Polyphase Sequences With Flexible Zero-Ambiguity-Zone Configurations for Integrated Sensing and Communications

Gangsan Kim, *Member, IEEE*, Hong-Yeop Song, *Senior Member, IEEE*, and Guang Gong, *Fellow, IEEE*

***Abstract*—This paper develops the theory and constructions of polyphase zero-ambiguity-zone (ZAZ) sequences for ISAC waveforms, enabling the ZAZ shape to be designed over delay–Doppler regions of interest and supporting flexible (including multi-mode) sensing–communication operation. We first prove that a polyphase sequence with an optimal rectangular auto-ZAZ must be a member of some uncorrelated optimal ZCZ sequence family, and conversely, any member of an uncorrelated optimal ZCZ sequence family has an optimal rectangular auto-ZAZ. We generalize the optimality condition on the rectangular ZAZ to that on centrally symmetric convex ZAZs in general. We propose some constructions of families of polyphase sequences with a strictly or asymptotically optimal rectangular ZAZ, and asymptotically optimal rhombic or hexagonal ZAZ from the flexible ZAZ configuration.**

***Index Terms*—Integrated sensing and communication (ISAC), polyphase sequences, zero-ambiguity-zone sequences, zero-correlation-zone sequences, uncorrelated sequences.**

I. Introduction

INTEGRATED sensing and communication (ISAC) has emerged as a foundational technology for next-generation wireless communication systems, including 6G and beyond [1]. By integrating advanced sensing capabilities with reliable communication within a unified framework, ISAC enhances spectrum efficiency and could optimize resource utilization. This innovative approach supports some broad applications, ranging from autonomous driving to environmental monitoring and the Internet of Things (IoT) [1], [2]. The growing importance of ISAC has catalyzed research into waveform designs, which are generally categorized into sensing-centric, communication-centric, and joint designs [3].

Received 12 June 2025; revised 23 February 2026; accepted 24 February 2026. Date of publication 26 February 2026; date of current version 23 April 2026. This work was supported by the National Research Foundation of Korea (NRF) Grant by Korean Government through the Ministry of Sciences and ICT (MSIT) under Grant RS-2023-00209000. *(Corresponding author: Gangsan Kim.)*

Gangsan Kim and Hong-Yeop Song are with the School of Electrical and Electronic Engineering, Yonsei University, Seoul 03722, South Korea (e-mail: gs.kim@yonsei.ac.kr; hysong@yonsei.ac.kr).

Guang Gong is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: ggong@uwaterloo.ca).

Communicated by C. Carlet, Associate Editor for Sequences and Cryptography.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIT.2026.3668351.

Digital Object Identifier 10.1109/TIT.2026.3668351

In sensing-centric design of ISAC, waveforms utilizing sequences with favorable ambiguity function are among the key candidates being considered [4], [5], [6], [7], [8]. The ambiguity function generalizes the concept of correlation by incorporating both time shifts and Doppler shifts, as a two-dimensional correlation measure. If a sequence has low sidelobe ambiguity function, then it can be used as a radar waveform for accurately estimating the target position and Doppler [9], [10], [11], [12], [13], [14], [15], [16]. It can also be used in communications as a modulation waveform that carries data while tolerating Doppler shifts [8], [11], [17], [18], [19], [20].

Some famous candidate waveforms for ISAC applications are polyphase sequences (also referred to as unimodular or constant amplitude sequences) with Low-/ Zero-Ambiguity-Zone (LAZ / ZAZ). These sequences have a low or zero (non-trivial) ambiguity function within a local two-dimensional (time shift, Doppler shift) region [8], [17], [18], [19], [20], [21], [22], [23], [24], [25]. Research on the design of these sequences can be categorized based on several criteria: the type of ambiguity zone, such as ZAZ [8], [18], [20], [21], [24], [25] or LAZ [8], [17], [18], [19], [20], [22], [23]; the number of sequences, distinguishing between single sequences with auto-ZAZ/LAZ [8], [18], [21], [22], [23], [24], [25] and multiple sequences with cross-ZAZ/LAZ [8], [17], [19], [20]; the nature of the ambiguity function, whether periodic [8], [20], [21] or aperiodic [8], [17], [18], [19], [22], [23], [24], [25]; and the construction method, whether deterministic [8], [17], [19], [20], [21], [24], [25] or algorithmic [18], [22], [23]. Such sequences may also be applied in other scenarios such as training sequences in high-mobility communications, where robustness against large Doppler shifts is essential [26], [27].

For the polyphase sequences of length L with a rectangular auto-ZAZ, the area of the auto-ZAZ is upper bounded by $4L$ [8], which we refer to as the *Ye–Zhou–Fan–Liu–Lei–Tang auto-ZAZ bound*. An auto-ZAZ attaining this upper bound is referred to as an optimal auto-ZAZ. They also showed that for the families of K polyphase sequences of length L with a rectangular ZAZ, the ZAZ area is upper bounded by $4L/K$ [8], which we refer to as the *Ye–Zhou–Fan–Liu–Lei–Tang cross-ZAZ bound*. The ZAZ attaining this upper bound is also referred to as optimal.

An (L, K, W)-Zero-Correlation-Zone (ZCZ) sequence family consists of K sequences of length L, where the periodic

0018-9448 © 2026 IEEE. All rights reserved, including rights for text and data mining, and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Yonsei Univ. Downloaded on May 26,2026 at 02:31:12 UTC from IEEE Xplore. Restrictions apply.

out-of-phase auto-correlation is zero for time shifts $|\tau| < W$, and the periodic cross-correlation between any two sequences is also zero within the same range of time shifts, including $\tau = 0$ [28], [29], [30]. It is well-known that $K \leq L/W$ [31] and it is called an optimal family when the equality is satisfied. An uncorrelated ZCZ sequence family has an additional property that the periodic cross-correlation is zero for all time shifts, even outside the zero-correlation-zone. Uncorrelated optimal ZCZ sequence families have been proposed through various constructions [32], [33], [34], [35], [36]. Furthermore, Kim and Song proved earlier in [48] that any uncorrelated optimal ZCZ sequence family can be obtained by Popović's construction [35].

In practical sensing systems, the ability to support multi-mode operation is increasingly important, particularly for scenarios with varying target range and Doppler shift requirements [37], [38], [39]. Multi-mode systems aim to optimize performance across distinct operational modes such as wide Doppler shift tolerance for high-speed applications and precise range resolution for stationary targets. Previous multi-mode approaches are often faced with significant trade-offs, such as reduced performance in each mode or the need for additional resources to maintain reasonable performance [37], [38], [39]. We introduce in this paper some sequence families with dual ZAZs as shown in Fig. 1, where ZAZ-I and ZAZ-II can contribute simultaneously to range and Doppler resolution, respectively. Such types of families can exhibit multifunctionality in sensing and communication, respectively, as follows.

- **Sensing:** When used as MIMO radar waveforms, the ZAZ's time-shift dimension corresponds to range resolution, while its Doppler-shift dimension corresponds to Doppler resolution [9], [10], [11], [12], [40]. Incorporating two ZAZs enables versatile target detection and tracking:
  - *Broad-Range Detection (ZAZ-I).* Suited for diverse target distances and moderate speeds, providing a wider window of time shifts.
  - *High-Speed Proximity Detection (ZAZ-II).* Geared toward nearby, fast-moving objects, tolerating larger Doppler shifts despite a narrower range of time shifts.
- **Communication:** Beyond sensing, the sequence families with dual ZAZs also accommodate changing channel conditions in communication systems:
  - *High Time-Shift Tolerant Mode (ZAZ-I).* Allows significant time delays with moderate Doppler shifts, supporting flexible transmission schemes such as code-shift keying (CSK) [41] that benefit from robustness to timing variations [8].
  - *High Doppler-Shift Tolerant Mode (ZAZ-II).* Focuses on scenarios with substantial Doppler shifts and smaller time offsets.

This paper also tries to advance the theory of ZAZ configurations by establishing the relationship between traditional ZAZ configurations and uncorrelated optimal ZCZ sequences. Building on this, it introduces *the flexible ZAZ configurations*, extending the ZAZ shape from a single rectangular region to a centrally symmetric convex region and incorporating multiple ZAZs. For centrally symmetric convex ZAZ, this

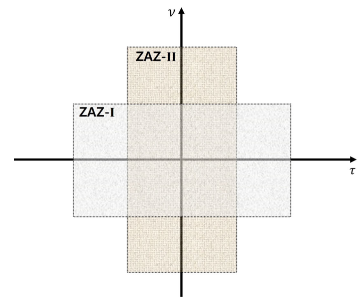


Fig. 1. Dual rectangular ZAZs.

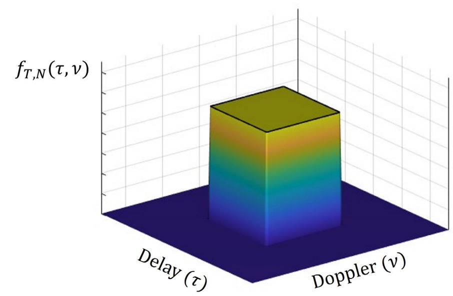


Fig. 2. An example of uniform probability density function over the delay–Doppler plane.

paper finds and proves the upper bound on its area, which is a non-trivial generalization of Ye–Zhou–Fan–Liu–Lei–Tang cross-ZAZ bound [8] for rectangular ZAZ. All these results will contribute to the multifunctionality of ISAC systems.

To better understand why such general or multiple ZAZs are meaningful, consider a practical sensing system operating under additive white Gaussian noise (AWGN), where the received signal can be expressed as

$$r(t) = \alpha\, s(t - \tau_0)e^{j2\pi\nu_0 t} + n(t),$$

where $s(t)$ denotes the transmitted waveform, (τ_0, ν_0) are the true delay and Doppler parameters of the target, and $n(t)$ represents complex Gaussian noise. Under this model, the likelihood function of (τ, ν) is proportional to the squared magnitude of the ambiguity function evaluated between the received signal and the transmitted waveform (under whitened AWGN with unknown α concentrated out). Hence, the likelihood surface inherits its shape directly from the ambiguity characteristics of the waveform in the delay–Doppler plane: a waveform with a sharply localized ambiguity peak produces a narrow and distinct likelihood ridge centered at the true parameters, whereas one exhibiting broader or skewed ambiguity features leads to a more diffuse and anisotropic likelihood distribution. Accordingly, the local geometry of this likelihood surface determines the achievable accuracy of parameter estimation in noise.

A rectangular zero-ambiguity zone (ZAZ) has been widely adopted in the literature because it effectively represents many practical sensing scenarios in a simple and analytically tractable way. When the uncertainty of delay (τ) and Doppler (ν) is known to lie uniformly within bounded intervals

Authorized licensed use limited to: Yonsei Univ. Downloaded on May 26,2026 at 02:31:12 UTC from IEEE Xplore. Restrictions apply.

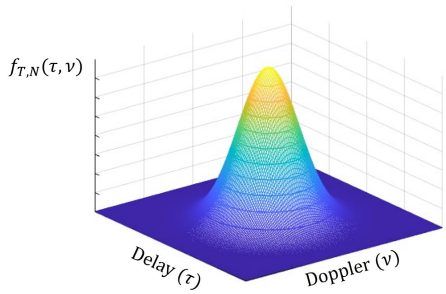


Fig. 3. An example of single-modal probability density function over the delay–Doppler plane.

(i.e. $\tau_1 \leq \tau \leq \tau_2$ and $\nu_1 \leq \nu \leq \nu_2$), the corresponding parameter space forms a rectangular region of uniform probability density (Fig. 2). Beyond this baseline, many real sensing environments exhibit structured or directional uncertainty. In practice, non-uniform joint priors over (range, velocity) naturally arise from extended or group targets that induce spatially distributed returns and anisotropic support [42], from target micro-motions (e.g., rotation, vibration) that create characteristic sidebands and localized ridges [43], from heavy-tailed compound-Gaussian clutter that skews the likelihood toward particular delay–Doppler sectors [44], and from accelerating targets whose kinematic coupling concentrates probability along curved manifolds [45]. Depending on the observation geometry, target trajectory, or platform motion, the joint likelihood of (τ, ν) may become concentrated along certain orientations or decay smoothly from a dominant mode, as depicted in Fig. 3. In such cases, the high-likelihood region in the delay–Doppler plane becomes anisotropic or tilted, suggesting that the region of minimal ambiguity should conform to the equiprobability contours of the underlying parameter distribution rather than only fixed rectangular boundaries. By aligning the ZAZ boundary with these contours, the waveform's ambiguity suppression focuses on the region where the true parameters are most probable, leading to improved robustness under AWGN.

This interpretation aligns with the Neyman–Pearson lemma [46] in detection theory, which states that the optimal decision region for a fixed false-alarm rate follows likelihood-ratio level sets. If the probability density function is uniform over bounded intervals, as in Fig. 2, the corresponding ZAZ is rectangular; if the probability density function exhibits a single dominant mode or directional concentration, as in Fig. 3, the appropriate ZAZ may take on rhombic, hexagonal, or elliptical contours that more closely follow the structure of the uncertainty. From this perspective, the rectangular ZAZ remains a fundamental and broadly applicable model, but it represents one case within a more general theoretical framework in which ZAZ geometries can be adapted to diverse sensing priors. Allowing the ZAZ boundary to align with the statistical structure of $f_{T,N}(\tau, \nu)$ enables waveform designs that more naturally capture the characteristics of real-world sensing environments, providing a unified foundation for both conventional rectangular and generalized non-rectangular ZAZ designs.

Some key contributions of this paper include the following:

- **Equivalence with uncorrelated optimal ZCZ sequence family:** We prove that a polyphase sequence with an optimal rectangular auto-ZAZ must be a member of some uncorrelated optimal ZCZ sequence families, and conversely, any member of an uncorrelated optimal ZCZ sequence family has an optimal rectangular auto-ZAZ. These implications are obtained by leveraging the frequency distance sequence set introduced in [47] and the unique form of uncorrelated optimal ZCZ sequence families established in [48].
- **Construction for families of polyphase sequences with an optimal rectangular ZAZ**: We propose a construction for families of K polyphase sequences of length L with optimal rectangular ZAZ $(-X, X) \times (-Y, Y)$ of area $4L/K$ (so that $KXY = L$), attaining the Ye–Zhou–Fan–Liu–Lei–Tang cross-ZAZ bound. Our construction covers all the parameters of integer quadruples (L, K, X, Y) satisfying $KXY = L$, including those parameters that have not yet been discovered. This is achieved by carefully selecting sequences from an uncorrelated optimal ZCZ sequence family to constitute a new family.
- **Optimality condition on centrally symmetric convex ZAZs in general:** We generalize the optimality condition from rectangular ZAZs to centrally symmetric convex ZAZs in general. The practical ZAZs for radar waveforms have not been limited to rectangular shapes and have been explored in various geometries [12], such as rhombuses [24], [25]. We prove that the upper bound on the area of rectangular ZAZs can be applied to these centrally symmetric convex regions as well. This extends the result of [8] via Blichfeldt's Theorem [49].
- **Construction for families of polyphase sequences with dual asymptotically optimal rectangular ZAZs:** We propose families of polyphase sequences that have dual asymptotically optimal rectangular ZAZs as in Fig. 1. ZAZ-I may support larger time shifts with narrower Doppler-shift tolerance, while ZAZ-II could prioritize broader Doppler-shift tolerance alongside smaller time shifts. Unlike prior multi-mode radar research [37], [38], [39], the proposed sequences retain asymptotic optimality in both modes without adding extra resources, where the asymptotic optimality is with respect to the Ye–Zhou–Fan–Liu–Lei–Tang cross-ZAZ bound. This result is obtained by carefully selecting perfect sequences as constituents in the construction of an uncorrelated optimal ZCZ sequence family.
- **Optimality analysis of polyphase sequences with ZAZ of various shapes:** Building upon the polyphase sequence families with dual ZAZs that we previously introduced, we extend the analysis to centrally symmetric convex ZAZs, including shapes such as rhombuses and hexagons. We identify that the previously discussed sequence families have other ZAZs with diverse shapes, including two rectangular ZAZs, several rhombic ZAZs, and several hexagonal ZAZs, which are all asymptotically optimal with respect to our new bound.

Authorized licensed use limited to: Yonsei Univ. Downloaded on May 26,2026 at 02:31:12 UTC from IEEE Xplore. Restrictions apply.

This paper is organized as follows. Section II introduces some notation, definitions, and some well-known facts related to our work. Section III presents our main results with four subsections. Finally, Section IV concludes this paper.

II. Preliminaries

A. Some Notation, Definitions, and Known Facts

- $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$ are the sets of integers, real numbers, and complex numbers, respectively.
- ω_v is a primitive v-th root of unity over $\mathbb{C}$.
- A root-of-unity sequence is a complex sequence over an alphabet which is a subset of the unit circle in $\mathbb{C}$. Such a sequence is sometimes called a polyphase sequence when the alphabet is (a part of) a regular polygon over the unit circle.
- A complex-valued sequence $\boldsymbol{a} = \{a(0), a(1), \ldots\}$ is said to have a period L if $a(t+L) = a(t)$ for all $t \geq 0$. A sequence with period L is also said to be a sequence of length L, and is denoted by $\boldsymbol{a} = \{a(t)\}_{t=0}^{L-1}$. Sometimes, the notation $\boldsymbol{a} = \{a(t)\}_{t=0}^{L-1}$ for a sequence can be understood as an L-tuple row vector $(a(0), a(1), \ldots, a(L-1))$. We also implicitly use a row-vector of length L for a sequence of length L. In this paper, all the sequences are complex-valued unless otherwise specified.
- For any two sequences $\boldsymbol{a} = \{a(t)\}_{t=0}^{L-1}$ and $\boldsymbol{b} = \{b(t)\}_{t=0}^{L-1}$ both of length L, their Hadamard product $\boldsymbol{a} \circledast \boldsymbol{b} = \{(a \circledast b)(t)\}_{t=0}^{L-1}$ is given by
$$(a \circledast b)(t) = a(t)b(t) \quad \text{for } t = 0, 1, \ldots, L-1.$$
- For any two sequences $\boldsymbol{a} = \{a(t)\}_{t=0}^{L-1}$ and $\boldsymbol{b} = \{b(t)\}_{t=0}^{L-1}$ both of length L, their inner product is given by
$$< \boldsymbol{a}, \boldsymbol{b} >= \sum_{t=0}^{L-1} a(t)b^*(t),$$
where $b^*(t)$ is the complex conjugate of $b(t)$.
- For a sequence $\boldsymbol{a} = \{a(t)\}_{t=0}^{L-1}$ of length L, we denote by $\hat{\boldsymbol{a}} = \{\hat{a}(n)\}_{n=0}^{L-1}$ its DFT sequence given by
$$\hat{a}(n) = \frac{1}{\sqrt{L}} \sum_{j=0}^{L-1} \omega_L^{jn} a(j), \quad n = 0, 1, \ldots, L-1.$$
Each $\hat{a}(n)$ will occasionally be expressed as DFT$[\boldsymbol{a}](n)$.
- For a sequence $\hat{\boldsymbol{a}} = \{\hat{a}(n)\}_{n=0}^{L-1}$ of length L, we denote by $\boldsymbol{a} = \{a(t)\}_{t=0}^{L-1}$ its inverse DFT (IDFT) sequence given by
$$a(t) = \frac{1}{\sqrt{L}} \sum_{j=0}^{L-1} \omega_L^{-jt} \hat{a}(j), \quad t = 0, 1, \ldots, L-1.$$
Each $a(t)$ will occasionally be expressed as IDFT$[\hat{\boldsymbol{a}}](t)$.
- For any two sequences $\boldsymbol{a} = \{a(t)\}_{t=0}^{L-1}$ and $\boldsymbol{b} = \{b(t)\}_{t=0}^{L-1}$ both of length L, their periodic correlation is given by
$$C(\boldsymbol{a}, \boldsymbol{b}; \tau) = \sum_{t=0}^{L-1} a(t+\tau)b^*(t), \text{ for } \tau = 0, 1, \ldots, L-1,$$
where $t + \tau$ is computed mod L. When $\boldsymbol{a} \neq \boldsymbol{b}$, the above is sometimes called the cross-correlation. When $\boldsymbol{a} = \boldsymbol{b}$, it is called the auto-correlation and we use $C(\boldsymbol{a}; \tau)$ for simplicity.
- A sequence is said to be perfect if its auto-correlation is zero at all the non-trivial time shifts.
- A pair of sequences of the same length L is said to be uncorrelated if their cross-correlation is zero at all the time shifts $\tau = 0, 1, \ldots, L-1$.
  - *Known-fact 1: [50, Corollary 2]:* Let $\boldsymbol{a}$ and $\boldsymbol{b}$ be two sequences of length L and consider their DFT sequences $\hat{\boldsymbol{a}}$ and $\hat{\boldsymbol{b}}$. If $\hat{\boldsymbol{a}} \circledast \hat{\boldsymbol{b}}^*$ is the all-zero sequence—equivalently, if $\hat{\boldsymbol{a}} \circledast \hat{\boldsymbol{b}}$ is the all-zero sequence—then $(\boldsymbol{a}, \boldsymbol{b})$ is an uncorrelated sequence pair.
- Consider some pairwise uncorrelated K sequences $\boldsymbol{a}_i = \{a_i(t)\}_{t=0}^{L-1}$ of length L for $i = 0, 1, \ldots, K-1$. A set $\mathcal{A} \triangleq \{\boldsymbol{a}_i | i = 0, 1, \ldots, K-1\}$ of these sequences is said to be an uncorrelated (L, K, W)-ZCZ sequence family if, for any i,
$$C(\boldsymbol{a}_i; \tau) = 0 \quad \text{for } \tau = 1, 2 \ldots, W-1.$$
  - *Known-fact 2: [31, Corollary 3]:* For any uncorrelated (L, K, W)-ZCZ sequence family, we must have
$$K \leq L/W.$$
  - If $K = L/W$, such a family is said to be an uncorrelated optimal ZCZ sequence family.
- For any two polyphase sequences $\boldsymbol{a} = \{a(t)\}_{t=0}^{L-1}$ and $\boldsymbol{b} = \{b(t)\}_{t=0}^{L-1}$ both of length L, the periodic ambiguity function $F(\boldsymbol{a}, \boldsymbol{b}; \tau, \nu)$ between $\boldsymbol{a}$ and $\boldsymbol{b}$ at time shift $\tau \in \mathbb{Z}$ and Doppler shift $\nu \in \mathbb{Z}$ is defined as
$$F(\boldsymbol{a}, \boldsymbol{b}; \tau, \nu) = \sum_{t=0}^{L-1} a(t+\tau)b^*(t)\omega_L^{\nu t}, \tag{1}$$
where $t + \tau$ is computed mod L. When $\boldsymbol{a} = \boldsymbol{b}$, we write $F(\boldsymbol{a}; \tau, \nu)$ for simplicity. The correlation of $\boldsymbol{a}$ and $\boldsymbol{b}$ can be obtained from their ambiguity function since they are related as follows:
$$C(\boldsymbol{a}, \boldsymbol{b}; \tau) = F(\boldsymbol{a}, \boldsymbol{b}; \tau, 0) \quad \text{for all } \tau. \tag{2}$$
- For any two real numbers $A < B$, we often use the open interval notation $(A, B) \subset \mathbb{R}$, where
$$(A, B) \triangleq \{x \in \mathbb{R} \,|\, A < x < B\}.$$
- Consider a bounded region Π over the Euclidean plane. We denote by $|\Pi|$ the area of the region $\Pi \subset \mathbb{R}^2$. Further, we denote by $|\Pi \cap \mathbb{Z}^2|$ the number of integer lattice points in Π.
- For an integer L, consider a bounded region $\Pi_a \subset (-L, L)^2 \subset \mathbb{R}^2$. A polyphase sequence $\boldsymbol{s}$ of length L is said to have Π_a as its auto-zero-ambiguity-zone (auto-ZAZ) if
$$F(\boldsymbol{s}; \tau, \nu) = 0 \quad \text{for } (\tau, \nu) \in (\Pi_a \cap \mathbb{Z}^2) \backslash \{(0, 0)\}. \tag{3}$$
If
$$\Pi_a = (-X, X) \times (-Y, Y)$$
for some integers X and Y and satisfies (3), then Π_a is called a rectangular auto-ZAZ.

Authorized licensed use limited to: Yonsei Univ. Downloaded on May 26,2026 at 02:31:12 UTC from IEEE Xplore. Restrictions apply.

- *Known-fact 3: (Ye–Zhou–Fan–Liu–Lei–Tang auto-ZAZ bound [8, Theorem 1]):* For a polyphase sequence of length L with a rectangular auto-ZAZ Π_a of the form above, we have:

$$|\Pi_a| = 4XY \leq 4L. \tag{4}$$

- When the equality holds, the rectangular auto-ZAZ Π_a is called optimal.
- *Known-fact 4: [8, Lemma 1]* All the polyphase sequences have a trivial optimal rectangular auto-ZAZ of the form $(-1, 1) \times (-L, L)$.

- Consider a bounded region $\Pi \subset (-L, L)^2 \subset \mathbb{R}^2$. A family $\{\boldsymbol{a}_i = \{a_i(t)\}_{t=0}^{L-1} | i = 0, 1, \ldots, K-1\}$ of K polyphase sequences of length L is called a sequence family with ZAZ Π if it satisfies that, for any integers $i, j \in \{0, 1, \ldots, K-1\}$,

$$F(\boldsymbol{a}_i, \boldsymbol{a}_j; \tau, \nu) = 0 \quad \text{for } (\tau, \nu) \in (\Pi \cap \mathbb{Z}^2),$$

except for the case where $(\tau, \nu) = (0, 0)$ and $i = j$. Therefore, a ZAZ is an auto-ZAZ as well as, for a family, a cross-ZAZ. If $\Pi = (-X', X') \times (-Y', Y')$ for some integers X' and Y', then Π is called a rectangular ZAZ.

- *Known-fact 5: (Ye–Zhou–Fan–Liu–Lei–Tang cross-ZAZ bound [8, Theorem 1]):* For a family of K polyphase sequences of length L with rectangular ZAZ Π, we have

$$|\Pi| = 4X'Y' \leq 4L/K. \tag{5}$$

- When the equality holds, the rectangular ZAZ Π is called optimal.

B. Frequency Distance Sequence Set (FDSS)

In this subsection, we review some research results presented in [47] and derive several related lemmas. To set up the discussion, we introduce the following operators.

- For an integer Y, we denote by E_Y the Y-fold-expander that operates on a sequence. When it is applied to a sequence $\boldsymbol{g} = \{g(t)\}_{t=0}^{X-1}$ of length X, the result is a sequence $\mathrm{E}_Y \circ \boldsymbol{g} = \{(\mathrm{E}_Y \circ g)(t)\}_{t=0}^{XY-1}$ of length XY where

$$(\mathrm{E}_Y \circ g)(t) = \begin{cases} g(t/Y) & \text{for } t \text{ with } Y|t \\ 0 & \text{otherwise.} \end{cases}$$

For example, the 3-fold expansion of a sequence (w, x, y, z) of length 4 becomes the sequence $(w, 0, 0, x, 0, 0, y, 0, 0, z, 0, 0)$ of length 12.

- For an integer i, we denote by R^i the cyclic (right) shift operator that operates on a sequence. When it is applied to a sequence $\boldsymbol{s} = \{s(t)\}_{t=0}^{L-1}$ of length L, the result is a sequence $\mathrm{R}^i \circ \boldsymbol{s} = \{(\mathrm{R}^i \circ s)(t)\}_{t=0}^{L-1}$ of the same length given by

$$(\mathrm{R}^i \circ s)(t) = s(t - i) \quad \text{for all } t,$$

where $t - i$ is computed mod L.

Known-fact 6: ([51, pages 587–595]) Let X and Y be two integers. Consider a DFT sequence $\hat{\boldsymbol{g}} = \{\hat{g}(n)\}_{n=0}^{X-1}$ of length X and an integer i. Apply E_Y to $\hat{\boldsymbol{g}}$ and then apply R^i to the result to obtain $\hat{\boldsymbol{s}}_i = \{\hat{s}_i(n)\}_{n=0}^{XY-1}$ given by

$$\hat{\boldsymbol{s}}_i \triangleq \mathrm{R}^i \circ (\mathrm{E}_Y \circ \hat{\boldsymbol{g}}).$$

Let $\boldsymbol{s}_i = \{s_i(t)\}_{t=0}^{XY-1}$ and $\boldsymbol{g} = \{g(t)\}_{t=0}^{X-1}$ be IDFT sequences of $\hat{\boldsymbol{s}}_i$ and $\hat{\boldsymbol{g}}$, respectively. Then,

$$s_i(t) = g(t \bmod X)\omega_{XY}^{it} \quad \text{for } t = 0, 1, 2, \ldots, XY-1. \tag{6}$$

Remark 1: For $i = 0, 1, \ldots, Y-1$, consider $\boldsymbol{s}_i$ in (6) in Known-Fact 6. The family $\{\boldsymbol{s}_i | i = 0, 1, 2, \ldots, Y-1\}$ proposed in [47] is referred to as the frequency distance sequence set (FDSS). Various correlation and frequency properties of this sequence set are demonstrated in [47]. The sequences of the form in (6) become an important building block of the constructions of this paper for various ZAZ sequences.

For the sequences within the FDSS of the form (6), the ambiguity function has the following properties, which will be used extensively in the remainder of this paper:

Lemma 1: *Let X and Y be given integers and two integer parameters l and m. Consider two arbitrary DFT sequences $\hat{\boldsymbol{g}} = \{\hat{g}(t)\}_{t=0}^{X-1}$ and $\hat{\boldsymbol{h}} = \{\hat{h}(t)\}_{t=0}^{X-1}$ both of length X. Define $\boldsymbol{a} = \{a(t)\}_{t=0}^{XY-1}$ and $\boldsymbol{b} = \{b(t)\}_{t=0}^{XY-1}$ to be IDFT sequences of length XY given as, for $t = 0, 1, \ldots, XY-1$,*

$$a(t) \triangleq \mathrm{IDFT}[\mathrm{R}^l \circ (E_Y \circ \hat{\boldsymbol{g}})](t) \quad \textit{and}$$
$$b(t) \triangleq \mathrm{IDFT}[\mathrm{R}^m \circ (E_Y \circ \hat{\boldsymbol{h}})](t).$$

Then, we have the following relations:

1) $F(\boldsymbol{a}, \boldsymbol{b}; \tau, \nu) = \omega_{XY}^{-\nu\tau} C(\boldsymbol{a}_\nu, \boldsymbol{b}; \tau)$, *for all τ and ν, where $\boldsymbol{a}_\nu = \{a_\nu(t)\}_{t=0}^{XY-1}$ and*

$$a_\nu(t) = \mathrm{IDFT}[\mathrm{R}^{l+\nu} \circ (E_Y \circ \hat{\boldsymbol{g}})](t) \quad \textit{for all } t. \tag{7}$$

2) $|F(\boldsymbol{a}, \boldsymbol{b}; \tau, \nu)|$

$$= \begin{cases} 0, & \textit{when} \quad Y \nmid (l - m + \nu) \\ Y|F(\boldsymbol{g}, \boldsymbol{h}; \tau \bmod X, (l - m + \nu)/Y)|, & \textit{otherwise} \end{cases} \tag{8}$$

where $\boldsymbol{g}$ and $\boldsymbol{h}$ are IDFT sequences of $\hat{\boldsymbol{g}}$ and $\hat{\boldsymbol{h}}$, respectively.

Proof:

1) It is straightforward to check by using the relation

$$a_\nu(t) = a(t)\omega_{XY}^{\nu t} \quad \text{for all } t.$$

2) The case of $Y|(l - m + \nu)$ can be derived through some direct calculation from the ambiguity function of $\boldsymbol{a}$ and $\boldsymbol{b}$ to those of $\boldsymbol{g}$ and $\boldsymbol{h}$ using the relation (6). Now, we assume that $Y \nmid (l - m + \nu)$. From the first item of this Lemma, we have

$$F(\boldsymbol{a}, \boldsymbol{b}; \tau, \nu) = \omega_{XY}^{-\nu\tau} C(\boldsymbol{a}_\nu, \boldsymbol{b}; \tau),$$

where $\boldsymbol{a}_\nu = \{a_\nu(t)\}_{t=0}^{XY-1}$ is given in (7). Note that DFT sequence $\hat{\boldsymbol{a}}_\nu$ of $\boldsymbol{a}_\nu$ is represented as

$$\hat{\boldsymbol{a}}_\nu = \mathrm{R}^{l+\nu} \circ (E_Y \circ \hat{\boldsymbol{g}}).$$

Recall that the DFT sequence $\hat{\boldsymbol{b}}$ of $\boldsymbol{b}$ is represented as

$$\hat{\boldsymbol{b}} = \mathrm{R}^m \circ (E_Y \circ \hat{\boldsymbol{h}}).$$

Authorized licensed use limited to: Yonsei Univ. Downloaded on May 26,2026 at 02:31:12 UTC from IEEE Xplore. Restrictions apply.

Note that $Y \nmid (l - m + \nu)$ implies $l + \nu \not\equiv m \pmod{Y}$. Therefore, none of the nonzero terms in $\hat{\boldsymbol{a}}_\nu$ is overlapped with the nonzero terms in $\hat{\boldsymbol{b}}$. Therefore, $\hat{\boldsymbol{a}}_\nu \circledast \hat{\boldsymbol{b}}$ is the all-zero sequence. From Known-Fact 1, the cross-correlation of $\boldsymbol{a}_\nu$ and $\boldsymbol{b}$ is zero for any τ. ■

Lemma 2: *Consider (not necessarily distinct) two sequences* $\boldsymbol{a} = \{a(t)\}_{t=0}^{L-1}$ *and* $\boldsymbol{b} = \{b(t)\}_{t=0}^{L-1}$ *of length* L. *For any two integers* τ *and* ν, *let* $\boldsymbol{a}^{(\tau,\nu)} = \{a^{(\tau,\nu)}(t)\}_{t=0}^{L-1}$ *and* $\boldsymbol{b}^{(\tau,\nu)} = \{b^{(\tau,\nu)}(t)\}_{t=0}^{L-1}$ *be sequences of length* L *given by*

$$a^{(\tau,\nu)}(t) \triangleq a(t+\tau)\omega_L^{\nu t}$$

and

$$b^{(\tau,\nu)}(t) \triangleq b(t+\tau)\omega_L^{\nu t},$$

where $t + \tau$ *is computed mod* L. *Consider (not necessarily distinct) two integer pairs* (τ_0, ν_0) *and* (τ_1, ν_1). *Then, the inner product between* $\boldsymbol{a}^{(\tau_0,\nu_0)}$ *and* $\boldsymbol{b}^{(\tau_1,\nu_1)}$ *can be calculated as*

$$< \boldsymbol{a}^{(\tau_0,\nu_0)}, \boldsymbol{b}^{(\tau_1,\nu_1)} >= \omega_L^{-\tau_1(\nu_0-\nu_1)} F(\boldsymbol{a}, \boldsymbol{b}; \tau_0 - \tau_1, \nu_0 - \nu_1).$$

III. Main Results

In this section, we design various types of polyphase sequences with ZAZ in four subsections.

A. Sequences With Optimal Rectangular ZAZ

Theorem 1: *Let* X, Y *and* K *be positive integers with* $K \le Y$. *Consider a collection*

$$\{\boldsymbol{g}_i = \{g_i(t)\}_{t=0}^{X-1} | i = 0, 1, \ldots, K-1\}$$

of (not necessarily distinct) K *polyphase perfect sequences of length* X. *For each integer* $c \in \{0, 1, \ldots, Y-1\}$, *we define a set of* K *sequences* $\boldsymbol{a}_i = \{a_i(t)\}_{t=0}^{XY-1}$ *given by*

$$a_i(t) \triangleq g_i(t \bmod X)\omega_{XY}^{(\lfloor iY/K \rfloor + c)t}, \quad t = 0, 1, \ldots, XY-1$$

for $i = 0, 1, \ldots, K-1$. *Then,* $\{\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{K-1}\}$ *has the following individual optimal auto-ZAZ (attaining the Ye–Zhou–Fan–Liu–Lei–Tang auto-ZAZ bound)*

$$\Pi_a \triangleq (-X, X) \times (-Y, Y), \tag{9}$$

and the following ZAZ

$$\Pi_z \triangleq (-X, X) \times (-\lfloor Y/K \rfloor, \lfloor Y/K \rfloor), \tag{10}$$

which becomes optimal ZAZ when $K|Y$ *(attaining the Ye–Zhou–Fan–Liu–Lei–Tang cross-ZAZ bound).*

Proof: We note here that Π_a in (9) and Π_z in (10) are fixed and used in the remainder of this paper. We note also that $\Pi_z \subset \Pi_a$ and the equality holds when $K = 1$.

1) For the optimal auto-ZAZ Π_a of individual member sequence, we will use the second item of Lemma 1 with $\boldsymbol{g} = \boldsymbol{h}$ and $l = m = \lfloor iY/K \rfloor + c$. When $Y \nmid \nu$, the left-hand side (LHS) of (8) becomes zero for any τ. When $Y \mid \nu$, it becomes
$$Y|F(\boldsymbol{g}; \tau \bmod X, \nu/Y)|$$
which becomes $Y|C(\boldsymbol{g}; \tau)|$ for $\nu = 0$ by (2), which becomes zero when $\tau \in (-X, X)$ except for $\tau = 0$ since $\boldsymbol{g}$ is a perfect sequence. Therefore, $\boldsymbol{a}$ has the ZAZ in (9). It is now obvious to check the optimality of the auto-ZAZ in (9).
2) It is sufficient to show that the family has ZAZ Π_z in (10). Without loss of generality, we assume that $c = 0$. The cases where $c > 0$ can be similarly proved. Then, for two distinct sequences $\boldsymbol{a}_i$ and $\boldsymbol{a}_j$ $(i > j)$ in the family with $c = 0$, their ambiguity function at (τ, ν) becomes zero when
$$Y \nmid (\lfloor iY/K \rfloor - \lfloor jY/K \rfloor + \nu),$$
by the second item of Lemma 1, since $l = \lfloor iY/K \rfloor$ and $m = \lfloor jY/K \rfloor$. Therefore, it becomes zero when
$$\nu \in \left(-\left(\left\lfloor \frac{iY}{K} \right\rfloor - \left\lfloor \frac{jY}{K} \right\rfloor \right), Y - \left(\left\lfloor \frac{iY}{K} \right\rfloor - \left\lfloor \frac{jY}{K} \right\rfloor \right) \right). \tag{11}$$
The superadditivity of the floor function implies
$$\begin{aligned} -(\lfloor iY/K \rfloor - \lfloor jY/K \rfloor) &\le -(\lfloor (i-j)Y/K \rfloor) \\ &\le -(\lfloor Y/K \rfloor), \end{aligned}$$
since $i > j$. Similarly,
$$\begin{aligned} &Y - (\lfloor iY/K \rfloor - \lfloor jY/K \rfloor) \\ &\ge Y - \lfloor iY/K \rfloor \\ &= \lfloor K(Y/K) \rfloor - \lfloor i(Y/K) \rfloor \\ &\ge \lfloor (K-i)(Y/K) \rfloor \\ &\ge \lfloor Y/K \rfloor. \end{aligned}$$
Therefore, $(-\lfloor Y/K \rfloor, \lfloor Y/K \rfloor)$ is a subset of the open interval in (11). This proves that the family of sequences has ZAZ given in (10), whose optimality is easy to check when $K|Y$. ■

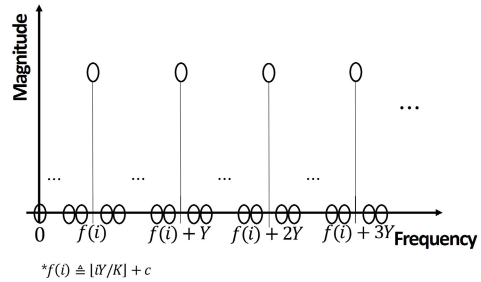


Fig. 4. Frequency domain magnitude of $\boldsymbol{a}_i$ in Theorem 1.

Remark 2: Fig. 4 shows the frequency-domain magnitude of $\boldsymbol{a}_i$ in Theorem 1. Consistent with Known-Fact 6, the nonzero frequency samples occur at uniformly spaced bins. Moreover, since $\boldsymbol{g}_i$ in Theorem 1 is a perfect sequence, and it is a well-known property that its DFT has constant magnitude [50], the nonzero frequency-domain magnitude of $\boldsymbol{a}_i$ is constant across all active bins. Equivalently, the frequency-domain profile of $\boldsymbol{a}_i$ is an evenly spaced comb with a flat top, as shown in Fig. 4.

Remark 3: Table I compares the known constructions by others for polyphase sequences with an optimal rectangular auto-ZAZ to any one member of the family from Theorem 1

Authorized licensed use limited to: Yonsei Univ. Downloaded on May 26,2026 at 02:31:12 UTC from IEEE Xplore. Restrictions apply.

TABLE I

COMPARISON OF SINGLE POLYPHASE SEQUENCE WITH AN OPTIMAL RECTANGULAR AUTO-ZAZ (ATTAINING THE YE–ZHOU–FAN–LIU–LEI–TANG AUTO-ZAZ BOUND)

Construction	Length	auto-ZAZ	Comments
[8, Theorem 8]	XY	$(-X,X)\times(-Y,Y)$	$Y \equiv XY \pmod 2$
Any one member of the family from Theorem 1	XY	$(-X,X)\times(-Y,Y)$	No constraint

TABLE II

COMPARISON OF FAMILIES OF POLYPHASE SEQUENCES WITH A (STRICTLY OR ASYMPTOTICALLY) OPTIMAL RECTANGULAR ZAZ WITH RESPECT TO THE YE–ZHOU–FAN–LIU–LEI–TANG CROSS-ZAZ BOUND

Construction	Length	Family Size	ZAZ / auto-ZAZ	Comments
[8, Construction 2]	XY	K	$(-\lfloor \frac{X}{K}\rfloor, \lfloor \frac{X}{K}\rfloor)\times(-Y,Y)$ / $(-X,X)\times(-Y,Y)$	$Y \equiv XY \pmod 2$
[20, Corollary 1]	MN^2	MN	$(-\lfloor \frac{N}{Y}\rfloor, \lfloor \frac{N}{Y}\rfloor)\times(-Y,Y)$ / $(-\lfloor \frac{N}{Y}\rfloor, \lfloor \frac{N}{Y}\rfloor)\times(-Y,Y)$	$\gcd(N,Y)=1$
[20, Theorem 3]	$X(XY+P)$	X	$(-X,X)\times(-Y,Y)$ / $(-X,X)\times(-Y,Y)$	$\gcd(P,XY)=1$
Theorem 1 with $K>1$	XY	K	$(-X,X)\times(-\lfloor \frac{Y}{K}\rfloor, \lfloor \frac{Y}{K}\rfloor)$ / $(-X,X)\times(-Y,Y)$	No constraint

*Auto-ZAZs are shown for completeness and are not necessarily (strictly or asymptotically) optimal.

including the case with $K = 1$. Unlike the construction in [8, Theorem 8], the proposed construction in Theorem 1 covers the parameters X and Y where X is even and Y is odd.

Remark 4: Table II compares the known constructions by others for families of polyphase sequences with an (asymptotically or strictly) optimal rectangular ZAZ (with respect to the Ye–Zhou–Fan–Liu–Lei–Tang cross-ZAZ bound) to Theorem 1 with $K > 1$. Some observations from Table II are the following:

1) Constructions in [8, Construction 2] and Theorem 1 result in a strictly optimal rectangular ZAZ. The rectangular ZAZ becomes strictly optimal when $K|X$ in [8, Construction 2] and when $K|Y$ in Theorem 1.
2) Constructions in [8, Construction 2] and Theorem 1 always result in a strictly optimal rectangular auto-ZAZ for individual member sequences.
3) Unlike all others, Theorem 1 has no constraint on the parameters, X and Y.

According to Theorem 1, designing polyphase sequences with an optimal rectangular ZAZ essentially involves selecting some (not necessarily distinct) appropriate polyphase perfect sequences. Zadoff-Chu polyphase perfect sequences are famous and they exist for arbitrary lengths [52], [53]. Some other perfect sequences are reported in [54], [55], [56], and [57] including Fermat-quotient sequences in [58].

B. Unique Form of the Polyphase Sequences With an Optimal Rectangular Auto-ZAZ

The converse of Theorem 1 with $K = 1$ turns out to be true.

Theorem 2: *Let $X > 1$ and Y be positive integers and $L = XY$. Consider an auto-ZAZ Π_a in (9). Any polyphase sequence $\boldsymbol{a} = \{a(t)\}_{t=0}^{L-1}$ of length L with the optimal auto-ZAZ Π_a (attaining the Ye–Zhou–Fan–Liu–Lei–Tang auto-ZAZ bound) can be represented as*

$$a(t) = g(t \bmod X)\omega_L^{ct}, \quad t = 0, 1, \ldots, L-1 \qquad (12)$$

for some polyphase perfect sequence $\boldsymbol{g} = \{g(t)\}_{t=0}^{X-1}$ of length X and some integer $c \in \{0, 1, \ldots, Y-1\}$.

Proof: For any two integers τ and ν, let $\boldsymbol{a}^{(\tau,\nu)} = \{a^{(\tau,\nu)}(t)\}_{t=0}^{L-1}$ be a sequence given by

$$a^{(\tau,\nu)}(t) \triangleq a(t+\tau)\omega_L^{\nu t}.$$

Authorized licensed use limited to: Yonsei Univ. Downloaded on May 26,2026 at 02:31:12 UTC from IEEE Xplore. Restrictions apply.

Consider two distinct integer pairs (τ_0, ν_0) and (τ_1, ν_1). Then, by Lemma 2, the inner product between $\boldsymbol{a}^{(\tau_0,\nu_0)}$ and $\boldsymbol{a}^{(\tau_1,\nu_1)}$ can be calculated as follows.

$$< \boldsymbol{a}^{(\tau_0,\nu_0)}, \boldsymbol{a}^{(\tau_1,\nu_1)} >= \omega_L^{-\tau_1(\nu_0-\nu_1)} F(\boldsymbol{a}; \tau_0 - \tau_1, \nu_0 - \nu_1).$$

Therefore, $\boldsymbol{a}^{(\tau_0,\nu_0)}$ and $\boldsymbol{a}^{(\tau_1,\nu_1)}$ are orthogonal to each other whenever $(\tau_0 - \tau_1, \nu_0 - \nu_1) \in \Pi_a \cap \mathbb{Z}^2 \backslash \{(0,0)\}$. This implies that they are orthogonal to each other whenever (τ_0, ν_0) and (τ_1, ν_1) are two distinct points in a rectangular region composed of XY integer coordinates in the (τ, ν)-plane, where the range of τ-coordinates consists of X adjacent integers and the range of ν-coordinates consists of Y adjacent integers. Moreover, the number of sequences $\boldsymbol{a}^{(\tau,\nu)}$ corresponding to (τ, ν) within that region is $L = XY$. Since each $\boldsymbol{a}^{(\tau,\nu)}$ is an element of $\mathbb{C}^L$, the set of $\boldsymbol{a}^{(\tau,\nu)}$ corresponding to the points (τ, ν) within that region forms an orthogonal basis of $\mathbb{C}^L$. For example, we consider the following four sets as 4 possibly distinct orthogonal bases of $\mathbb{C}^L$:

$$A \triangleq \{\boldsymbol{a}^{(\tau,\nu)} | (\tau, \nu) \in \{0, 1, \ldots, X-1\} \times \{0, 1, \ldots, Y-1\}\},$$
$$B \triangleq \{\boldsymbol{a}^{(\tau,\nu)} | (\tau, \nu) \in \{0, 1, \ldots, X-1\} \times \{1, 2, \ldots, Y\}\},$$
$$C \triangleq \{\boldsymbol{a}^{(\tau,\nu)} | (\tau, \nu) \in \{1, 2, \ldots, X\} \times \{0, 1, \ldots, Y-1\}\},$$
$$D \triangleq \{\boldsymbol{a}^{(\tau,\nu)} | (\tau, \nu) \in \{1, 2, \ldots, X\} \times \{1, 2, \ldots, Y\}\}.$$

Therefore, we have

$$\mathbb{C}^L = \mathrm{span}(A) = \mathrm{span}(B) = \mathrm{span}(C) = \mathrm{span}(D),$$

where $\mathrm{span}(\cdot)$ denotes the linear span of a set, i.e., the collection of all finite linear combinations of its elements. This implies

$$\mathrm{span}(A \backslash (A \cap C)) = \mathrm{span}(C \backslash (A \cap C)) = \mathrm{span}(A \cap C)^{\perp} \text{ and}$$
$$\mathrm{span}(B \backslash (B \cap D)) = \mathrm{span}(D \backslash (B \cap D)) = \mathrm{span}(B \cap D)^{\perp}.$$

Let

$$U_0 \triangleq A \backslash (A \cap C) = \{\boldsymbol{a}^{(0,\nu)} | \nu \in \{0, 1, \ldots, Y-1\}\},$$
$$U_1 \triangleq C \backslash (A \cap C) = \{\boldsymbol{a}^{(X,\nu)} | \nu \in \{0, 1, \ldots, Y-1\}\},$$
$$V_0 \triangleq B \backslash (B \cap D) = \{\boldsymbol{a}^{(0,\nu)} | \nu \in \{1, 2, \ldots, Y\}\},$$
$$V_1 \triangleq D \backslash (B \cap D) = \{\boldsymbol{a}^{(X,\nu)} | \nu \in \{1, 2, \ldots, Y\}\},$$
$$Z_0 \triangleq \{\boldsymbol{a}^{(0,\nu)} | \nu \in \{1, 2, \ldots, Y-1\}\},$$
$$Z_1 \triangleq \{\boldsymbol{a}^{(X,\nu)} | \nu \in \{1, 2, \ldots, Y-1\}\}.$$

Then,

$$\mathrm{span}(U_0) = \mathrm{span}(U_1), \tag{13}$$
$$\mathrm{span}(V_0) = \mathrm{span}(V_1), \tag{14}$$

with all the dimensions of the above in (13) and (14) equal to Y. Therefore,

$$\mathrm{span}(U_0) \cap \mathrm{span}(V_0) = \mathrm{span}(U_1) \cap \mathrm{span}(V_1), \tag{15}$$

and we are interested in the dimension of this subspace in (15). We denote this subspace by W. We then claim that W contains both $\mathrm{span}(Z_0)$ and $\mathrm{span}(Z_1)$ since

$$W = \mathrm{span}(U_0) \cap \mathrm{span}(V_0) \supset \mathrm{span}(U_0 \cap V_0) \supset \mathrm{span}(Z_0) \tag{16}$$

and also

$$W = \mathrm{span}(U_1) \cap \mathrm{span}(V_1) \supset \mathrm{span}(U_1 \cap V_1) \supset \mathrm{span}(Z_1), \tag{17}$$

since $U_0 \cap V_0 \supset Z_0$ and $U_1 \cap V_1 \supset Z_1$. Therefore,

$$\dim(W) \geq \dim(\mathrm{span}(Z_0)) = \dim(\mathrm{span}(Z_1)) = Y - 1.$$

On the other hand, since

$$W = (\mathrm{span}(U_0) \cap \mathrm{span}(V_0)) \subset \mathrm{span}(U_0) \tag{18}$$

and

$$W = (\mathrm{span}(U_0) \cap \mathrm{span}(V_0)) \subset \mathrm{span}(V_0), \tag{19}$$

we have

$$\dim(W) \leq \dim(\mathrm{span}(U_0)) = \dim(\mathrm{span}(V_0)) = Y.$$

Therefore, $\dim(W) = Y - 1$ or Y. Now, we distinguish these two cases.

Case where $\dim(W) = Y - 1$:

In this case, the three vector spaces connected by $\supset$ in (16) are the same and so are those in (17). Therefore,

$$\mathrm{span}(Z_0) = \mathrm{span}(Z_1).$$

From this and the relation in (13),

$$\mathrm{span}(U_0) \cap (\mathrm{span}(Z_0)^{\perp}) = \mathrm{span}(U_1) \cap (\mathrm{span}(Z_1)^{\perp}). \tag{20}$$

Note that LHS of the above is a 1-dimensional vector space since $\dim(\mathrm{span}(U_0)) = Y$, $\dim(\mathrm{span}(Z_0)) = Y - 1$ and $\mathrm{span}(U_0) \supset \mathrm{span}(Z_0)$. Now, we claim that $\boldsymbol{a}^{(0,0)}$ is a member of LHS of (20). By definition of U_0, $\boldsymbol{a}^{(0,0)} \in U_0$. Also, $\boldsymbol{a}^{(0,0)} \in \mathrm{span}(Z_0)^{\perp}$ since A is an orthogonal basis, $\boldsymbol{a}^{(0,0)} \in A$ and $Z_0 \subset A$. Similarly, the right-hand side (RHS) of (20) is the same 1-dimensional vector space and $\boldsymbol{a}^{(X,0)}$ is in RHS of (20). Therefore,

$$\boldsymbol{a}^{(0,0)} = \kappa \boldsymbol{a}^{(X,0)}$$

for some constant κ. That is, for all t,

$$a(t) = \kappa a(t + X) = \kappa^2 a(t + 2X) = \cdots = \kappa^Y a(t),$$

where $t + X$, $t + 2X$,...are computed mod L. Therefore, κ is a complex Y-th root of unity, and hence, we may denote it by ω_Y^{-c} for some non-negative integer $c < Y$. Let $\boldsymbol{g} = \{g(t)\}_{t=0}^{X-1}$ be a polyphase sequence of length X given by

$$g(t) \triangleq a(t)\omega_L^{-ct} \quad \text{for } t = 0, 1, \ldots, X-1.$$

Then, $\boldsymbol{a}$ can be represented as

$$a(t) = g(t \bmod X)\omega_L^{ct} \quad \text{for } t = 0, 1, \ldots, L-1.$$

Now it is sufficient to show that $\boldsymbol{g}$ is a perfect sequence. The magnitude of the ambiguity function of $\boldsymbol{a}$ at time shift τ and Doppler shift ν is given as LHS of (8) in Lemma 1 with $\boldsymbol{g} = \boldsymbol{h}$ and $l = m = c$. When $Y \nmid \nu$, it becomes zero for any τ. When $Y \mid \nu$, it becomes $Y|F(\boldsymbol{g}; \tau \bmod X, \nu/Y)|$ which becomes $Y|C(\boldsymbol{g}; \tau)|$ for $\nu = 0$ by (2), which must be zero when $\tau \in (-X, X)$ except for $\tau = 0$ since Π_a in (9) is the given auto-ZAZ. Therefore, $\boldsymbol{g}$ must be a perfect sequence.

Authorized licensed use limited to: Yonsei Univ. Downloaded on May 26,2026 at 02:31:12 UTC from IEEE Xplore. Restrictions apply.

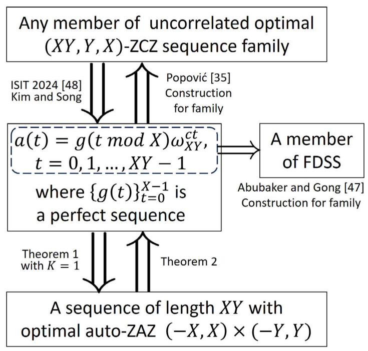


Fig. 5. Relation of various sequences in Theorem 3.

Case where $\dim(W) = Y$**:**

In this case, the two vector spaces connected by $\subset$ in (18) are the same and so are those in (19). Therefore,

$$\mathrm{span}(U_0) = \mathrm{span}(V_0),$$

and hence,

$$\mathrm{span}(U_0) \cap (\mathrm{span}(Z_0)^{\perp}) = \mathrm{span}(V_0) \cap (\mathrm{span}(Z_0)^{\perp}).$$

We now use some similar steps to the previous case. Note that both sides of the above are 1-dimensional vector spaces, $\boldsymbol{a}^{(0,0)}$ is a member of LHS of the above and $\boldsymbol{a}^{(0,Y)}$ is a member of RHS, so that

$$\boldsymbol{a}^{(0,0)} = \lambda \boldsymbol{a}^{(0,Y)}$$

for some constant λ. Comparing only the first two terms of the sequences on both sides above, we get the following:

$$a(0) = \lambda a(0) \quad \text{and} \quad a(1) = \lambda a(1)\omega_L^Y.$$

This implies that

$$\lambda = 1 = \omega_X^{-1}$$

which is impossible since $X > 1$. ∎

We now explain the relation between the polyphase sequence with rectangular optimal auto-ZAZ and any member of a polyphase uncorrelated optimal (XY, Y, X)-ZCZ sequence family by locating the equation (12) in the middle in Fig. 5. Recall that an (XY, Y, X)-ZCZ sequence family is a set of Y sequences all of length XY and the ZCZ width X. The upper box in Fig. 5 illustrates that any member of a polyphase uncorrelated optimal ZCZ sequence family always comes from the sequence of the form in the middle box, which are the combined result of Kim and Song [48] and Popović [35]. On the other hand, the lower box in the figure illustrates that a polyphase sequence with an optimal rectangular auto-ZAZ (attaining the Ye–Zhou–Fan–Liu–Lei–Tang auto-ZAZ bound) always comes from the sequence of the form in the middle box, which are the combined result of Theorems 1 and 2. In the meantime, by Abubaker and Gong [47], Y sequences of the form in the middle box with Y distinct values of c (without the condition that $\boldsymbol{g}$ has to be perfect) are defined as FDSS as we have already discussed in Remark 1.

Theorem 3: *Let $X > 1$ and Y be positive integers.*

1) *Any member of an arbitrary polyphase uncorrelated optimal (XY, Y, X)-ZCZ sequence family is a polyphase sequence of length XY with an optimal auto-ZAZ $(-X, X) \times (-Y, Y)$ (attaining the Ye–Zhou–Fan–Liu–Lei–Tang auto-ZAZ bound).*
2) *Any polyphase sequence of length XY with an optimal auto-ZAZ $(-X, X) \times (-Y, Y)$ (attaining the Ye–Zhou–Fan–Liu–Lei–Tang auto-ZAZ bound) is a member of some polyphase uncorrelated optimal (XY, Y, X)-ZCZ sequence family.*

C. Centrally Symmetric Convex ZAZs

We will derive an upper bound on the area of centrally symmetric convex ZAZs, which is similar to (5). For this, we will introduce some transformation of a bounded region on $\mathbb{R}^2$. We will generalize this to any bounded and centrally symmetric convex region. We will first introduce the notion of a "centrally symmetric convex region" in $\mathbb{R}^2$, following the definition provided in [59]:

Definition 1 *[59, p.143]*: Consider a convex region $\Pi \subset \mathbb{R}^2$ and let $-\Pi \triangleq \{(-\tau, -\nu) | (\tau, \nu) \in \Pi\}$. Then, Π is called *centrally symmetric to the origin*, or simply, *centrally symmetric*, if $\Pi = -\Pi$.

For a region $\Pi \subset \mathbb{R}^2$, consider its difference region [59, p.124] defined as

$$D(\Pi) \triangleq \frac{1}{2}(\Pi + (-\Pi))$$

$$= \{(\tau + \tau', \nu + \nu') | (\tau, \nu) \in \Pi \text{ and } (\tau', \nu') \in (-\Pi)\} \tag{21}$$

Lemma 3: *For any centrally symmetric convex region $\Pi \subset \mathbb{R}^2$, we have*

$$D(\Pi) = \Pi.$$

Proof: $(\subset)$ Consider two points $(\tau_1, \nu_1), (\tau_2, \nu_2) \in \frac{1}{2}\Pi$. Obviously, $(2\tau_1, 2\nu_1), (2\tau_2, 2\nu_2) \in \Pi$. Since Π is centrally symmetric, $(-2\tau_2, -2\nu_2) \in \Pi$. Since Π is convex,

$$\frac{1}{2}(2\tau_1, 2\nu_1) + \frac{1}{2}(-2\tau_2, -2\nu_2) = (\tau_1 - \tau_2, \nu_1 - \nu_2) \in \Pi.$$

$(\supset)$ Consider a point $(\tau, \nu) \in \Pi$. Since Π is centrally symmetric, $(-\tau, -\nu) \in \Pi$. Obviously,

$$\left(\frac{1}{2}\tau, \frac{1}{2}\nu\right) \in \frac{1}{2}\Pi \text{ and } \left(-\frac{1}{2}\tau, -\frac{1}{2}\nu\right) \in \frac{1}{2}\Pi.$$

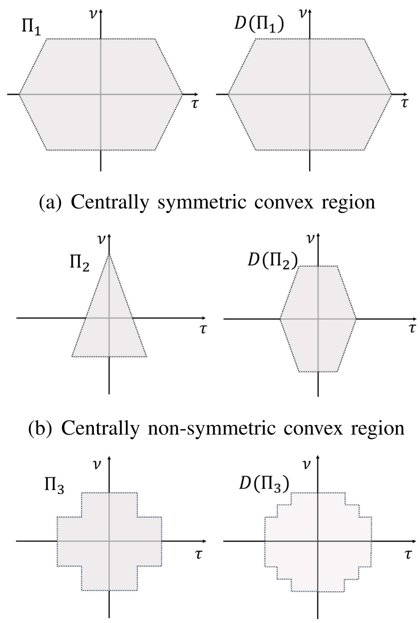
Therefore,

$$\left(\frac{1}{2}\tau, \frac{1}{2}\nu\right) - \left(-\frac{1}{2}\tau, -\frac{1}{2}\nu\right) = (\tau, \nu) \in D(\Pi).$$

∎

Fig. 6 shows three examples of bounded regions in $\mathbb{R}^2$. The first example is centrally symmetric convex, and it is equal to its difference. For the other two examples, the region and its difference are distinct.

Authorized licensed use limited to: Yonsei Univ. Downloaded on May 26,2026 at 02:31:12 UTC from IEEE Xplore. Restrictions apply.



(a) Centrally symmetric convex region

(b) Centrally non-symmetric convex region

(c) Centrally symmetric non-convex region

Fig. 6. Illustration of Lemma 3.

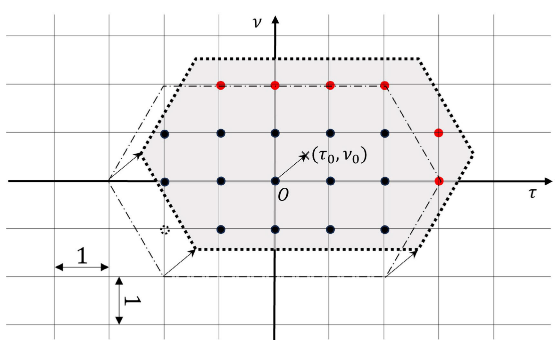


Fig. 7. An example of Blichfeldt's Theorem using an open hexagon with an area of 20.

Known-fact 7 (Blichfeldt's Theorem [49]): Consider a bounded region $\Pi \subset \mathbb{R}^2$. Then, there exists a point $(x, y) \in \mathbb{R}^2$ such that the following inequality is satisfied:

$$|((x, y) + \Pi) \cap \mathbb{Z}^2| \geq |\Pi|.$$

Fig. 7 illustrates an example of Blichfeldt's Theorem using an open hexagon with an area of 20. Note that the inequality in *Known-Fact 7* is over $\mathbb{R}$. Before translation, this hexagonal shape has area 20 but encloses only 15 integer lattice points. A slight translation to the point (τ_0, ν_0) allows it to enclose 20 integer lattice points.

Theorem 4: *For a family of K polyphase sequences of length L with centrally symmetric convex ZAZ* Π, *the following inequality holds*

$$|\Pi| \leq 4L/K. \tag{22}$$

Proof: Let $\{\boldsymbol{a}_i | i = 0, 1, \ldots, K-1\}$ be a family of K polyphase sequences of length L with a centrally symmetric convex ZAZ $\Pi \subset (-L, L)^2$. By Blichfeldt's Theorem, there exists a point $(x, y) \in \mathbb{R}^2$ such that

$$\Pi' \triangleq (x, y) + \frac{1}{2}\Pi$$

contains at least $\lceil|\frac{1}{2}\Pi|\rceil (= \lceil|\Pi|/4\rceil)$ points in $\mathbb{Z}^2$. Note that, by Lemma 3 and (21),

$$\Pi' + (-\Pi') = D(\Pi) = \Pi.$$

Therefore,

$$(\Pi' + (-\Pi')) \cap \mathbb{Z}^2 \subset \Pi. \tag{23}$$

Consider

$$\{\boldsymbol{a}_i^{(\tau,\nu)} | (\tau, \nu) \in \Pi' \cap \mathbb{Z}^2 \text{ and } i = 0, 1, \ldots, K-1\}$$

where $\boldsymbol{a}_i^{(\tau,\nu)} = \{a_i^{(\tau,\nu)}(t)\}_{t=0}^{L-1}$ is given by

$$a_i^{(\tau,\nu)}(t) \triangleq a_i(t+\tau)\omega_L^{\nu t} \quad \text{for } t = 0, 1, \ldots, L-1.$$

By Lemma 2, the inner product between $\boldsymbol{a}_{i_1}^{(\tau_1,\nu_1)}$ and $\boldsymbol{a}_{i_2}^{(\tau_2,\nu_2)}$ can be calculated as follows.

$$\begin{aligned} &< \boldsymbol{a}_{i_1}^{(\tau_1,\nu_1)}, \boldsymbol{a}_{i_2}^{(\tau_2,\nu_2)} > \\ &= \omega_L^{-(\nu_1-\nu_2)\tau_2} F(\boldsymbol{a}_{i_1}, \boldsymbol{a}_{i_2}; \tau_1 - \tau_2, \nu_1 - \nu_2). \end{aligned}$$

Since $(\tau_1 - \tau_2, \nu_1 - \nu_2) \in \Pi$ by (23), the above becomes 0. Therefore, all the $K|\Pi' \cap \mathbb{Z}^2|$ sequences $\boldsymbol{a}_i^{(\tau,\nu)}$ with $(\tau, \nu) \in \Pi' \cap \mathbb{Z}^2$ and $i = 0, 1, \ldots, K-1$ are mutually orthogonal. Since each sequence $\boldsymbol{a}_i^{(\nu,\tau)}$ lies in L-dimensional vector space $\mathbb{C}^L$,

$$K|\Pi' \cap \mathbb{Z}^2| \leq L.$$

By definition of Π',

$$|\Pi' \cap \mathbb{Z}^2| \geq |\Pi|/4.$$

Combining these two inequalities, we complete the proof. ■

From the above theorem, the optimality of centrally symmetric convex ZAZs can be discussed. To do so, we define the optimality factor as follows.

Definition 2 (Optimality Factor): Consider a family $\mathcal{U}$ of K sequences of length L and their centrally symmetric convex ZAZ Π. Define the optimality factor $\delta(\mathcal{U}, \Pi)$ of Π for $\mathcal{U}$ as

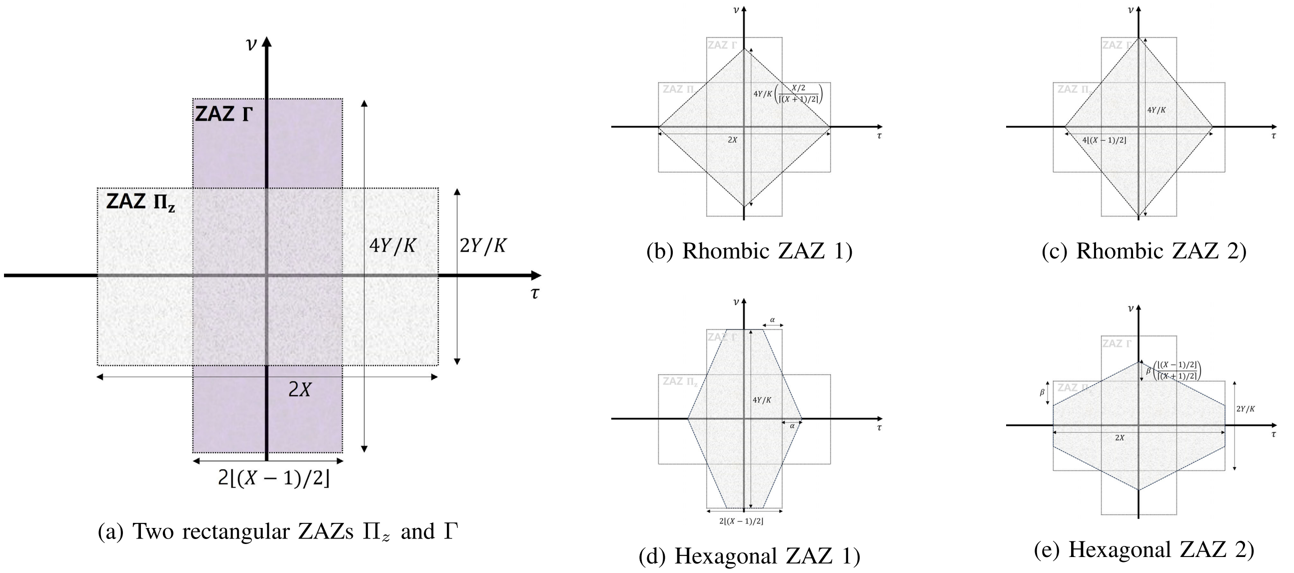
$$\delta(\mathcal{U}, \Pi) \triangleq \frac{|\Pi|}{4L/K}.$$

The optimality factor is less than or equal to 1 and greater than 0. We may say that the closer it is to 1, the closer it is to achieving the optimal ZAZ with respect to the proposed cross-ZAZ bound in Theorem 4 (which, in the rectangular case, specializes to the Ye–Zhou–Fan–Liu–Lei–Tang cross-ZAZ bound).

D. Families of Polyphase Sequences With Dual Asymptotically Optimal Rectangular ZAZs

We construct some polyphase sequence families that simultaneously possess two rectangular ZAZs from Theorem 1 with two different but some specific choices of perfect sequences. The input perfect sequences in Theorem 5 are selected to be some cyclically distinct Zadoff-Chu sequences [53]. One

Authorized licensed use limited to: Yonsei Univ. Downloaded on May 26,2026 at 02:31:12 UTC from IEEE Xplore. Restrictions apply.



(a) Two rectangular ZAZs Π_z and Γ

(b) Rhombic ZAZ 1)

(c) Rhombic ZAZ 2)

(d) Hexagonal ZAZ 1)

(e) Hexagonal ZAZ 2)

Fig. 8. Various forms of centrally symmetric convex ZAZs in Remark 5 (from Theorem 5).

single perfect sequence and its cyclically shifted versions are used in Theorem 6. Therefore, the proposed sequence families in both theorems are already known to possess a ZAZ Π_z in (10) from Theorem 1. They will be shown to possess an additional ZAZ in the following.

Theorem 5: *Consider the sequence set* $\{\boldsymbol{a}_i | i = 0, 1, \ldots, K-1\}$ *using the perfect sequences* $\{\boldsymbol{g}_i | i = 0, 1, \ldots, K-1\}$ *in Theorem 1 where* $\boldsymbol{g}_i$ *for* $i = 0, 1, \ldots, K-1$ *are given as*

$$g_i(t) \triangleq \omega_{2X}^{Bt(t-2\lfloor iA/K \rfloor + (X \bmod 2))} \text{ for } t = 0, 1, \ldots, X-1, \tag{24}$$

where $A < KX$ *is a positive integer with* $\gcd(A, X) = 1$ *and* $B < X$ *is an integer with* $BA \equiv 1 \pmod X$. *Then,* $\{\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{K-1}\}$ *has a ZAZ* Γ *given by*

$$\Gamma \triangleq \left(-\left\lfloor \frac{A}{K} \right\rfloor, \left\lfloor \frac{A}{K} \right\rfloor\right) \times \left(-\left\lfloor \left\lfloor \frac{KX}{A} \right\rfloor \frac{Y}{K} \right\rfloor, \left\lfloor \left\lfloor \frac{KX}{A} \right\rfloor \frac{Y}{K} \right\rfloor\right) \tag{25}$$

in addition to the ZAZ Π_z *in (10).*

An example shape of Γ in (25) is shown in Fig. 8 (a). The proof of this theorem will be given in Appendix A.

Remark 5: Assume that $K|Y$ and A is equal to either $\left\lfloor \frac{KX-1}{2} \right\rfloor$ or $\left\lfloor \frac{KX-3}{2} \right\rfloor$ in Theorem 5. Note that X is relatively prime to either $\left\lfloor \frac{KX-1}{2} \right\rfloor$ or $\left\lfloor \frac{KX-3}{2} \right\rfloor$. Consider the sequence set $\mathcal{U} \triangleq \{\boldsymbol{a}_i | i = 0, 1, \ldots, K-1\}$ and its two rectangular ZAZs Π_z and Γ in Theorem 5.

- The ZAZ Γ becomes
$$\Gamma = \left(-\left\lfloor \frac{X-1}{2} \right\rfloor, \left\lfloor \frac{X-1}{2} \right\rfloor\right) \times \left(-\frac{2Y}{K}, \frac{2Y}{K}\right).$$
Therefore, the optimality factor $\delta(\mathcal{U}, \Gamma)$ becomes
$$\delta(\mathcal{U}, \Gamma) = \frac{\lfloor (X-1)/2 \rfloor}{X/2}. \tag{26}$$
It asymptotically approaches 1 as X increases. Therefore, it is asymptotically optimal with respect to the Ye–Zhou–Fan–Liu–Lei–Tang cross-ZAZ bound.
- The family $\mathcal{U}$ also has a ZAZ $\Pi_z \cup \Gamma$ as in Fig. 8 (a). Therefore, as illustrated in Fig. 8 (b), (c), (d), and (e), it has various shapes of centrally symmetric convex ZAZs. Each ZAZ depicted in these figures has an optimality factor that is greater than or equal to $\delta(\mathcal{U}, \Gamma)$ in (26), and less than or equal to $\delta(\mathcal{U}, \Pi_z) = 1$. The value or range of the optimality factor for the ZAZ corresponding to each figure is calculated as follows:
  - Fig. 8 (b): $\frac{X/2}{\lceil (X+1)/2 \rceil}$
  - Fig. 8 (c) and (d): $\frac{\lfloor (X-1)/2 \rfloor}{X/2}$
  - Fig. 8 (e): $1 - \frac{\beta K}{2Y}\left(1 - \frac{\lfloor (X-1)/2 \rfloor}{\lceil (X+1)/2 \rceil}\right)$ for $0 < \beta < Y/K$ (greater than $\frac{X/2}{\lceil (X+1)/2 \rceil}$, less than 1)

  All these optimality factors asymptotically approach 1 as X increases. Therefore, all the ZAZs depicted in Fig. 8(b), (c), (d) and (e) are asymptotically optimal with respect to the proposed cross-ZAZ bound in Theorem 4.

Theorem 6: *Assume that* X *is even and* $K|Y$ *in Theorem 1. We further assume that* $K \geq 3$. *Consider the sequence set* $\{\boldsymbol{a}_i | i = 0, 1, \ldots, K-2\}$ *using the perfect sequences* $\{\boldsymbol{g}_i | i = 0, 1, \ldots, K-2\}$ *in Theorem 1 where* $\boldsymbol{g}_i = \{g_i(t)\}_{t=0}^{X-1}$ *for* $i = 0, 1, \ldots, K-2$ *are given as*

$$g_i(t) \triangleq g(t + iX/2 \bmod X) \quad \text{for } t = 0, 1, \ldots, X-1,$$

where $\boldsymbol{g} = \{g(t)\}_{t=0}^{X-1}$ *is any given perfect sequence of length* X. *Then* $\{\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{K-2}\}$ *has a ZAZ* Λ *given by*

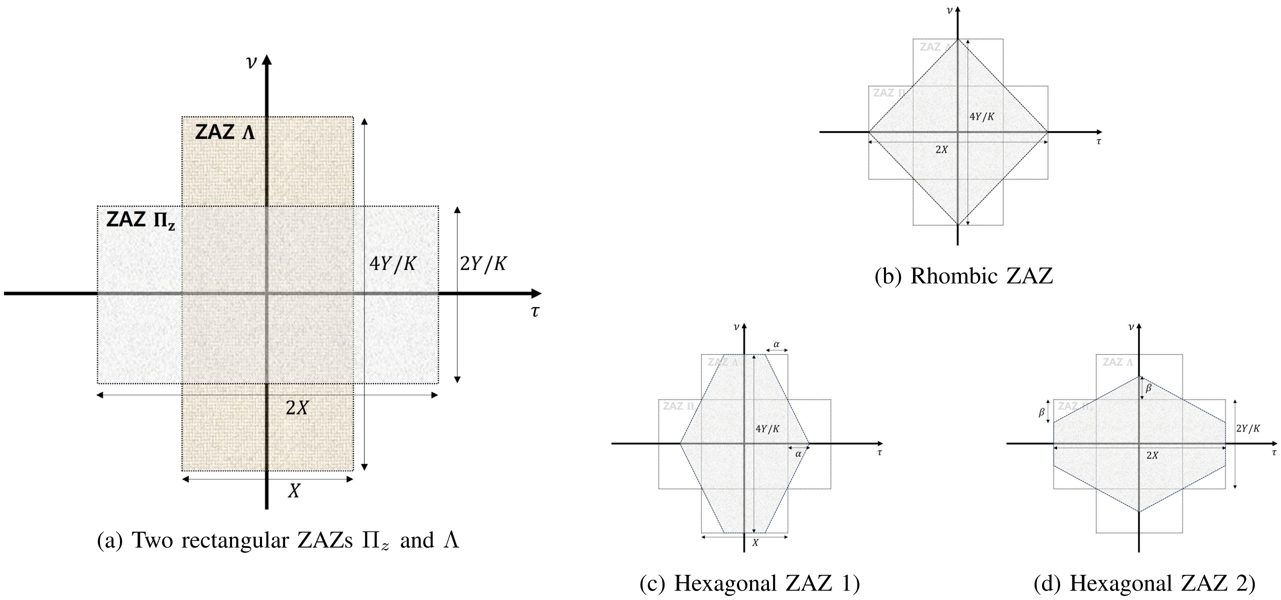
$$\Lambda \triangleq (-X/2, X/2) \times (-2Y/K, 2Y/K) \tag{27}$$

in addition to the ZAZ Π_z *in (10) where* $|\Lambda| = |\Pi_z|$.

An example shape of Λ in (27) is shown in Fig. 9 (a). The proof of this theorem will be given in Appendix B.

Remark 6: In Theorem 6, with $\boldsymbol{a}_{K-1}$ missing from the family, we have Λ as an additional ZAZ with the same area as Π_z, which are not strictly but asymptotically optimal with respect to the Ye–Zhou–Fan–Liu–Lei–Tang cross-ZAZ bound.

Authorized licensed use limited to: Yonsei Univ. Downloaded on May 26,2026 at 02:31:12 UTC from IEEE Xplore. Restrictions apply.



(a) Two rectangular ZAZs Π_z and Λ

(b) Rhombic ZAZ

(c) Hexagonal ZAZ 1)

(d) Hexagonal ZAZ 2)

Fig. 9. Various forms of centrally symmetric convex ZAZs in Remark 6 (from Theorem 6).

Furthermore, in addition to Π_z and Λ, we have many other shapes as depicted in Fig. 9. Note that Π_z and Λ have the same area, with the horizontal side of Π_z being twice that of Λ, and the vertical side of Λ being twice that of Π_z. From this fact, it follows that all the ZAZs depicted in Fig. 9 (b), (c) and (d) have the same area as Π_z and Λ. Therefore, they have the same optimality factor, which is calculated as

$$\frac{K-1}{K}.$$

It asymptotically approaches 1 as K increases. Therefore, they are all asymptotically optimal with respect to the proposed cross-ZAZ bound in Theorem 4.

IV. Concluding Remarks

In this paper, we proved that a polyphase sequence with an optimal rectangular auto-ZAZ (attaining the Ye–Zhou–Fan–Liu–Lei–Tang auto-ZAZ bound) must be a member of some uncorrelated optimal ZCZ sequence family and conversely, any member of an uncorrelated optimal ZCZ sequence family has an optimal rectangular auto-ZAZ. We also proposed an upper bound on the area of centrally symmetric convex ZAZs in general, further expanding the design space for ISAC waveforms. In addition, we proposed some constructions of families of polyphase sequences with a (1) strictly or asymptotically optimal rectangular ZAZ (attaining the Ye–Zhou–Fan–Liu–Lei–Tang cross-ZAZ bound), (2) dual asymptotically optimal rectangular ZAZs, and (3) asymptotically optimal rhombic or hexagonal ZAZ (asymptotically attaining the proposed cross-ZAZ bound) from the flexible ZAZ configuration.

Here are some open problems for further investigation:

1) Does there exist a family of polyphase sequences with two non-trivial strictly optimal rectangular ZAZs (each attaining the Ye–Zhou–Fan–Liu–Tang–Fan cross-ZAZ bound)?
2) Does there exist a family of polyphase sequences with a strictly optimal ZAZ that is not a rectangle (i.e., attaining the proposed bound for some non-rectangular cyclically symmetric convex shape)?
3) Can constraints on the area of centrally symmetric convex LAZs be established, analogous to the upper bounds we derived for the area of centrally symmetric convex ZAZs? The bound on the area of rectangular LAZs was studied in [8], but such constraint for centrally symmetric convex LAZs remains unexplored.

Appendix

A. Proof of Theorem 5

We will prove that the magnitude of the ambiguity function between $\boldsymbol{a}_i$ and $\boldsymbol{a}_j$ at time shift τ and Doppler shift ν becomes zero whenever $(\tau,\nu) \in \Gamma$. Note that any $(\tau,\nu) \in \Gamma$ satisfies either $Y | (\lfloor iY/K \rfloor - \lfloor jY/K \rfloor + \nu)$ or not. Easy case is for those $(\tau,\nu) \in \Gamma$ with $Y \nmid (\lfloor iY/K \rfloor - \lfloor jY/K \rfloor + \nu)$. By Lemma 1, the magnitude of the ambiguity function in this case becomes zero, since $l = \lfloor iY/K \rfloor$ and $m = \lfloor jY/K \rfloor$.

For the other case, that is, for $(\tau,\nu) \in \Gamma$ with $Y | (\lfloor iY/K \rfloor - \lfloor jY/K \rfloor + \nu)$, by Lemma 1 again, the magnitude becomes Y times the following magnitude:

$$|F(\boldsymbol{g}_i, \boldsymbol{g}_j; \tau \bmod X, \alpha)|,$$

where

$$\alpha \triangleq (\lfloor iY/K \rfloor - \lfloor jY/K \rfloor + \nu)/Y. \tag{28}$$

Then,

$$\begin{aligned} &F(\boldsymbol{g}_i, \boldsymbol{g}_j; \tau \bmod X, \alpha) \\ &= \sum_{t=0}^{X-1} g_i(t+\tau \bmod X) g_j^*(t) \omega_X^{\alpha t} \\ &= \sum_{t=0}^{X-1} \left\{ \omega_{2X}^{B(t+\tau)(t+\tau-2\lfloor iA/K \rfloor + (X \bmod 2))} \right. \end{aligned}$$

Authorized licensed use limited to: Yonsei Univ. Downloaded on May 26,2026 at 02:31:12 UTC from IEEE Xplore. Restrictions apply.

$$\omega_{2X}^{-Bt(t-2\lfloor jA/K\rfloor+(X \bmod 2))}\omega_X^{BA\alpha t}\Big\}$$
$$= \omega_{2X}^{z}\sum_{t=0}^{X-1}\omega_X^{B(\tau-\lfloor iA/K\rfloor+\lfloor jA/K\rfloor+A\alpha)t},$$

where z is some integer independent of t. Since B is coprime with X, the above is non-zero if and only if

$$\tau - \lfloor iA/K\rfloor + \lfloor jA/K\rfloor + A\alpha = \eta X, \quad (29)$$

from some integer η.

We claim that if $(\tau,\nu) \in \Gamma$ satisfies (29), then $i = j$ and $(\tau,\nu) = (0,0)$. This will complete the proof that Γ is indeed a ZAZ. From the definition of α in (28), we have

$$\nu = \alpha Y - (\lfloor iY/K\rfloor - \lfloor jY/K\rfloor). \quad (30)$$

Since $(\tau,\nu) \in \Gamma$ in (25), we see that

$$-\left\lfloor\left\lfloor\frac{KX}{A}\right\rfloor\frac{Y}{K}\right\rfloor < \nu < \left\lfloor\left\lfloor\frac{KX}{A}\right\rfloor\frac{Y}{K}\right\rfloor.$$

Substituting ν in (30) into the above, we have:

$$-\left\lfloor\left\lfloor\frac{KX}{A}\right\rfloor\frac{Y}{K}\right\rfloor<\alpha Y-\left(\left\lfloor\frac{iY}{K}\right\rfloor-\left\lfloor\frac{jY}{K}\right\rfloor\right)<\left\lfloor\left\lfloor\frac{KX}{A}\right\rfloor\frac{Y}{K}\right\rfloor \quad (31)$$

From the left inequality of (31) and by the superadditivity of the floor function,

$$\left\lfloor(i-\alpha K)\frac{Y}{K}\right\rfloor < \left\lfloor\left\lfloor\frac{KX}{A}\right\rfloor\frac{Y}{K}\right\rfloor + \left\lfloor\frac{jY}{K}\right\rfloor \le \left\lfloor\left(\left\lfloor\frac{KX}{A}\right\rfloor + j\right)\frac{Y}{K}\right\rfloor.$$

It implies that $i-\alpha K < \lfloor\frac{KX}{A}\rfloor + j$, so that

$$i - j - \alpha K \le \left\lfloor\frac{KX}{A}\right\rfloor - 1. \quad (32)$$

From the right inequality of (31) and by the superadditivity of the floor function,

$$\left\lfloor(\alpha K + j)\frac{Y}{K}\right\rfloor < \left\lfloor\left\lfloor\frac{KX}{A}\right\rfloor\frac{Y}{K}\right\rfloor + \left\lfloor\frac{iY}{K}\right\rfloor \le \left\lfloor\left(\left\lfloor\frac{KX}{A}\right\rfloor + i\right)\frac{Y}{K}\right\rfloor.$$

It implies that $\alpha K + j < \lfloor KX/A\rfloor + i$. Therefore, combining with (32), we have

$$-\left(\left\lfloor\frac{KX}{A}\right\rfloor - 1\right) \le i - j - \alpha K \le \left\lfloor\frac{KX}{A}\right\rfloor - 1. \quad (33)$$

On the other hand, we will proceed with the range of τ. From the relation in (29), we have

$$\tau = \left\lfloor\left(i + \frac{\eta KX}{A}\right)\frac{A}{K}\right\rfloor - \left\lfloor(j+\alpha K)\frac{A}{K}\right\rfloor. \quad (34)$$

Since $(\tau,\nu) \in \Gamma$ in (25), we see that

$$-\left\lfloor\frac{A}{K}\right\rfloor < \tau < \left\lfloor\frac{A}{K}\right\rfloor. \quad (35)$$

Substituting τ in (34) into the above, we have

$$-\left\lfloor\frac{A}{K}\right\rfloor<\left\lfloor\left(i+\frac{\eta KX}{A}\right)\frac{A}{K}\right\rfloor-\left\lfloor(j+\alpha K)\frac{A}{K}\right\rfloor<\left\lfloor\frac{A}{K}\right\rfloor \quad (36)$$

By the superadditivity of the floor function, the left inequality of (36) implies the following:

$$\begin{aligned}
&\left\lfloor(j+\alpha K)\frac{A}{K}\right\rfloor\\
&< \left\lfloor\frac{A}{K}\right\rfloor + \left\lfloor\left(i+\frac{\eta KX}{A}\right)\frac{A}{K}\right\rfloor\\
&\le \left\lfloor\left(1+i+\frac{\eta KX}{A}\right)\frac{A}{K}\right\rfloor\\
&\le \left\lfloor\left(j+\alpha K+\left\lfloor\frac{KX}{A}\right\rfloor+\frac{\eta KX}{A}\right)\frac{A}{K}\right\rfloor \quad \text{by (33)}\\
&\le \left\lfloor\left(j+\alpha K+\frac{(\eta+1)KX}{A}\right)\frac{A}{K}\right\rfloor.
\end{aligned}$$

Therefore, we have

$$\eta \ge 0. \quad (37)$$

Similarly, the right inequality of (36) implies the following:

$$\begin{aligned}
\left\lfloor\left(i+\frac{\eta KX}{A}\right)\frac{A}{K}\right\rfloor &< \left\lfloor\frac{A}{K}\right\rfloor + \left\lfloor(j+\alpha K)\frac{A}{K}\right\rfloor\\
&\le \left\lfloor(1+j+\alpha K)\frac{A}{K}\right\rfloor\\
&\le \left\lfloor\left(i+\left\lfloor\frac{KX}{A}\right\rfloor\right)\frac{A}{K}\right\rfloor \quad \text{by (33)}\\
&\le \left\lfloor\left(i+\frac{KX}{A}\right)\frac{A}{K}\right\rfloor.
\end{aligned}$$

Therefore, $\eta \le 0$, and hence, we must have by (37)

$$\eta = 0.$$

Then, from (29),

$$\tau = \lfloor(i-\alpha K)A/K\rfloor - \lfloor jA/K\rfloor.$$

If $i - \alpha K > j$, then

$$\begin{aligned}\tau &= \lfloor(i-\alpha K)A/K\rfloor - \lfloor jA/K\rfloor\\ &\ge \lfloor(i-\alpha K-j)A/K\rfloor \ge \lfloor A/K\rfloor.\end{aligned}$$

If $i - \alpha K < j$, then

$$\begin{aligned}\tau &= -(-\lfloor(i-\alpha K)A/K\rfloor + \lfloor jA/K\rfloor)\\ &\le -\lfloor(j-(i-\alpha K))A/K\rfloor \le -\lfloor A/K\rfloor.\end{aligned}$$

The value τ then falls outside the range in (35) in both cases. Therefore, $i - \alpha K = j$ or

$$\alpha K = i - j.$$

Since $0 \le i, j < K$, this implies that $\alpha = 0$. Then, we have $i = j$, $\alpha = 0$ and $\eta = 0$, and hence, $(\tau,\nu) = (0,0)$ by (34) and (30).■

B. Proof of Theorem 6

When $i = j$, by Theorem 1, the magnitude of $F(\boldsymbol{a}_i, \boldsymbol{a}_i; \tau, \nu)$ becomes 0 for any $(\tau,\nu) \in \Lambda \subset \Pi_a$, where Π_a is given in (9).

We now assume that $i \ne j$. The magnitude $F(\boldsymbol{a}_i, \boldsymbol{a}_j; \tau, \nu)$ becomes 0 for $(\tau,\nu) \in \Lambda$ such that

$$Y \nmid (\nu + (i-j)Y/K), \quad (38)$$

by Lemma 1, since $K|Y$,

$$l = iY/K \quad \text{and} \quad m = jY/K.$$

Authorized licensed use limited to: Yonsei Univ. Downloaded on May 26,2026 at 02:31:12 UTC from IEEE Xplore. Restrictions apply.

We first claim that (38) becomes true if $(|i-j| \bmod K) \geq 2$ for $(\tau, \nu) \in \Lambda$. Assume $i > j$ WOLG. Then, from the range of ν in Λ,

$$(-2+i-j)Y/K < \nu + (i-j)Y/K < (2+i-j)Y/K. \quad (39)$$

Since $2 \leq i-j \leq K-2$, this implies that

$$0 < \nu + (i-j)Y/K < Y,$$

which implies that $\nu + (i-j)Y/K$ cannot be a multiple of Y. This proves the claim and it is now sufficient to show that

$$F(\boldsymbol{a}_i, \boldsymbol{a}_j; \tau, \nu) = 0 \quad \text{for } j = i+1 \text{ and } (\tau, \nu) \in \Lambda$$

for any $i = 0, 1, \ldots, K-3$.

Observe that $\nu + (i-j)Y/K = \nu - Y/K$ for $j = i+1$. When $\nu - Y/K$ is not a multiple of Y, the magnitude of the ambiguity function will be 0 by Lemma 1. On the other hand, assume that $Y|(\nu - Y/K)$. Since the inequality (39) becomes

$$-3Y/K < \nu - Y/K < Y/K,$$

for $j = i+1$, the only possible ν in Λ is $\nu = Y/K$. For this ν, the magnitude of the ambiguity function can be expressed as, by Lemma 1:

$$\begin{aligned} |F(\boldsymbol{a}_i, \boldsymbol{a}_{i+1}; \tau, \nu)| &= Y|F(\boldsymbol{g}_i, \boldsymbol{g}_{i+1}; \tau, (\nu - Y/K)/Y))| \\ &= Y|F(\boldsymbol{g}_i, \boldsymbol{g}_{i+1}; \tau, 0)| \\ &= Y|C(\boldsymbol{g}_i, \boldsymbol{g}_{i+1}; \tau)|. \end{aligned}$$

Since $\boldsymbol{g}_i$ and $\boldsymbol{g}_{i+1}$ are the same perfect sequences but cyclically shifted by $X/2$, the above is non-zero only at $\tau \equiv X/2 \pmod X$. Therefore, the above must be zero for $\tau \in (-X/2, X/2)$. ■

References

[1] F. Liu et al., "Integrated sensing and communications: Toward dual-functional wireless networks for 6G and beyond," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 6, pp. 1728–1767, Jun. 2022.

[2] Y. Cui, F. Liu, X. Jing, and J. Mu, "Integrating sensing and communications for ubiquitous IoT: Applications, trends, and challenges," *IEEE Netw.*, vol. 35, no. 5, pp. 158–167, Sep. 2021.

[3] F. Liu, C. Masouros, A. P. Petropulu, H. Griffiths, and L. Hanzo, "Joint radar and communication design: Applications, state-of-the-art, and the road ahead," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3834–3862, Jun. 2020.

[4] G. Gong, "Character sums and polyphase sequence families with low correlation, DFT and ambiguity," in *Character Sums and Polynomials*. Berlin, Germany: De Gruyter, 2013, pp. 1–43.

[5] K.-U. Schmidt, "Sequence families with low correlation derived from multiplicative and additive characters," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2291–2294, Apr. 2011.

[6] Z. Wang and G. Gong, "New sequences design from Weil representation with low two-dimensional correlation in both time and phase shifts," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4600–4611, Jul. 2011.

[7] Z. Wang, G. Gong, and N. Y. Yu, "New polyphase sequence families with low correlation derived from the Weil bound of exponential sums," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3990–3998, Jun. 2013.

[8] Z. Ye, Z. Zhou, P. Fan, Z. Liu, X. Lei, and X. Tang, "Low ambiguity zone: Theoretical bounds and Doppler-resilient sequence design in integrated sensing and communication systems," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 6, pp. 1809–1822, Jun. 2022.

[9] F. C. Robey, S. Coutts, D. Weikle, J. C. McHarg, and K. Cuomo, "MIMO radar theory and experimental results," in *Proc. Conf. Rec. Asilomar Conf. Signals, Syst. Comput.*, vol. 1, 2004, pp. 300–304.

[10] R. Sharma, "Analysis of MIMO radar ambiguity functions and implications on clear region," in *Proc. IEEE Radar Conf.*, May 2010, pp. 544–548.

[11] S. Stein, "Algorithms for ambiguity function processing," *IEEE Trans. Acoust., Speech, Signal Process.*, vol. ASSP-29, no. 3, pp. 588–599, Jun. 1981.

[12] Y. I. Abramovich and G. J. Frazer, "Bounds on the volume and height distributions for the MIMO radar ambiguity function," *IEEE Signal Process. Lett.*, vol. 15, pp. 505–508, 2008.

[13] G. Cui, Y. Fu, X. Yu, and J. Li, "Local ambiguity function shaping via unimodular sequence design," *IEEE Signal Process. Lett.*, vol. 24, no. 7, pp. 977–981, Jul. 2017.

[14] A. Freedman and N. Levanon, "Properties of the periodic ambiguity function," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 30, no. 3, pp. 938–941, Jul. 1994.

[15] S. W. Golomb and G. Gong, *Signal Design for Good Correlation for Wireless Communication, Cryptography, and Radar*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[16] B. Getz and N. Levanon, "Weight effects on the periodic ambiguity function," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 31, no. 1, pp. 182–193, Jan. 1995.

[17] Z. Gu, Z. Zhou, P. Fan, A. R. Adhikary, and Z. Liu, "Oversampled low ambiguity zone sequences for channel estimation over doubly selective channels," *IEEE Trans. Commun.*, vol. 73, no. 4, pp. 2616–2630, Apr. 2025.

[18] Y. Jing, J. Liang, B. Tang, and J. Li, "Designing unimodular sequence with low peak of sidelobe level of local ambiguity function," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 3, pp. 1393–1406, Jun. 2019.

[19] A. Pezeshki, A. R. Calderbank, W. Moran, and S. D. Howard, "Doppler resilient Golay complementary waveforms," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4254–4266, Sep. 2008.

[20] L. Tian, X. Song, Z. Liu, and Y. Li, "Asymptotically optimal sequence sets with low/zero ambiguity zone properties," *IEEE Trans. Inf. Theory*, vol. 71, no. 6, pp. 4785–4796, Jun. 2025.

[21] J. J. Benedetto and J. J. Donatelli, "Ambiguity function and frame-theoretic properties of periodic zero-autocorrelation waveforms," *IEEE J. Sel. Topics Signal Process.*, vol. 1, no. 1, pp. 6–20, Jun. 2007.

[22] G. E. Coxson, C. R. Hill, and J. C. Russo, "Adiabatic quantum computing for finding low-peak-sidelobe codes," in *Proc. IEEE High Perform. Extreme Comput. Conf. (HPEC)*, Sep. 2014, pp. 1–6.

[23] R. L. Haupt and S. E. Haupt, *Practical Genetic Algorithms*. Hoboken, NJ, USA: Wiley, 2004.

[24] X. Jin, S. Chae, H. Cho, H. Choi, G. Kim, and H.-Y. Song, "Zero-correlation-zone sonar sequences," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2023, pp. 892–896.

[25] X. Jin, G. Kim, S. Chae, and H.-Y. Song, "Some constructions and mathematical properties of zero-correlation-zone sonar sequences," *Entropy*, vol. 26, no. 4, p. 317, Apr. 2024.

[26] L. Meng, Y. Liang Guan, Y. Ge, Z. Liu, and P. Fan, "Generalized Arlery-Tan-Rabaste-Levenshtein lower bounds on ambiguity function and their asymptotic achievability," *IEEE Trans. Inf. Theory*, vol. 71, no. 7, pp. 5744–5754, Jul. 2025.

[27] L. Meng, Y. L. Guan, Y. Ge, and Z. Liu, "Flag sequence set design for low-complexity delay-Doppler estimation," *IEEE Trans. Veh. Technol.*, vol. 74, no. 8, pp. 12131–12147, Aug. 2025.

[28] P. Z. Fan, N. Suehiro, N. Kuroyanagi, and X. M. Deng, "A class of binary sequences with zero correlation zone," *Electron. Lett.*, vol. 35, no. 10, pp. 777–779, 1999.

[29] Q. Fang and Z. Wang, "A note on 'optimum sets of interference-free sequences with zero autocorrelation zone,'" in *Proc. IEEE 10th Int. Conf. Inf., Commun. Netw. (ICICN)*, Aug. 2022, pp. 443–464.

[30] N. Suehiro, "A signal design without co-channel interference for approximately synchronized CDMA systems," *IEEE J. Sel. Areas Commun.*, vol. 12, no. 5, pp. 837–841, Jun. 1994.

[31] 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, no. 6, pp. 1–2, 2000.

[32] A. K. Brodzik, "On certain sets of polyphase sequences with sparse and highly structured zak and Fourier transforms," *IEEE Trans. Inf. Theory*, vol. 59, no. 10, pp. 6907–6916, Oct. 2013.

[33] A. K. Brodzik, "Polyphase Golay sequences with semi-polyphase Fourier transform and all-zero crosscorrelation: Construction B," in *Excursions in Harmonic Analysis*. Cham, Switzerland: Springer, 2015, pp. 211–229.

[34] G. Kim, H. Choi, D.-K. Kim, W. Kim, X. Jin, and H.-Y. Song, "Optimal uncorrelated polyphase ZCZ sequences over an alphabet of minimum size," presented at the IEEE Int. Symp. Inf. Theory, Jun. 2023.

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

Authorized licensed use limited to: Yonsei Univ. Downloaded on May 26,2026 at 02:31:12 UTC from IEEE Xplore. Restrictions apply.

[36] D. Zhang, "Zero correlation zone sequences from a unified construction of perfect polyphase sequences," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 2269–2273.

[37] Y. Cao and Q.-Y. Yu, "A dual mode multi-beam and integrated CPM-LFM signal for dual-functional radar communication systems," *IEEE Trans. Veh. Technol.*, vol. 73, no. 10, pp. 15270–15285, Oct. 2024.

[38] S. Lee, S.-Y. Kwon, B.-J. Kim, H.-S. Lim, and J.-E. Lee, "Dual-mode radar sensor for indoor environment mapping," *Sensors*, vol. 21, no. 7, p. 2469, Apr. 2021.

[39] J.-M. Muñoz-Ferreras, Z. Peng, R. Gómez-García, and C. Li, "Review on advanced short-range multimode continuous-wave radar architectures for healthcare applications," *IEEE J. Electromagn., RF Microw. Med. Biol.*, vol. 1, no. 1, pp. 14–25, Jun. 2017.

[40] H. He, J. Li, and P. Stoica, *Waveform Design for Active Sensing Systems: A Computational Approach*. Cambridge, U.K.: Cambridge Univ. Press, 2012.

[41] G. M. Dillard, M. Reuter, J. Zeiddler, and B. Zeidler, "Cyclic code shift keying: A low probability of intercept communication technique," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 39, no. 3, pp. 786–798, Jul. 2003.

[42] K. Gilholm and D. Salmond, "Spatial distribution model for tracking extended objects," *IEE Proc.-Radar, Sonar Navigat.*, vol. 152, no. 5, pp. 364–371, Oct. 2005.

[43] V. C. Chen, F. Li, S.-S. Ho, and H. Wechsler, "Micro-Doppler effect in radar: Phenomenon, model, and simulation study," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 42, no. 1, pp. 2–21, Jan. 2006.

[44] K. J. Sangston, F. Gini, and M. S. Greco, "Coherent radar target detection in heavy-tailed compound-Gaussian clutter," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 48, no. 1, pp. 64–77, Jan. 2012.

[45] R. Rytel-Andrianik, "On the ambiguity function for accelerating target in FMCW radar," in *Proc. Int. Conf. Microw., Radar Wireless Commun.*, May 2006, pp. 207–210.

[46] J. Neyman and E. S. Pearson, "IX. On the problem of the most efficient tests of statistical hypotheses," *Phil. Trans. Roy. Soc. London. Ser., Containing Papers Math. Phys. Character*, vol. 231, nos. 694–706, pp. 289–337, Feb. 1933.

[47] R. Abubaker and G. Gong, "Frequency distance sequences for packet detection in physical-layer security: In memory of kai-uwe Schmidt," *Design Code. Cryptogr.*, vol. 93, pp. 997–1020, Aug. 2025.

[48] G. Kim and H.-Y. Song, "The unique form of the uncorrelated optimal ZCZ sequence families," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2024, pp. 1338–1342.

[49] H. F. Blichfeldt, "A new principle in the geometry of numbers, with some applications," *Trans. Amer. Math. Soc.*, vol. 15, no. 3, pp. 227–235, 1914.

[50] 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.

[51] C. L. Phillips, J. M. Parr, E. A. Riskin, and T. Prabhakar, *Signals, Systems, and Transforms*. Upper Saddle River, NJ, USA: Prentice-Hall, 2003.

[52] *Technical Specification Group Radio Access Network; NR; Physical Channels and Modulation*, document TS 38.211 v. 18.3.0, 3GPP, 2024.

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

[54] W. Ho Mow, "A unified construction of perfect polyphase sequences," in *Proc. IEEE Int. Symp. Inf. Theory*, Sep. 1995, p. 459.

[55] W. Ho Mow, "A new unified construction of perfect root-of-unity sequences," in *Proc. Int. Symp. Spread Spectr. Techn. Appl.*, vol. 3, 1996, pp. 955–959.

[56] M. K. Song and H.-Y. Song, "A construction of odd length generators for optimal families of perfect sequences," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 2901–2909, Apr. 2018.

[57] M. K. Song and H.-Y. Song, "New framework for sequences with perfect autocorrelation and optimal crosscorrelation," *IEEE Trans. Inf. Theory*, vol. 67, no. 11, pp. 7490–7500, Nov. 2021.

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

[59] D. Hug and W. Weil, *Lectures on Convex Geometry*(Graduate Text in Mathematics), vol. 286. Cham, Switzerland: Springer, 2020.

Gangsan Kim (Member, IEEE) received the B.S. and Ph.D. degrees in electronic engineering from Yonsei University, Seoul, South Korea, in 2016 and 2025, respectively. In 2022, he was an AI Science and Technology Soldier with Republic of Korea Army Training and Doctrine Command, where he focused on quantum devices and quantum information theory. He is currently a Post-Doctoral Fellow with the Research Group of Prof. Hong-Yeop Song, Yonsei University. His area of research interests include coding theory, PN sequences, related discrete mathematics, and their applications to digital communication systems.

Hong-Yeop Song (Senior Member, IEEE) received the B.S. degree in electronic engineering from Yonsei University, Seoul, South Korea, in 1984, and the M.S.E.E. and Ph.D. degrees from the University of Southern California (USC), Los Angeles, CA, USA, in 1986 and 1991, respectively. He spent two years as a Research Associate with USC. He was a Senior Engineer in Standard Team of Qualcomm Inc., San Diego, CA, for two years. Since September 1995, he has been with the Department of Electrical and Electronic Engineering, Yonsei University. His research interests include digital communications and channel coding, design and analysis of various pseudorandom sequences for communications, and cryptography. He is a member of the National Academy of Engineering of Korea (NAEK), the Mathematical Association of America (MAA), Korean Mathematical Society (KMS), KICS, IEIE, and KIISC. He was awarded the 2017 Special Contribution Award from Korean Mathematical Society and the 2021 S. J. Choi Award from Korean Government, both for his contribution to the global wide-spread of the fact that S. J. Choi (1646–1715) from South Korea had discovered a pair of orthogonal Latin squares of order nine much earlier than Euler. He has been serving for IEEE IT Society Seoul Chapter as the Chair from 2009 to 2016. He served as the General Co-Chair for IEEE ITW 2015, Jeju, South Korea.

Guang Gong (Fellow, IEEE) received the B.S. degree in mathematics from Xichang Normal College in 1981, the M.S. degree in applied mathematics from Xidian University in 1985, and the Ph.D. degree in electrical engineering from the University of Electronic Science and Technology of China (UESTC) in 1990.

She obtained a Post-Doctoral Fellowship from Fondazione Ugo Bordoni, Rome, Italy, and spent the following year there. She was promoted to the position of an Associate Professor with UESTC in 1993. She worked with Dr. Solomon W. Golomb at the University of Southern California from 1996 to 1998. She joined the University of Waterloo, Canada, in 1998, where she was an Associate Professor with the Department of Electrical and Computer Engineering in 2000 and a Full Professor in 2004. She has authored or co-authored more than 360 technical articles, two books, and three patents. Her research is supported by the Government Grant Agencies and Industrial Grants. Her research interests include pseudorandom generation, cryptography, and communication security. Currently, her research focuses on pseudorandom generation, lightweight cryptography (LWC), the IoT security, blockchain privacy, privacy preserving machine learning, and post-quantum cryptography.

Dr. Gong was a fellow of IEEE "for her contributions to sequences and cryptography applied to communications and security" in 2014. She has received several awards, including the Premier's Research Excellence Award in 2001, Ontario, Canada; Ontario Research Fund-Research Excellence Award in 2010, Canada; the University Research Chair from 2018 to 2024; The George Boole Prize in 2023; and The Cyber-security and Privacy Institute Faculty Fellow in 2024 (University of Waterloo). She has served on numerous technical program committees and conferences as the co-chair/organizer or a committee member. She serves/served as an Associate Editor for several journals, including IEEE TRANSACTIONS ON INFORMATION THEORYfrom 2005 to 2008, from 2017 to 2018, and from 2020 to 2022, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTINGfrom 2021 to 2023, and *Cryptography and Communications*since 2007.

Authorized licensed use limited to: Yonsei Univ. Downloaded on May 26,2026 at 02:31:12 UTC from IEEE Xplore. Restrictions apply.