le 4$*; and*
- $|R_{\mathbf{s}_u^m, \mathbf{s}_v^n}(\tau)| = 5$ *for all* $0 \le \tau \le 24$, $1 \le m \ne n \le 4$, *and* $0 \le u, v \le 4$.

These observations are consistent with Theorem 1.

Remark 3. *In [20], Popovic and Mauritz proposed a construction of ZCZ sequence sets based on the well-known Zadoff-Chu sequences [4]. The basic idea of this construction is to modulate a Zadoff-Chu sequence using a set of different orthogonal sequences. As pointed out by one of the anonymous reviews, by modulating a group of appropriately chosen Zadoff-Chu sequences, this construction can be extended to obtain multiple ZCZ sequence sets achieving the Sarwate bound by modulating suitably chosen Zadoff-Chu sequences. However, one point that should be mentioned here is that some ZCZ sequences generated in [20] may be cyclically equivalent.*

Let $N = ML$ *for two positive integers* M *and* L, *and let* I *be a subset of* $\{i : 1 \le i < N, \gcd(i, N) = 1\}$ *such that* $\gcd(i_1 - i_2, N) = 1$ *for all* $i_1 \ne i_2 \in I$. *For each* $i \in I$, *let* $\mathbf{a}_i = (a_i(0), a_i(1), \cdots, a_i(N-1))$ *be the Zadoff-Chu sequence of period* N *defined by*

$$a_i(t) = \omega_N^{it(t+N \bmod 2)/2},\ t = 0, 1, \cdots, N-1.$$

We now give a brief introduction to the construction of ZCZ sequences in [20]. Let $\mathbf{a}_i$ *be defined as above and* $B = \{\mathbf{b}_j = (b_j(0), b_j(1), \cdots, b_j(M-1)) : 0 \le j \le M-1\}$ *be a set of* M *orthogonal sequences with period* M. *From each* $\mathbf{a}_i$ $(i \in I)$ *and* B, *one can obtain a sequence set*

$$C^i = \{\mathbf{c}_j^i = (c_j^i(0), c_j^i(1), \cdots, c_j^i(N-1)) : 0 \le j \le M-1\} \tag{8}$$

in which each $\mathbf{c}_j^i$ *is a sequence of period* N *defined by*

$$c_j^i(t) = a_i(t) b_j(t \bmod M),\ 0 \le t \le N-1.$$

It turns out in [20] that each C^i *is an* (N, M, L) *sequence set meeting the Tang-Fan-Matusufuji bound. Furthermore, according to Theorem 2 in [21], the cross-correlation between each*

sequence in C^{i_1} and each sequence in C^{i_2} ($i_1, i_2 \in I$) achieves the Sarwate bound. This observation is due to one of the anonymous reviews.

In [20], two interesting classes of modulation orthogonal sequences were chosen from the discrete Fourier transform (DFT) matrix and and the binary Hadamard sequences (See Section II of [20] for more details). In these two cases, the numerical data by Magma Program shows that there always exist cyclically equivalent sequences in each C^i for each period $N = ML$ with $6 \le N \le 200$ and $M \ge 3$. Two specific examples are given as follows.

Let $N = 9$, $M = 3$ and $L = 3$. Let the modulation orthogonal sequences be chosen from the DFT matrix of order M as

$$b_j(t) = \omega_M^{jt}, 0 \le j, t \le M-1.$$

Then the sequences in C^1 are given by

$$\mathbf{c}_0^1 = (\omega_9^0, \omega_9^1, \omega_9^3, \omega_9^6, \omega_9^1, \omega_9^6, \omega_9^3, \omega_9^1, \omega_9^0),$$

$$\mathbf{c}_1^1 = (\omega_9^0, \omega_9^4, \omega_9^0, \omega_9^6, \omega_9^4, \omega_9^3, \omega_9^3, \omega_9^4, \omega_9^6),$$

$$\mathbf{c}_2^1 = (\omega_9^0, \omega_9^7, \omega_9^6, \omega_9^6, \omega_9^7, \omega_9^0, \omega_9^3, \omega_9^7, \omega_9^3).$$

Note that $c_2^1(t) = w_9^3 c_1^1(t+3) = w_9^6 c_0^1(t+6)$ for all $0 \le t < 9$. Therefore all sequences in C^1 are cyclically equivalent and are essentially the same sequence.

Let $N = 8$, $M = 4$, and $L = 2$. Let the modulation orthogonal sequences be chosen from the binary Hadamard sequences as

$$b_n(j) = (-1)^{\sum_{l=0}^{e-1} n_l j_l}, \quad n, j = 0, 1, 2, \cdots, M-1, M = 2^e,$$

where n_l, j_l are the bits of the binary e-bits long binary representations of integers n and j. Then the sequences in C^1 are given by

$$\mathbf{c}_0^1 = (\omega_8^0, \omega_8^{\frac{1}{2}}, \omega_8^2, \omega_8^{\frac{9}{2}}, \omega_8^0, \omega_8^{\frac{9}{2}}, \omega_8^2, \omega_8^{\frac{1}{2}}),$$

$$\mathbf{c}_1^1 = (\omega_8^0, \omega_8^{\frac{9}{2}}, \omega_8^2, \omega_8^{\frac{1}{2}}, \omega_8^0, \omega_8^{\frac{1}{2}}, \omega_8^2, \omega_8^{\frac{9}{2}}),$$

$$\mathbf{c}_2^1 = (\omega_8^0, \omega_8^{\frac{1}{2}}, \omega_8^6, \omega_8^{\frac{1}{2}}, \omega_8^0, \omega_8^{\frac{9}{2}}, \omega_8^6, \omega_8^{\frac{9}{2}}),$$

$$\mathbf{c}_3^1 = (\omega_8^0, \omega_8^{\frac{9}{2}}, \omega_8^6, \omega_8^{\frac{9}{2}}, \omega_8^0, \omega_8^{\frac{1}{2}}, \omega_8^6, \omega_8^{\frac{1}{2}}).$$

It is easily seen that $\mathbf{c}_0^1$ and $\mathbf{c}_1^1$ are cyclically equivalent, and $\mathbf{c}_2^1$ and $\mathbf{c}_3^1$ are also cyclically equivalent.

Therefore an interesting problem is to study how to select the orthogonal sequences $\mathbf{b}_i$ such that all the resultant ZCZ sequences from the construction in [20] can be mathematically proven to be cyclically distinct.

Remark 4. *Note that there is a one-to-one correspondence between complex roots of unity sequences of period N with perfect autocorrelation and perfect nonlinear functions over the cyclic group $\mathbb{Z}_N$. For the PNFs in Lemma 3, where $\pi(x) = x$ and $\sigma(x) = 0$ for any $x \in \mathbb{Z}_p$, the corresponding sequence is the well-known Frank-Zadoff sequence [11, 14] of period p^2 with perfect autocorrelation. However, this class of PNFs does not meet the conditions on π and σ in Construction 1 and cannot lead to multiple ZCZ sequence sets in which any two sequences are cyclically inequivalent. However, the interpretation of Frank-Zadoff sequences in terms of PNFs motivates us to utilize PNFs in Lemma 5 to obtain the desirable multiple ZCZ sequence*

sets. This interpretation also convert the problem of finding inequivalent ZCZ sequences to the one of searching two suitable permutations meeting the conditions in Construction 1. An infinite family of such permutations does exist as shown by Lemma 7.

It may be possible to address the equivalent problem of ZCZ sequences in [20] from the viewpoint of perfect nonlinear functions under the framework developed in this paper. This would be one of our future work. The reader is also kindly invited to join this adventure.

4 Concluding remarks

In this paper, we proposed a method to construct multiple optimal ZCZ sequence sets with favorable inter-set cross-correlation property from perfect nonlinear functions. It would be possible and interesting to obtain more multiple ZCZ sequence sets with good properties from other known perfect nonlinear functions. One of our future work is to combine the method from the view point of perfect nonlinear functions and the construction in [20] to get multiple optimal ZCZ sequences in other parameter regimes such that all sequences are pairwise cyclically distinct.

Acknowledgments

The authors are very grateful to the reviewers and the Associate Editor, Prof. Sihem Mesnager, for their valuable comments that improved the presentation and quality of this paper. Special thanks go to one of the reviewers for pointing out the construction based on Zadoff-Chu sequences in [20] can be extended to obtain multiple ZCZ sequences meeting the Sarwate bound.

References

[1] R. Appuswamy and A. K. Chaturvedi, "A new framework for constructing mutually orthogonal complementary sets and ZCZ sequences," *IEEE Trans. Inform. Theory*, vol. 52, no. 8, pp. 3817-3826, 2006.

[2] C. Carlet, C. Ding, and J. Yuan, "Linear codes from highly nonlinear functions and their secret sharing schemes," *IEEE Trans. Inform Theory*, vol. 51, no. 6, pp. 2089-2102, 2005.

[3] C. Carlet and C. Ding, "Highly nonlinear mappings," *J. Complexity*, vol. 20, no. 2, pp. 205–244, Apr. 2004.

[4] D. C. Chu, "Polyphase codes with good periodic correlation properties," *IEEE Trans. Inform. Theory,* vol. IT-18, pp. 531-532, July 1972.

[5] J. D. Coker, and A. H. Tewfik, "Simplified ranging systems using discrete wavelet decomposition," *IEEE Trans. Signal Process.*, vol. 58, no. 2, pp. 575-582, 2010.

[6] C. Ding, M. J. Moisio, and J. Yuan, "Algebraic constructions of optimal frequency-hopping sequences," *IEEE Trans. Inform. Theory*, vol. 53, no. 7, pp. 2606-2610, 2007.

[7] C. Ding and H. Niederreiter, "Systematic authentication codes from highly nonlinear functions," *IEEE Trans. Inform Theory*, vol. 50, no. 10, pp. 2421–2428, 2004.

[8] X. M. Deng and P. Z. Fan, “Spreading sequence sets with zero correlation zone,” *Electron. Letters,* vol. 36, no. 11, pp. 993-994, 2000.

[9] P. Z. Fan and L. Hao,“Generalized orthogonal sequences and their applications in synchronous CDMA systems," *IEICE Trans. Fundam.*, vol. 83, no. 11, pp. 2054-2069, Nov. 2000.

[10] P. Z. Fan, “Spreading sequence design and theoretical limits for quasisynchronous CDMA systems," *EURASIP J. Wireless Commun. Netw.,* vol. 2004, no. 1, pp. 19-31, 2004.

[11] R. L. Frank and S. A. Zadoff, “Phase shift pulse codes with good periodic correlation properties,” *IEEE Trans. Inform. Theory*, vol. IT-4, pp. 381 - 382, Oct. 1962.

[12] G. Gong, “Constructions of multiple shift-distinct signal sets with low correlation,” *Proc.2007 IEEE Intl. Symp. Inf. Theory (ISIT 2007)*, pp. 2306-2310, Nice, France, Jun. 2007.

[13] S. W. Golomb and G. Gong, Signal Designs With Good Correlation: For Wireless Communications, Cryptography and Radar Applications. Cambridge, U.K.: Cambridge University Press, 2005.

[14] R. C. Heimiller, “Phase shift pulse codes with good periodic correlation properties,” *IRE Trans. Inform. Theory*, vol. IT-7, pp. 245 - 257, Oct. 1961.

[15] K. M. Islam, T. Y. Al-Naffouri, and N. A. Dhahir, “On optimum pilot design for comb-type OFDM transmission over doubly-selective channels,” *IEEE Trans. Communications*, vol. 59, no. 4, pp. 930-935, 2011.

[16] P. V. Kumar, R. A. Scholtz, and L. R. Welch, “Generalized bent functions and their properties,” *J. Combin. Theory Ser. A,* vol. 40, no. 1, pp. 90-107, Sept. 1985.

[17] J. Li, J. Fan, and X.H. Tang, “A generic construction of generalized chirp-like sequence sets with optimal zero correlation property," *IEEE Communications Letters*, vol. 17, no. 3, pp. 549-552, 2013.

[18] Y. C. Liu, C. W. Chen, and Y. T. Su, “New constructions of zero-correlation zone sequences,” *IEEE Trans. Inform. Theory*, vol. 59, no. 8, pp. 4994-5007, 2013.

[19] K. Nyberg, “Differentially uniform mappings for cryptography,” in: Advances in Cryptography? Eurocrypt93, Lecture Notes in Computer Science, Vol. 765, Springer, New York, pp. 55-64, 1994.

[20] B. M. Popovic and O. Mauritz, “Generalized chirp-like sequences with zero correlation zone," *IEEE Trans. Inform. Theory,* vol. 56, no. 6, pp. 2957-2960, June 2010.

[21] B. M. Popovic, “Generalized chirp-like polyphase sequences with optimum correlation properties” *IEEE Trans. Inform. Theory*, vol. 38, no. 4, pp. 1406-1409, July 1992.

[22] D. Sarwate, “Bounds on crosscorrelation and autocorrelation of sequences,” *IEEE Trans. Inform. Theory*, vol. IT-25, no. 6, pp. 720 - 724, Nov. 1979.

[23] X. H. Tang, P. Z. Fan, and S. Matsufuji, “Lower bounds on correlation of spreading sequence set with low or zero correlation zone," *Electron. Lett,* vol. 36, pp. 551-552, Mar. 2000.

[24] X. H. Tang and W. H. Mow, "Design of spreading codes for quasi-synchronous CDMA with intercell interference," *IEEE J. Sel. Areas Commun.,* vol. 24, no. 1, pp. 84-93, Jan. 2006.

[25] X. H. Tang and W. H. Mow, "A new systematic construction of zero correlation zone sequences based on interleaved perfect sequences," *IEEE Trans. Inform. Theory,* vol. 54, no. 12, pp. 5279-5734, Dec. 2008.

[26] X. H. Tang, P. Z. Fan, and J. Lindner, "Multiple binary ZCZ sequence sets with good cross-correlation property based on complementary sequence sets," *IEEE Trans. Inform. Theory,* vol. 56, no. 8, pp. 4038-4045, Aug. 2010.

[27] H. Torii, M. Nakamura, and N. Suehiro, "A new class of zero-correlation zone sequences," *IEEE Trans. Inform. Theory,* vol. 50, no. 3, pp. 559-565, Mar. 2004.

[28] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inform. Theory*, vol. 20, no. 3, pp. 397-399, May 1974.

[29] K. Yang, Y. K. Kim and P. V. Kumar, "Quasi-orthogonal sequences for code-division multiple-access systems," *IEEE Trans. Inform. Theory*, vol. 46, no. 3, pp. 982-993, 2000.

[30] J. D. Yang, X. Jin, K. Y. Song, J. S. No and D. J. Shin, " Multicode MIMO systems with quaternary LCZ and ZCZ sequences," *IEEE Trans. Vehicular Technology*, vol. 57, no. 4, pp. 2334-2341, 2008.

[31] Z. C. Zhou, X. H. Tang, and G. Gong, "A new class of sequences with zero or low correlation zone based on interleaving technique," *IEEE Trans. Inform. Theory,* vol. 54, no. 9, pp. 4267-4273, 2008.

Authors' Biographies

Zhengchun Zhou

Zhengchun Zhou received the B.S. and M.S. degrees in mathematics and the Ph.D. degree in information security from Southwest Jiaotong University, Chengdu, China, in 2001, 2004, and 2010, respectively. From 2012 to 2013, he was a postdoctoral member in the Department of Computer Science and Engineering, the Hong Kong University of Science and Technology. From 2013 to 2014, he was a research associate in the Department of Computer Science and Engineering, the Hong Kong University of Science and Technology. Since 2001, he has been in the Department of Mathematics, Southwest Jiaotong University, where he is currently a professor. His research interests include sequence design, Boolean function, coding theory, and compressed sensing.

Dr. Zhou was the recipient of the National excellent Doctoral Dissertation award in 2013 (China).

Dan Zhang

Dan Zhang received the B.S. and M.S. degrees in mathematics from Henan University, Kaifeng, China, in 2011 and 2014 respectively. From Sept. 2012 to June 2014, she was a visiting student in the Academy of Mathematics and System Science, Chinese Academy of Sciences, China.

She is currently a Ph.D. student in the Department of Informatics at the University of Bergen, Norway. Her research interests lie in sequence design, Boolean function, coding theory, and quantum computers.

Tor Helleseth

Tor Helleseth (M'89-SM'96-F'97) received the Cand. Real. and Dr. Philos. degrees in mathematics from the University of Bergen, Bergen, Norway, in 1971 and 1979, respectively. From 1973 to 1980, he was a Research Assistant at the Department of Mathematics, University of Bergen. From 1981 to 1984, he was at the Chief Headquarters of Defense in Norway. Since 1984, he has been a Professor in the Department of Informatics at the University of Bergen. During the academic years 1977-1978 and 1992-1993, he was on sabbatical leave at the University of Southern California, Los Angeles, and during 1979-1980, he was a Research Fellow at the Eindhoven University of Technology, Eindhoven, The Netherlands. His research interests include coding theory and cryptology. Prof. Helleseth served as an Associate Editor for Coding Theory for IEEE TRANSACTIONS ON INFORMATION THEORY from 1991 to 1993. He was Program Chairman for Eurocrypt'93 and for the Information Theory Workshop in 1997 in Longyearbyen, Norway. He was a Program Co-Chairman for SETA04 in Seoul, Korea, and SETA06 in Beijing, China. He was also a Program Co-Chairman for the IEEE Information Theory Workshop in Solstrand, Norway in 2007. During 2007-2009 he served on the Board of Governors for the IEEE Information Theory Society. In 1997 he was elected an IEEE Fellow for his contributions to coding theory and cryptography. In 2004 he was elected a member of Det Norske Videnskaps-Akademi.

Jinming Wen

Jinming Wen received his Bachelor degree in Information and Computing Science from Jilin Institute of Chemical Technology, Jilin, China, in 2008, his M.Sc. degree in Pure Mathematics from the Mathematics Institute of Jilin University, Jilin, China, in 2010, and his Ph.D degree in Applied Mathematics from McGill University, Montreal, Canada, in 2015. He was a postdoctoral research fellow at Laboratoire LIP, ENS de Lyon and University of Alberta from March 2015 to August 2017. Since September 2017, he is a postdoctoral research fellow at department of Electrical and Computer Engineering, University of Toronto. His research interests are in the areas of lattice reduction with applications in communications, signal processing and cryptography, and sparse recovery. He is an associate editor of IEEE Access.

Paper VI

3.6 Polyphase zero correlation zone sequences from generalised bent functions

Dan Zhang, Matthew Geoffrey Parker, and Tor Helleseth
Cryptogr. Commun., 12, 325–335 (2020)

Polyphase Zero Correlation Zone Sequences from Generalised Bent Functions

Dan Zhang
email: dan.zhang@uib.no

Matthew Geoffrey Parker
email: wangsungi@gmail.com

Tor Helleseth
email: tor.helleseth@uib.no

Abstract

Sequence families with zero correlation zone (ZCZ) have been extensively studied in recent years due to their important applications in quasi-synchronous code-division multiple-access (QS-CDMA) systems. To accommodate multiuser environments, multiple ZCZ sequence sets with low inter-set cross-correlation are expected. In this paper, we propose a construction of polyphase ZCZ sequences based on generalised bent functions. Moreover, multiple polyphase ZCZ sequence sets with good inter-set cross-correlation are presented. Each generated ZCZ sequence set is optimal with respect to the Tang-Fan-Matsufuji bound.

***Index terms*—** quasi-synchronous code-division multiple-access (QS-CDMA), zero correlation zone (ZCZ), sequences, perfect autocorrelation, orthogonal sequences.

1 Introduction

To implement an interference-free asynchronous code-division multiple-access (A-CDMA) communication system, one would like to have an *ideal periodic sequence set*, where the out-of-phase autocorrelation (AC) of each sequence is zero and the cross-correlation (CC) of any pair of sequences at any shift is also zero. Unfortunately, such an ideal sequence set does not exist according to the Welch bound [23] or the Sawarte bound [17]. It is therefore impossible to have sequences which have simultaneously impulse-like AC and zero CC during an entire period. However, for QS-CDMA systems, a time delay is allowed between the signals of different users within a few shifts. To utilize this advantage, a new class of sequences having impulse-like AC and zero CC in some smaller zone around the origin (called the zero-correlation zone), was introduced to eliminate both multiple access interference and multipath interference in such a system [3, 6]. Sequences with such properties are known as Zero Correlation Zone (ZCZ) sequences. A ZCZ sequence set is generally characterized by the sequence period, the size of the set, the length of the ZCZ and the number of phases of the sequence elements. To accommodate multiple access users and to ease the synchronization requirement, it is desirable to have a ZCZ sequence set with the set size and the ZCZ length as large as possible for any given period. However, the Tang-Fan-Matsufuji bound [20] implies that there is a tradeoff between the set size and the ZCZ length for any given sequence period. ZCZ sequence sets are said to be optimal if they meet this bound. A number of studies on optimal ZCZ sequence sets have been reported in the literature ([5, 6, 14, 15, 19, 22]).

To resist inter-cell interference caused by users from different cells in CDMA systems, a concept of intraference among sequences was introduced in [9, 24], which is referred to as the inter-set cross-correlation of multiple sequence sets. Facing the same challenge in the design of ZCZ sequences, it is expected to construct multiple ZCZ sequence sets with low inter-set cross-correlation. This would allow us to extend the application of ZCZ sequences in multiuser environments [19]. Some progress on the construction of multiple ZCZ sequence sets has been made in recent years. Mutually orthogonal binary ZCZ sequence sets from mutually orthogonal complementary sequence sets (MOCSS) and orthogonal matrices were constructed in [1]. Tang and Mow presented systematic constructions of generalized loosely synchronized codes with low intercode cross-correlation properties within a certain window [19]. Later, multiple ZCZ sequence sets from some specific families of MOCSS were generated in [18]. Recently, Tang and Li [12] obtained quaternary multiple sets with low correlation based on Zadoff-Chu sequences. Very recently, [13] and [25] presented multiple ZCZ sequence sets with good inter-set cross-correlation from discrete Fourier transform matrices and perfect nonlinear functions, respectively. According to the requirements in [25], the construction in [13] may lead to equivalent sequences.

In this paper, we employ generalised bent functions to construct optimal polyphase ZCZ sequence sets. Some conditions are derived under which all the ZCZ sequences generated by our construction are cyclically distinct (meaning that one sequence cannot be obtained by taking a cyclic shift of another). Moreover, we propose a general construction of multiple ZCZ sequence sets. To implement this general construction, we need a set of permutations satisfying some given properties. Given such a permutation set, we derive $p_{min} - 1$ multiple optimal polyphase ZCZ sequence sets with good inter-set cross-correlation in the sense that the maximum inter-set cross-correlation of multiple sequence sets achieves the Sarwate bound [17], where p_{min} is the smallest prime divisor of the period of the sequences. Our construction includes some previous results as a special case [25].

The paper is organised as follows. We give some preliminaries and useful notation in Sect. 2. In Sect. 3, we obtain optimal polyphase ZCZ sequence sets from generalised bent functions. In Sect. 4, we present a generic construction of multiple polyphase ZCZ sequence sets with good inter-set cross-correlation. An example is presented to illustrate our main results in Sect. 5. Finally, we give some concluding remarks.

2 Preliminaries

We denote the ring of integers modulo N by $\mathbb{Z}_N$, where N is a positive integer. Denote by $\langle x \rangle_N$ the remainder x mod N for any integer x. Let $\mathbf{u} = \{u(t)\}_{t=0}^{N-1}$ and $\mathbf{v} = \{v(t)\}_{t=0}^{N-1}$ be two complex sequences of period N. The (periodic) *cross-correlation* (CC) of $\mathbf{u}$ and $\mathbf{v}$ at shift τ is defined as

$$R_{\mathbf{u},\mathbf{v}}(\tau) = \sum_{t=0}^{N-1} u(t+\tau)v^*(t), \quad 0 \le \tau < N,$$

where $t + \tau$ is taken modulo N and x^* is the complex conjugate of the complex number x. When $\mathbf{u} = \mathbf{v}$, $R_{\mathbf{u},\mathbf{u}}(\tau)$ is called the *auto-correlation* (AC) of $\mathbf{u}$, or $R_{\mathbf{u}}(\tau) = R_{\mathbf{u},\mathbf{u}}(\tau)$ for short. A sequence $\mathbf{u}$ is said to be *perfect* if $R_{\mathbf{u}}(\tau) = 0$ for all $0 < \tau < N$.

Let $\mathcal{S} = \{\mathbf{s}_m,\ 0 \le m < M\}$ be a set of M sequences of period N. The maximum out-of-phase periodic auto-correlation magnitude is denoted by R_a and defined by

$$R_a = \max\{|R_{\mathbf{s}_i}(\tau)| : \mathbf{s}_i \in \mathcal{S}, 0 < \tau < N\}.$$

The maximum periodic cross-correlation magnitude is denoted by R_c and defined by

$$R_c = \max\{|R_{\mathbf{s}_i,\mathbf{s}_j}(\tau)| : \mathbf{s}_i \neq \mathbf{s}_j \in \mathcal{S}, 0 \leq \tau < N\}.$$

The following lemma is the well-known Sarwate bound on R_a and R_c. The set $\mathcal{S}$ is said to be *optimal* if R_a and R_c meet the bound.

Lemma 1. *[17] For any sequence set $\mathcal{S}$ with M sequences of period N,*

$$\frac{R_c^2}{N} + \frac{N-1}{N(M-1)}\frac{R_a^2}{N} \geq 1.$$

Lemma 1 implies that it is impossible to have sequences which have simultaneously impulse-like AC and zero CC during an entire period. However, sets of sequences satisfying both of these properties in some smaller zone around the origin do exist, and they are called ZCZ sequence sets.

Definition 1. *Let $\mathcal{S} = \{\mathbf{s}_m = \{s_m(t)\}_{t=0}^{N-1},\ 0 \leq m < M\}$ be a set of M sequences of period N. The set $\mathcal{S}$ is called an* (N, M, Z_{cz})-ZCZ sequence set *if*

$$R_{\mathbf{s}_i,\mathbf{s}_j}(\tau) = 0 \ \textit{for}\ (0 < |\tau| < Z_{cz})$$

and

$$R_{\mathbf{s}_i,\mathbf{s}_j}(\tau) = 0 \ \textit{for}\ (\tau = 0 \ \textit{and}\ i \neq j),$$

where Z_{cz} is called the length of the zero correlation zone.

The following lemma shows that the length of the ZCZ is upper bounded by a value depending on the sequence period and the size of the sequence set. Any sequence set meeting this bound is called an *optimal ZCZ set*.

Lemma 2. *[20] Let $\mathcal{S}$ be an (N, M, Z_{cz})-ZCZ sequence set. Then*

$$MZ_{cz} \leq N.$$

Let q and m be positive integers and ω_q be a primitive q-th root of unity. Let $\mathbb{Z}_q^m$ denote the set of all m-tuples of elements from $\mathbb{Z}_q$. A function $f : \mathbb{Z}_q^m \to \mathbb{Z}_q$ is called a *generalised bent function* (GBF) if all of the complex Fourier coefficients $F_f(\lambda)$ defined by

$$F_f(\lambda) = \frac{1}{\sqrt{q^m}} \sum_{x \in \mathbb{Z}_q^m} \omega_q^{f(x)-\lambda^T x}, \lambda \in \mathbb{Z}_q^m$$

have unit magnitude. The integer m is the *dimension* of the generalised bent function.

Bent functions are a highly active area of research due to their numerous applications in information theory, cryptography and coding theory. Research on GBFs started with the work of Rothaus [16] and Dillon [4], initially focussing on the binary case. Later, Kumar et al. [11] defined generalised bent functions as the maps from $\mathbb{Z}_q^m$ to $\mathbb{Z}_q$. A survey of GBFs and related objects is given in [21]. One known class of GBFs that will be used in our constructions is as follows.

Lemma 3. *[11] Let N be a positive integer. The function over $\mathbb{Z}_{N^2}$ given by*

$$f(t) = N \cdot t_2\pi(t_1) + \sigma(t_1),\ \ 0 \leq t < N^2,$$

where $t = t_1 + t_2 \cdot N$, $0 \leq t_1, t_2 < N$, π is an arbitrary permutation over $\mathbb{Z}_N$, and σ is an arbitrary function on $\mathbb{Z}_N$, is bent.

When N is an odd prime, the function f above is a perfect non-linear function [2], which corresponds to the well-known Frank-Zadoff sequence [7, 10]. Multiple ZCZ sequence sets based on this perfect nonlinear function were presented in [25]. In this paper, we will employ the GBFs in Lemma 3 to construct multiple optimal ZCZ sequences with some desirable properties, which generalise some results in [25].

3 Optimal ZCZ sequence set

For any rational function h, one can get its corresponding polyphase sequence by the map

$$h(k) \mapsto exp(2\pi\sqrt{-1}h(k)/N), \ \ \forall k \in \mathbb{Z}_N, \ h(k) \in R,$$

where h is called an index sequence of period N. The corresponding polyphase sequence is denoted by $\mathbf{s}$. From the properties of the Fourier transform, it is easy to show that

$$|F_h(\lambda)| = 1, \ \forall \lambda \in \mathbb{Z}_q^m \iff R_{\mathbf{s}}(\tau) = 0, \ \forall \tau \in \mathbb{Z}_N^*,$$

where $\mathbb{Z}_N^* = \mathbb{Z}_N \setminus \{0\}$. Thus, a GBF in fact corresponds to a perfect polyphase sequence. In particular, the perfect sequences induced by the GBFs in Lemma 3 are known as generalised Frank sequences [11]. Our construction of ZCZ sequence sets based on the GBFs in Lemma 3 is as follows.

Construction 1. *Let π and σ be permutations over $\mathbb{Z}_N$ such that there exist no c_1 and c_2 in $\mathbb{Z}_N^*$ satisfying $c_1 \cdot \pi(t_1) + c_2 \cdot \sigma(t_1) = 0$. A sequence set is defined as*

$$\mathcal{S} = \{\mathbf{s}_n \mid \mathbf{s}_n = \omega_N^{\pi(t_1)\cdot t_2 + n\cdot\sigma(t_1)}, 0 \le n < N\},$$

where $t = t_1 + t_2 \cdot N$ and $0 \le t_1, t_2 < N$.

Note that cyclically equivalent sequences are not desirable in practical applications [8]. Thus, it is important to ensure that all the sequences in the constructed set are cyclically distinct. Before doing so, we introduce the following notation. For any shift $0 \le \tau < N^2$, we write $\tau = \tau_1 + \tau_2 \cdot N$, where $0 \le \tau_1, \tau_2 < N$, and define

$$\delta_{t_1,\tau_1} = \begin{cases} 0 & \text{if } t_1 + \tau_1 < N, \\ 1 & \text{if } t_1 + \tau_1 \ge N. \end{cases}$$

Lemma 4. *All the sequences in $\mathcal{S}$, given in Construction 1, are cyclically distinct.*

Proof. Let $\mathbf{s}_{n_1}$ and $\mathbf{s}_{n_2}$ be two sequences in $\mathcal{S}$, where $0 \le n_1 \ne n_2 < N$. Assume on the contrary that they are cyclically shift equivalent, then there exists some integer $0 \le \tau < N^2$ such that

$$s_{n_1}(t) = s_{n_2}(t + \tau)$$

for all $0 \le t < N^2$. In other words,

$$\pi(t_1) \cdot t_2 + n_1 \cdot \sigma(t_1) \equiv \pi(t_1 + \tau_1) \cdot (t_2 + \tau_2 + \delta_{t_1,\tau_1}) + n_2 \cdot \sigma(t_1 + \tau_1) \mod N \qquad (1)$$

for all $0 \le t_1, t_2 < N$.

Case i) $\tau_1 \ne 0$: Equation (1) can be written as

$$(\pi(t_1) - \pi(t_1 + \tau_1)) \cdot t_2 - \pi(t_1 + \tau_1) \cdot (\tau_2 + \delta_{t_1,\tau_1}) - n_2 \cdot \sigma(t_1 + \tau_1) + n_1 \cdot \sigma(t_1) \equiv 0 \mod N,$$

which cannot be simultaneously satisfied for all $0 \le t_2 < N$ given a fixed t_1 due to $\langle \pi(t_1+\tau_1) - \pi(t_1)\rangle_N \neq 0$.

Case ii) $\tau_1 = 0$ and $\tau_2 = 0$: Equation (1) yields $(n_2 - n_1) \cdot \sigma(t_1) \equiv 0 \mod N$, which is impossible for all $0 \le t_1 < N$ because $n_1 \neq n_2$ and $\sigma(t_1)$ is a permutation over $\mathbb{Z}_N$.

Case iii) $\tau_1 = 0$ and $\tau_2 \neq 0$: Equation (1) becomes $\pi(t_1) \cdot \tau_2 + (n_2 - n_1) \cdot \sigma(t_1) \equiv 0 \mod N$, which is impossible for all $0 \le t_1 < N$, since there exist no c_1 and c_2 in $\mathbb{Z}_N^*$ satisfying $c_1 \cdot \pi(t_1) + c_2 \cdot \sigma(t_1) = 0$.

Therefore, $\mathbf{s}_{n_1}$ and $\mathbf{s}_{n_2}$ are cyclically distinct. □

The above lemma ensures that the set $\mathcal{S}$ by Construction 1 contains N cyclically distinct sequences. Now we are ready to show that the generated set $\mathcal{S}$ is an optimal ZCZ sequence set.

Theorem 1. *The sequence set $\mathcal{S}$ given by Construction 1 is an optimal (N^2, N, N)-ZCZ sequence set.*

Proof. Since every sequence is based on the generalised bent function in Lemma 3, each sequence in the set is perfect in the sense that out-of-phase auto-correlation is 0. The cross-correlation function of $s_{n_1}(t)$ and $s_{n_2}(t)$ for $0 \le n_1 \neq n_2 < N$ at shift τ is

$$\begin{aligned} R_{\mathbf{s}_{n_1},\mathbf{s}_{n_2}}(\tau) &= \sum_{t_1=0}^{T-1} s_{n_1}(t+\tau) s_{n_2}^*(t) \\ &= \sum_{t_1=0}^{N-1} \sum_{t_2=0}^{N-1} \omega_N^{\pi(t_1+\tau_1)\cdot(t_2+\tau_2+\delta_{t_1,\tau_1}) - \pi(t_1)\cdot t_2 + n_1\cdot\sigma(t_1+\tau_1) - n_2\cdot\sigma(t_1)} \\ &= \sum_{t_1=0}^{N-1} \omega_N^{\pi(t_1+\tau_1)\cdot(\tau_2+\delta_{t_1,\tau_1}) + n_1\cdot\sigma(t_1+\tau_1) - n_2\cdot\sigma(t_1)} \sum_{t_2=0}^{N-1} \omega_N^{(\pi(t_1+\tau_1)-\pi(t_1))\cdot t_2}. \end{aligned} \tag{2}$$

Case i) $\tau_1 \neq 0$: Because $\pi(t_1)$ is a permutation over $\mathbb{Z}_N$, $\langle \pi(t_1+\tau_1) - \pi(t_1)\rangle_N \neq 0$ for $\tau_1 \neq 0$, which means that the inner sum of the last line in (2) is 0. Then $R_{\mathbf{s}_{n_1},\mathbf{s}_{n_2}}(\tau) = 0$ for $\tau_1 \neq 0$.

Case ii) $\tau = 0$: Then $\tau_1 = \tau_2 = 0$. It then follows from (2) that

$$R_{\mathbf{s}_{n_1},\mathbf{s}_{n_2}}(\tau) = N \cdot \sum_{t_1=0}^{N-1} \omega_N^{(n_1-n_2)\cdot\sigma(t_1)}$$

which is 0 since $\sigma(t_1)$ is a permutation over $\mathbb{Z}_N$ and $n_1 \neq n_2$.

Combining the above two cases, the sequence set $\mathcal{S}$ can be seen to be an (N^2, N, N)-ZCZ sequence set which is optimal with respect to the Tang-Fan-Matsufuji bound. □

By Theorem 1, the set $\mathcal{S}$ in Construction 1 produces sequences with zero AC across all out-of-phase shifts and nonzero CC only at sub-periodic correlation shifts. Based on the set $\mathcal{S}$, we will generate multiple optimal ZCZ sequence sets with good inter-set cross-correlation in the next section.

4 Multiple ZCZ sequence sets

In this section, we present multiple ZCZ sequence sets based on Construction 1. To get multiple sets, we need a set of permutations over $\mathbb{Z}_N$ satisfying certain conditions instead of a

single permutation π as in Construction 1. We first propose a general construction of multiple ZCZ sequence sets. After that, we show that a set of permutations over $\mathbb{Z}_N$ with the specific properties in Construction 2 does exist.

Construction 2. *Let N be a positive integer and σ be a permutation over $\mathbb{Z}_N$. We denote $\Pi = \{\pi_m \mid \pi_m$ is a permutation over $\mathbb{Z}_N$ for $m \in \mathcal{M}\}$, where $\mathcal{M}$ is an index set. For each $m \in \mathcal{M}$, we define a sequence set as*

$$\mathcal{S}^m = \{\mathbf{s}_n^m \mid \mathbf{s}_n^m(t) = \omega_N^{\pi_m(t_1)\cdot t_2 + n\cdot\sigma(t_1)}, 0 \le n < N\},$$

where $t = t_1 + t_2 \cdot N$ and $0 \le t_1, t_2 < N$.

Theorem 2. *If the following requirements are satisfied:*

1 for each $m \in \mathcal{M}$, there exist no c_1 and c_2 in $\mathbb{Z}_N^*$ satisfying $c_1 \cdot \pi_m(t_1) + c_2 \cdot \sigma(t_1) = 0$;

2 $\pi_{m_1}(t_1 + \tau_1) \equiv \pi_{m_2}(t_1) \pmod N$ has only one solution for $\tau_1 \in \mathbb{Z}_N$ and $m_1 \ne m_2 \in \mathcal{M}$,

then the sets $\mathcal{S}^m$ from Construction 2 have the following properties:

a each sequence in each set $\mathcal{S}^m$ for $m \in \mathcal{M}$ is perfect;

b each set $\mathcal{S}^m$ for $m \in \mathcal{M}$ is an optimal (N^2, N, N)-ZCZ sequence set;

c $|R_{\mathbf{s}_{n_1}^{m_1}, \mathbf{s}_{n_2}^{m_2}}(\tau)| = N$ for all $0 \le \tau < N^2 - 1$, $0 \le n_1, n_2 < N$ and $m_1 \ne m_2 \in \mathcal{M}$.

Proof. Since each $\pi_m(t_1)$ is a permutation over $\mathbb{Z}_N$ for $m \in \mathcal{M}$, each sequence in each set $\mathcal{S}^m$ is perfect. By Lemma 4, condition 1) ensures that each set consists of inequivalent sequences. For $m \in \mathcal{M}$, each set $\mathcal{S}^m$ is an optimal (N^2, N, N)-ZCZ sequence set by Lemma 1.

Now we consider the inter-set cross-correlation of two sequences from different sets. Let $\mathbf{s}_{n_1}^{m_1}$ and $\mathbf{s}_{n_2}^{m_2}$ be two sequences in $\mathcal{S}^{m_1}$ and $\mathcal{S}^{m_2}$, respectively, where $0 \le n_1, n_2 < N$ and $m_1 \ne m_2 \in \mathcal{M}$. Then, the inter-set cross-correlation between $\mathbf{s}_{n_1}^{m_1}$ and $\mathbf{s}_{n_2}^{m_2}$ is given by

$$\begin{aligned}
R_{\mathbf{s}_{n_1}^{m_1}, \mathbf{s}_{n_2}^{m_2}}(\tau) &= \sum_{t=0}^{N^2-1} s_{n_1}^{m_1}(t+\tau) s_{n_2}^{m_2 *}(t) \\
&= \sum_{t_2=0}^{N-1} \sum_{t_1=0}^{N-1} \omega_N^{\pi_{m_1}(t_1+\tau_1)(t_2+\tau_2+\delta_{t_1,\tau_1}) + n_1\sigma(t_1+\tau_1) - \pi_{m_2}(t_1)t_2 - n_2\sigma(t_1)} \\
&= \sum_{t_1=0}^{N-1} \omega_N^{\pi_{m_1}(t_1+\tau_1)(\tau_2+\delta_{t_1,\tau_1}) + n_1\sigma(t_1+\tau_1) - n_2\sigma(t_1)} \sum_{t_2=0}^{N-1} \omega_N^{(\pi_{m_1}(t_1+\tau_1) - \pi_{m_2}(t_1))t_2}.
\end{aligned}$$

The inner sum of the last identity above is zero unless

$$\pi_{m_1}(t_1 + \tau_1) \equiv \pi_{m_2}(t_1) \mod N.$$

Since $\pi_{m_1}(t_1 + \tau_1) - \pi_{m_2}(t_1) \equiv 0 \pmod N$ has a unique solution at any shift $\tau_1 \in \mathbb{Z}_N$ for $m_1 \ne m_2 \in \mathcal{M}$, we have $|R_{\mathbf{s}_{n_1}^{m_1}, \mathbf{s}_{n_2}^{m_2}}(\tau)| = N$ for all $0 \le \tau < N^2 - 1$, $0 \le n_1, n_2 < N$ and $m_1 \ne m_2 \in \mathcal{M}$.

□

Remark 1. *Denote by $|\mathcal{M}|$ the cardinality of the set $\mathcal{M}$. By Construction 2, $|\mathcal{M}|$ multiple ZCZ sequence sets are derived. Each sequence in each set is perfect and each set is an optimal ZCZ sequence set. The magnitude of the inter-set cross-correlation between any two sequences from different sets at any shift is constant, which is optimal with respect to the Sarwate bound. Hence, an optimal set of size $|\mathcal{M}|$ of period N^2 can be derived if we select one sequence from each set $\mathcal{S}^m$ for $m \in \mathcal{M}$.*

In order to perform Construction 2, we need to find permutations π_m for $m \in \mathcal{M}$ and σ satisfying the requirements in Theorem 2. Once π_m for $m \in \mathcal{M}$ are fixed, we can choose a proper permutation σ over $\mathbb{Z}_N$ satisfying the condition 1). Therefore, how to produce permutations π_m for $m \in \mathcal{M}$ satisfying the second requirement of Theorem 2 is crucial for the construction. For convenience, we call a set of such permutations over $\mathbb{Z}_N$ *a permutation set*.

One easy approach to generate permutation sets over $\mathbb{Z}_N$ is as follows. Let p_{min} be the smallest prime divisor of N and π be any permutation over $\mathbb{Z}_N$. Then a set of permutations $\pi_m(t_1) = \pi(m \cdot t_1)$ for $1 \le m \le p_{min} - 1$ is a permutation set, which can be easily proved.

Another approach to generate new permutation sets is based on the known permutation sets. Let $N = KP$, where K and P are odd integers. Again p_{min} is the smallest prime divisor of N. We rewrite t_1 in the form of $t_3 + K \cdot t_4$, where $0 \le t_3 < K$ and $0 \le t_4 < P$. A set of functions on $\mathbb{Z}_N$ is defined as

$$\Pi = \{\pi_m \mid \pi_m(t_1) = K \cdot h(mt_4) + mg(t_3),\ 1 \le m \le p_{min} - 1\}, \tag{3}$$

where h is any permutation over $\mathbb{Z}_P$ and $\{m \cdot g(t_3),\ 1 \le m \le p_{min} - 1\}$ is a permutation set over $\mathbb{Z}_K$. The following lemma shows that Π is indeed a permutation set.

Lemma 5. *The set Π above is a set of permutations such that $\pi_{m_1}(t_1 + \tau_1) \equiv \pi_{m_2}(t_1) \pmod N$ has only one solution for any given $\tau_1 \in \mathbb{Z}_N$ and $1 \le m_1 \ne m_2 \le p_{min} - 1$.*

Proof. According to the definition in (3), the index set $\mathcal{M} = \{1, 2, \cdots, p_{min} - 1\}$. For any shift $0 \le \tau_1 < N$, we rewrite $\tau_1 = \tau_3 + K \cdot \tau_4$, where $0 \le \tau_3 < K$ and $0 \le \tau_4 < P$. Then for $m_1, m_2 \in \mathcal{M}$, we obtain

$$\pi_{m_1}(t_1 + \tau_1) - \pi_{m_2}(t_1) = K[h(m_1(t_4 + \tau_4 + \delta_{t_3,\tau_3})) - h(m_2t_4)] + m_1g(t_3 + \tau_3)) - m_2g(t_3),$$

where

$$\delta_{t_3,\tau_3} = \begin{cases} 0 & \text{if } t_3 + \tau_3 < N, \\ 1 & \text{if } t_3 + \tau_3 \ge N. \end{cases}$$

Note that $\langle \pi_{m_1}(t_1+\tau_1) - \pi_{m_2}(t_1) \rangle_N = 0$ implies $\langle \pi_{m_1}(t_1+\tau_1) - \pi_{m_2}(t_1) \rangle_K = 0$, which means $\langle m_1g(t_3 + \tau_3)) - m_2g(t_3) \rangle_K = 0$. Thus, it is easy to verify that $\langle \pi_{m_1}(t_1 + \tau_1) - \pi_{m_2}(t_1) \rangle_N = 0$ if and only if $\langle m_1g(t_3 + \tau_3)) - m_2g(t_3) \rangle_K = 0$ and $\langle h(m_1(t_4 + \tau_4 + \delta_{t_3,\tau_3})) - h(m_2t_4) \rangle_P = 0$.

For $m_1 = m_2 \in \mathcal{M}$, $\langle \pi_{m_1}(t_1 + \tau_1) - \pi_{m_2}(t_1) \rangle_N = 0$ if and only if $\tau_3 = 0$ and $\tau_4 = 0$, because g and h are permutations over $\mathbb{Z}_K$ and $\mathbb{Z}_P$, respectively. Therefore, $\tau_1 = 0$ which imply that $\pi_m(t_1)$ is a permutation over $\mathbb{Z}_N$ for each $m \in \mathcal{M}$.

For $m_1 \ne m_2 \in \mathcal{M}$, $\langle h(m_1(t_4 + \tau_4 + \delta_{t_3,\tau_3})) - h(m_2t_4) \rangle_P = 0$ if and only if $m_1(t_4 + \tau_4 + \delta_{t_3,\tau_3}) \equiv m_2t_4 \mod P$, because h is a permutation over $\mathbb{Z}_P$. Furthermore, $m_1(t_4 + \tau_4 + \delta_{t_3,\tau_3}) \equiv m_2t_4 \mod P$ has one unique solution for every $\tau_4 \in \mathbb{Z}_P$, because $\gcd(m_1 - m_2, P) = 1$. Since $\{m \cdot g(t_3),\ 1 \le m \le p_{min} - 1\}$ is a permutation set over $\mathbb{Z}_K$, $\langle m_1g(t_3 + \tau_3)) - m_2g(t_3) \rangle_K = 0$ has one unique solution for every $\tau_3 \in \mathbb{Z}_K$. Hence, $\pi_{m_1}(t_1 + \tau_1) - \pi_{m_2}(t_1) = 0$ has exactly one solution for every shift $\tau_1 \in \mathbb{Z}_N$ and $m_1 \ne m_2 \in \mathcal{M}$. □

We can use permutation sets generated above to construct multiple ZCZ sequence sets by Construction 2. The size of the generated permutation sets is $p_{min} - 1$, where p_{min} is the smallest prime divisor of N. Therefore, we can get $p_{min} - 1$ multiple optimal ZCZ sequence sets with good inter-set cross-correlation. As we can see that the size of a permutation set determines how many different multiple sets we can obtain, it would be interesting to construct other forms of permutation sets with a larger set size.

5 Example

In this section, we give an example to illustrate Construction 2. We first choose a permutation set, after which we find a permutation σ satisfying the condition 1) in Theorem 2. With these permutations, we perform Construction 2 in the following.

Example 1. *Let $N = 15$ with $K = 5$ and $P = 3$. The permutation set $\Pi = \{\pi_m \mid \pi_m(t_1) = K \cdot h(mt_4) + mg(t_3),\ 0 < m \leq 2\}$, where $h(x) = x$ and $g(x) = x^3$. Let $\sigma(x) = x$. By Construction 2, we can obtain 2 sequence sets of which the first two sequences in each set are as follows:*

$\mathbf{s}_0^1$ ={0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 3, 2, 4, 5, 6, 8, 7, 9, 10, 11, 13, 12, 14, 0, 2, 6, 4, 8, 10, 12, 1, 14, 3, 5, 7, 11, 9, 13, 0, 3, 9, 6, 12, 0, 3, 9, 6, 12, 0, 3, 9, 6, 12, 0, 4, 12, 8, 1, 5, 9, 2, 13, 6, 10, 14, 7, 3, 11, 0, 5, 0, 10, 5, 10, 0, 10, 5, 0, 5, 10, 5, 0, 10, 0, 6, 3, 12, 9, 0, 6, 3, 12, 9, 0, 6, 3, 12, 9, 0, 7, 6, 14, 13, 5, 12, 11, 4, 3, 10, 2, 1, 9, 8, 0, 8, 9, 1, 2, 10, 3, 4, 11, 12, 5, 13, 14, 6, 7, 0, 9, 12, 3, 6, 0, 9, 12, 3, 6, 0, 9, 12, 3, 6, 0, 10, 0, 5, 10, 5, 0, 5, 10, 0, 10, 5, 10, 0, 5, 0, 11, 3, 7, 14, 10, 6, 13, 2, 9, 5, 1, 8, 12, 4, 0, 12, 6, 9, 3, 0, 12, 6, 9, 3, 0, 12, 6, 9, 3, 0, 13, 9, 11, 7, 5, 3, 14, 1, 12, 10, 8, 4, 6, 2, 0, 14, 12, 13, 11, 10, 9, 7, 8, 6, 5, 4, 2, 3, 1, 0}.

$\mathbf{s}_1^1$ ={1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 0, 2, 5, 5, 8, 10, 12, 0, 0, 3, 5, 7, 10, 10, 13, 0, 3, 8, 7, 12, 0, 3, 8, 7, 12, 0, 3, 8, 7, 12, 0, 4, 11, 9, 1, 5, 9, 1, 14, 6, 10, 14, 6, 4, 11, 0, 5, 14, 11, 5, 10, 0, 9, 6, 0, 5, 10, 4, 1, 10, 0, 6, 2, 13, 9, 0, 6, 2, 13, 9, 0, 6, 2, 13, 9, 0, 7, 5, 0, 13, 5, 12, 10, 5, 3, 10, 2, 0, 10, 8, 0, 8, 8, 2, 2, 10, 3, 3, 12, 12, 5, 13, 13, 7, 7, 0, 9, 11, 4, 6, 0, 9, 11, 4, 6, 0, 9, 11, 4, 6, 0, 10, 14, 6, 10, 5, 0, 4, 11, 0, 10, 5, 9, 1, 5, 0, 11, 2, 8, 14, 10, 6, 12, 3, 9, 5, 1, 7, 13, 4, 0, 12, 5, 10, 3, 0, 12, 5, 10, 3, 0, 12, 5, 10, 3, 0, 13, 8, 12, 7, 5, 3, 13, 2, 12, 10, 8, 3, 7, 2, 0, 14, 11, 14, 11, 10, 9, 6, 9, 6, 5, 4, 1, 4, 1, 0, 0, 14, 1, 0, 0, 0, 14, 1, 0, 0, 0, 14, 1, 0, 0}.

$\mathbf{s}_0^2$ ={0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 1, 4, 3, 10, 12, 11, 14, 13, 5, 7, 6, 9, 8, 0, 4, 2, 8, 6, 5, 9, 7, 13, 11, 10, 14, 12, 3, 1, 0, 6, 3, 12, 9, 0, 6, 3, 12, 9, 0, 6, 3, 12, 9, 0, 8, 4, 1, 12, 10, 3, 14, 11, 7, 5, 13, 9, 6, 2, 0, 10, 5, 5, 0, 5, 0, 10, 10, 5, 10, 5, 0, 0, 10, 0, 12, 6, 9, 3, 0, 12, 6, 9, 3, 0, 12, 6, 9, 3, 0, 14, 7, 13, 6, 10, 9, 2, 8, 1, 5, 4, 12, 3, 11, 0, 1, 8, 2, 9, 5, 6, 13, 7, 14, 10, 11, 3, 12, 4, 0, 3, 9, 6, 12, 0, 3, 9, 6, 12, 0, 3, 9, 6, 12, 0, 5, 10, 10, 0, 10, 0, 5, 5, 10, 5, 10, 0, 0, 5, 0, 7, 11, 14, 3, 5, 12, 1, 4, 8, 10, 2, 6, 9, 13, 0, 9, 12, 3, 6, 0, 9, 12, 3, 6, 0, 9, 12, 3, 6, 0, 11, 13, 7, 9, 10, 6, 8, 2, 4, 5, 1, 3, 12, 14, 0, 13, 14, 11, 12, 5, 3, 4, 1, 2, 10, 8, 9, 6, 7, 0}.

$\mathbf{s}_1^2$ ={1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 0, 3, 3, 7, 7, 0, 3, 3, 7, 7, 0, 3, 3, 7, 7, 0, 5, 4, 11, 10, 10, 0, 14, 6, 5, 5, 10, 9, 1, 0, 0, 7, 5, 0, 13, 5, 12, 10, 5, 3, 10, 2, 0, 10, 8, 0, 9, 6, 4, 1, 0, 9, 6, 4, 1, 0, 9, 6, 4, 1, 0, 11, 7, 8, 4, 10, 6, 2, 3, 14, 5, 1, 12, 13, 9, 0, 13, 8, 12, 7, 5, 3, 13, 2, 12, 10, 8, 3, 7, 2, 0, 0, 9, 1, 10, 0, 0, 9, 1, 10, 0, 0, 9, 1, 10, 0, 2, 10, 5, 13, 10, 12, 5, 0, 8, 5, 7, 0, 10, 3, 0, 4, 11, 9, 1, 5, 9, 1, 14, 6, 10, 14, 6, 4, 11, 0, 6, 12, 13, 4, 0, 6, 12, 13, 4, 0, 6, 12, 13, 4, 0, 8, 13, 2, 7, 10, 3, 8, 12, 2, 5, 13, 3, 7, 12, 0, 10, 14, 6, 10, 5, 0, 4, 11, 0, 10, 5, 9, 1, 5, 0, 12, 0, 10, 13, 0, 12, 0, 10, 13, 0, 12, 0, 10, 13, 0, 14, 1, 14, 1, 10, 9, 11, 9, 11, 5, 4, 6, 4, 6, 0}.

It is easy to verify that

- *each sequence is perfect;*
- *each* $\mathcal{S}^m$ *is an optimal* $(225, 15, 15)$*-ZCZ sequence set, where* $1 \le m \le 2$*; and*
- $|R_{\mathbf{s}_{n_1}^{m_1}, \mathbf{s}_{n_2}^{m_2}}(\tau)| = 15$ *for all* $0 \le \tau \le 224$, $1 \le m_1 \ne m_2 \le 2$, *and* $0 \le n_1, n_2 \le 14$.

These observations are consistent with Theorem 2.

6 Conclusion

In this paper, we constructed a class of optimal polyphase ZCZ sequence sets from generalised bent functions. Some conditions were derived under which all the ZCZ sequences generated by our construction are cyclically distinct. Furthermore, we proposed a general construction of multiple ZCZ sequence sets based on generalised bent functions. To implement the general construction, we also introduced sets of permutation with desirable properties. With such a set of permutations generated, we derived $p_{min} - 1$ multiple optimal polyphase ZCZ sequence sets with good inter-set cross-correlation, where p_{min} is the smallest prime divisor of the period of the sequences. For further work, it would be worth to study other forms of permutation sets with the same properties but larger set size. Then we could generate more different sets with good inter-set cross-correlation by Construction 2. Finally, it would also be possible and interesting to obtain multiple ZCZ sequence sets with more flexible parameters from other known functions with high nonlinearity.

Acknowledgements

The authors gratefully acknowledge constructive criticisms by the anonymous reviewers and valuable comments from the SETA conference. In addition, the authors specially thank prof. Zhengchun Zhou for his invaluable discussions on this topic and Nikolay Stoyanov Kaleyski for his grammar correction.

References

[1] Appuswamy, R. and Chaturvedi, A. K.: A new framework for constructing mutually orthogonal complementary sets and ZCZ sequences. IEEE Transactions on Information theory **52**(8), 3817–3826 (2006)

[2] Carlet, C. and Ding, C.: Highly nonlinear mappings. Journal of complexity **20**(2), 205–244 (2004)

[3] Deng, X. and Fan, P.: Spreading sequence sets with zero correlation zone. Electronics Letters **36**(11), 1 (2000)

[4] Dillon, J. F.: Elementary Hadamard difference sets. Ph.D. thesis (1974)

[5] Fan, P.: Spreading sequence design and theoretical limits for quasisynchronous CDMA systems. EURASIP Journal on Wireless Communications and Networking **2004**(1), 19–31 (2004)

[6] Fan, P. and Hao, L.: Generalized orthogonal sequences and their applications in synchronous CDMA systems. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences **83**(11), 2054–2069 (2000)

[7] Frank, R. L.: Phase shift pulse codes with good periodic correlation properties. IRE Trans. Inform. Theory **8**(6), 381–382 (1962)

[8] Golomb, S. W. and Gong, G.: Signal design for good correlation: for wireless communication, cryptography, and radar. Cambridge University Press (2005)

[9] Gong, G.: Constructions of multiple shift-distinct signal sets with low correlation. In Information Theory, 2007. ISIT 2007. IEEE International Symposium on, 2306–2310. IEEE (2007)

[10] Heimiller, R.: Phase shift pulse codes with good periodic correlation properties. IRE Transactions on Information Theory **7**(4), 254–257 (1961)

[11] Kumar, P. V., Scholtz, R. A., and Welch, L. R.: Generalized bent functions and their properties. Journal of Combinatorial Theory, Series A **40**(1), 90–107 (1985)

[12] Li, J., Fan, J., and Tang, X.: A generic construction of generalized chirp-like sequence sets with optimal zero correlation property. IEEE Communications Letters **17**(3), 549–552 (2013)

[13] Liu, T., Xu, C., and Li, Y.: Constructions of Zero Correlation Zone Sequence Sets with Low Cross-Correlation Property. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences **100**(7), 1583–1587 (2017)

[14] Liu, Y.-C., Chen, C.-W., and Su, Y. T.: New constructions of zero-correlation zone sequences. IEEE Transactions on Information Theory **59**(8), 4994–5007 (2013)

[15] Popovic, B. M. and Mauritz, O.: Generalized chirp-like sequences with zero correlation zone. IEEE Transactions on Information Theory **56**(6), 2957–2960 (2010)

[16] Rothaus, O. S.: On bent functions. Journal of Combinatorial Theory, Series A **20**(3), 300–305 (1976)

[17] Sarwate, D.: Bounds on crosscorrelation and autocorrelation of sequences (Corresp.). IEEE Transactions on Information Theory **25**(6), 720–724 (1979)

[18] Tang, X., Fan, P., and Lindner, J.: Multiple Binary ZCZ Sequence Sets With Good Cross-Correlation Property Based on Complementary Sequence Sets. IEEE Transactions on Information Theory **56**(8), 4038–4045 (2010)

[19] Tang, X. and Mow, W. H.: Design of spreading codes for quasi-synchronous CDMA with intercell interference. IEEE Journal on Selected Areas in Communications **24**(1), 84–93 (2006)

[20] Tang, X. H., Fan, P. Z., and Matsufuji, S.: Lower bounds on correlation of spreading sequence set with low or zero correlation zone. Electronics Letters **36**(6), 551–552 (2000)

[21] Tokareva, N. N.: Generalizations of Bent Functions. A Survey. Journal of Applied and Industrial Mathematics **5**(1), 110–129 (2011)

[22] Torii, H., Nakamura, M., and Suehiro, N.: A new class of zero-correlation zone sequences. IEEE Transactions on Information Theory **50**(3), 559–565 (2004)

[23] Welch, L.: Lower bounds on the maximum cross correlation of signals (Corresp.). IEEE Transactions on Information Theory **20**(3), 397–399 (1974)

[24] Yang, K., Kim, Y.-K., and Kumar, P. V.: Quasi-orthogonal sequences for code-division multiple-access systems. IEEE Transactions on Information Theory **46**(3), 982–993 (2000)

[25] Zhou, Z., Zhang, D., Helleseth, T., and Wen, J.: A Construction of Multiple Optimal ZCZ Sequence Sets With Good Cross Correlation. IEEE Transactions on Information Theory **64**(2), 1340–1346 (2018)

Errata for
Design of sequences with good correlation properties

Dan Zhang

Thesis for the degree philosophiae doctor (PhD)
at the University of Bergen

__10th August 2021_ 17.08.21

(date and sign. of candidate) (date and sign. of faculty)

Errata

Page 22 line -7, -8 and -9 Typos: “(mod n)” – corrected to “(mod N)”

Page 23 line 1 Typos: “$\mathbf{u}_k = \{u_k(i)\}$” – corrected to “$\mathbf{b}_k = \{b_k(i)\}$”

Page 26 line 11 Typos: “$\omega_{rm}^{mc(r)\alpha(l)k^2+\beta(l)k+rg(l)}$ ” corrected to “$\omega_{rm}^{mc(r)\alpha(l)k^2+\beta(l)k+irg(l)}$,,

Graphic design: Communication Division, UiB / Print: Skipnes Kommunikasjon AS

uib.no

ISBN: 9788230845165 (print)
9788230840283 (PDF)