The Role of the Ambiguity Function in Waveform Design and Phase coded Waveforms

John J. Benedetto, Ioannis Konstantinidis, Member, IEEE, and Muralidhar Rangaswamy, Fellow, IEEE

Abstract

CAZAC (Constant Amplitude Zero Auto-Correlation) sequences are important in waveform design because of their optimal transmission efficiency and tight time localization properties. Certain classes of CAZAC sequences have been used in radar processing for many years, while recently discovered sequences invite further study. This paper compares different classes of CAZAC sequences with respect to the discrete periodic and aperiodic ambiguity function; and it analyzes the ambiguity function behavior of the phase coded waveforms associated with given CAZACs. The techniques are taken from classical signal processing methodologies, as well as from number theoretic and frame theoretic ideas which arise in a natural way. Computational results for different CAZAC classes are presented.

Index Terms

CAZAC sequence, ambiguity function, frame theory

This work was supported in part by the Department of the Navy, Office of Naval Research under Grant No. N00014-02-1-0398 and the Air Force Office of Scientific Research (AFOSR)under MURI grant AFOSR–FA9550–05–1–0443. Dr. Rangaswamy was supported by AFOSR under project 2311.

John J. Benedetto and Ioannis Konstantinidis are with the Norbert Wiener Center, Department of Mathematics, University of Maryland, College Park, MD 20782. Muralidhar Rangaswamy is with the Sensors Directorate of the Air Force Research Laboratory (AFRL), Hanscom Air Force Base, MA.

The Role of the Ambiguity Function in Waveform Design and Phase coded Waveforms

I. INTRODUCTION

The design of radar waveforms has received considerable attention since the 1950s. In 1953, P.M. Woodward [Woo53b], [Woo53a] defined the *narrow band radar ambiguity function* or, simply, *ambiguity function*. It is a device formulated to describe the effects of range and Doppler on matched filter receivers (see the Appendix). Woodward acknowledged the influence of Shannon's communication theory, from 1948, on his ideas; and he explained the relevance of "ambiguity" in radar signal processing, perhaps best conceived in terms of a form of the uncertainty principle (see Sections II and III). His book [Woo53a] ends with the astonishing, self–deprecating, heartfelt, statement:

"The reader may feel some disappointment, not unshared by the writer, that the basic question

of what to transmit remains substantially unanswered."

However, in the 50 odd years since Woodward's book appeared, radar signal processing has used the ambiguity function as an intricate and flexible tool in the design of waveforms to solve diverse problems in radar. In the process, substantial connections were established in mathematics, physics, and other areas of signal processing.

The rich history of the field and limitations of space preclude the presentation of a comprehensive summary on waveform design. Therefore, we focus on a specific piece of the waveform design problem as pertaining to the use of constant amplitude zero autocorrelation sequences in this paper. Constant amplitude (CA) sequences with zero autocorrelation (ZAC), which often serve as coefficients of the translates of the sampling function used to design a given waveform, arise naturally in a host of problems associated with radar, communications, coding theory, and various areas of signal processing. There are major books and surveys, such as [Lev04] and [Hel98], in the area, and literally thousands of articles from the second half of the 20th century.

As such, we are introducing two new methods, in Sections IV and V, respectively, which can be formulated in a relatively small space, but which fit in the broader context reflected by the diverse literature mentioned in the previous paragraph. Hopefully, these methods will serve as a catalyst for developing new waveform design methods to address the requirement of spectral efficiency imposed by a rapidly dwindling EM spectrum. The method of Section IV deals with CAZAC sequences. There have been quadratic phase CAZACs going back to Norbert Wiener [Wie30], and some say to Gauss. We construct new quadratic sequences as well as non-chirp-like sequences, and provide a discrete periodic ambiguity function analysis of them. Section V develops the analogue of Section IV, but for the aperiodic case. Section VI is the Epilogue. In Section II and the Appendix, we provide some motivation for waveform design and an elementary background on radar, respectively. Section III records the definition and basic properties of the ambiguity function.

II. MOTIVATION

The area of waveform design enjoys continued attention due to advances in radar hardware, computational algorithms, and coding schemes. These advances have had a creative, synergistic impact on the design of radar waveforms, providing improved ambiguity function and target detection properties.

Two basic desiderata that must be satisfied in the design of radar waveforms are the following [Woo53b], [Woo53a], [Coo67], [Lev04]:

- Short duration (in the time domain perforce large extent in the frequency domain) pulses, which are required for good range resolution;
- On the other hand target detection calls for sufficient energy on target.

These two guiding principles impose conflicting requirements on the radar waveform design problem. The idea, and associated methods, of pulse compression are employed to satisfy these conflicting requirements. In turn, this calls for waveforms with large compression ratios (time-bandwidth product) [Lev04]. Extension of this approach to multi–static radars is considered in [Blu06].

Early work on the problem of radar waveform design was devoted to the use of a fixed transmit signal. This was largely due to a hardware limitation, which precluded waveform agile operation. Consequently, radar resolution in delay and Doppler was inhibited by the Heisenberg uncertainty principle. Thus, increased resolution in range comes about at the expense of resolution in Doppler and vice–versa [Bel02], [Bel88], [Bel93]. Information theoretic criteria for radar waveform design are outlined in [Bel02], [Bel88], [Bel93], [Bel98]. The work of [Bel02] sheds light on ameliorating the intrinsic limitations dictated by the Heisenberg uncertainty principle. Specifically, it draws an analogy of the problem of delay – Doppler imaging to an equivalent problem in high resolution optical images are formed by coherently combining several low resolution images each having a specified point spread function. In this process, it is important to minimize the cross point spread functions between the combined images. In the radar context, the ambiguity function plays the role of

the point spread function. The work of [Bel02] exploits this concept for designing radar waveforms to produce high resolution delay – Doppler images. In that respect, it highlights the importance of designing libraries of waveforms with diverse characteristics in terms of their ambiguity functions. We address this issue in Section V.

The work of [VT68] shows that the ambiguity function results from both a detection and an estimation problem for mono–static radars. Extension of this approach to bi-static radars is not straightforward due to the large number of free parameters arising from the geometry of the bi-static radar set up. The work of [Tsa97] formulates the ambiguity function for bi–static radars taking into account the geometry of a given setting. Furthermore, this work makes significant strides in terms of the discrete time ambiguity function with key considerations of sampling, reconstruction, and aliasing. The corresponding exercise for multi–static radar ambiguity function analysis is very much an open problem. Recent results point to the advantages of studying this problem in the context of frames and filter banks, see Sections IV and VI.

Another important issue in this context is the design of discrete time radar waveforms with a given ambiguity function design specification. For a given waveform, the ambiguity function can be calculated. However, several waveforms can give rise to the same ambiguity function. Consequently, the problem of radar waveform design for a given ambiguity function design specification becomes an ill posed problem calling for suitable regularization techniques involving constraints on the time-bandwidth product. The design of constant modulus waveforms can shed valuable insight in tackling this important problem, see Sections III and IV.

III. AMBIGUITY FUNCTIONS

A. Narrow band radar ambiguity function

Let \mathbb{R} , resp., \mathbb{C} , be the set of real, resp., complex, numbers. A function $u : \mathbb{R} \to \mathbb{C}$ is a *finite energy* signal if

$$|u||_2 = \left(\int_{\mathbb{R}} |u(s)|^2 ds\right)^{\frac{1}{2}} < \infty$$

In this case, we write $u \in L^2(\mathbb{R})$. (For this article it is not necessary to be concerned with the definition of the Lebesgue integral.) The *Fourier transform*, $\hat{u} : \mathbb{R} \to \mathbb{C}$, of u can be well-defined by the formal expression,

$$\widehat{u}(\gamma) = \int_{\mathbb{R}} u(t) e^{-2\pi i t \gamma} dt, \ \gamma \in \mathbb{R},$$

where *i* denotes the imaginary unit in \mathbb{C} . For an explanation of this definition of the Fourier transform and the subtleties which can surround it, see, e.g., [Ben97].

Let \mathbb{R}^2 be the direct product $\mathbb{R} \times \mathbb{R}$. The narrow band radar ambiguity function A(u) of $u \in L^2(\mathbb{R})$ is defined by

$$A(u)(t,\gamma) = \int_{\mathbb{R}} u(s+t)\overline{u(s)}e^{-2\pi i s\gamma} ds$$

$$= e^{\pi i t\gamma} \int_{\mathbb{R}} u(s+\frac{t}{2})\overline{u(s-\frac{t}{2})}e^{-2\pi i s\gamma} ds,$$
(1)

for $(t, \gamma) \in \mathbb{R}^2$. For simplicity, we refer to A(u) as the *ambiguity function* of the signal u.

An elementary form of the uncertainty principle mentioned in the Introduction and Section II, apropos the ambiguity function, is the formula,

$$\iint_{\mathbb{R}^2} |A(u)(t,\gamma)|^2 dt d\gamma = ||u||_2^4,$$
(2)

where $u \in L^2(\mathbb{R})$. Equation 2 asserts that A(u) can not be concentrated arbitrarily closely to the origin $(0,0) \in \mathbb{R}^2$. A more refined form of Equation 2, which is called the *radar uncertainty principle*, is the following assertion. If $||u||_2 = 1$, and if $X \subseteq \mathbb{R}^2$ and $\epsilon > 0$ have the property that

$$\iint_X |A(u)(t,\gamma)|^2 dt d\gamma \ge 1-\epsilon,$$

then $|X| \ge 1 - \epsilon$, where |X| is the area (Lebesgue measure) of X.

It is not difficult to prove that A(u) is uniformly continuous on \mathbb{R}^2 if $u \in L^2(\mathbb{R})$.

Typically, in radar, the modulus $|A(u)(t,\gamma)|$ is the only quantity that is, or can be, measured. In 1968, Vakman [Vak68] posed the *narrow band radar ambiguity problem*: For a given $u \in L^2(\mathbb{R})$, find all signals $v \in L^2(\mathbb{R})$ with the property that

$$|A(v)(t,\gamma)| = |A(u)(t,\gamma)|$$
(3)

for all $(t, \gamma) \in \mathbb{R}^2$. The signal $v(s) = ce^{i\omega s}u(s+x)$, for fixed $(x, \omega) \in \mathbb{R}^2$ and constant $c \in \mathbb{C}$ for which |c| = 1, is a solution of Equation 3. However, the problem is not completely resolved, see [Jam99] for recent results.

Remark 1: There are applications in seismology and sonar, as well as other disciplines, where narrow band approximations, which give rise to Equation 1, are not valid. This leads to the *wide band ambiguity* function WA(u) of $u \in L^2(\mathbb{R})$, which is defined by

$$WA(u)(a,t) = \sqrt{a} \int_{\mathbb{R}} u\left(a(s-t)\right) \overline{u(s)} ds,\tag{4}$$

for a > 0 and $t \in \mathbb{R}$, see [Aus90] for its formulation. WA(u) is a *continuous wavelet transform* of $u \in L^2(\mathbb{R})$. In particular, in the wide band case, WA(u) is a time–scale operator, whereas the narrow band ambiguity function, A(u), is a time–frequency operator. There is a corresponding *wide band radar ambiguity problem* which is at least as intractable as the narrow band case.

Remark 2: The Wigner distribution W(u) of $u \in L^2(\mathbb{R})$ was introduced by E. Wigner in 1932 in the context of quantum mechanics. It is defined by

$$W(u)(t,\gamma) = \int_{\mathbb{R}} u(t+\frac{s}{2})\overline{u(t-\frac{s}{2})}e^{-2\pi i s \gamma} ds,$$

for $(t, \gamma) \in \mathbb{R}^2$. It is a remarkable fact that, up to a rotation, W(u) is the two dimensional Fourier transform of A(u), e.g., see [Gro01].

Remark 3: If $u, v \in L^2(\mathbb{R})$, the narrow band cross-ambiguity function A(u, v) of u and v is defined by

$$\begin{aligned} A(u,v)(t,\gamma) &= \int_{\mathbb{R}} u(s+t)\overline{v(s)}e^{-2\pi i s \gamma} ds \\ &= e^{2\pi i t \gamma} \int_{\mathbb{R}} u(s)\overline{v(s-t)}e^{-2\pi i s \gamma} ds \end{aligned}$$

Thus, A(u, v) is the *short-time Fourier transform* (STFT) of $u \in L^2(\mathbb{R})$ with *window v*. STFTs are a staple in spectral analysis where one analyzes *spectrograms* |A(u, v)| recorded from various experiments, e.g., in speech analysis. They are also the basis for time-frequency or Gabor or Weyl-Heisenberg analysis.

It is not difficult to verify the time-frequency analysis equation,

$$A(u,v)(t,\gamma) = e^{2\pi i t \gamma} A(\hat{u},\hat{v})(\gamma,-t),$$

for $u, v \in L^2(\mathbb{R})$ and $(t, \gamma) \in \mathbb{R}^2$.

B. Discrete ambiguity functions

Let \mathbb{Z} be the set of integers, let $N \ge 1$ be an integer, and denote the additive group of integers modulo N by \mathbb{Z}_N . For example, if N = 6, then $2 + 3 \equiv 5 \pmod{6}$ and $4 + 5 \equiv 3 \pmod{6}$.

Let $u = \{u[m] : m = 0, 1, ..., N - 1\}$ be a sequence of complex numbers of length N. We shall denote by u_p the periodic extension of u to a bi–infinite sequence on all of \mathbb{Z} , i.e., for each $m \in \mathbb{Z}$, $u_p[m] = u[k]$, where $0 \le k \le N - 1$ and $k \equiv m \pmod{N}$. We shall denote by u_a the following aperiodic extension of u to \mathbb{Z} :

$$u_a[m] = \begin{cases} u[m], & m = 0, 1, \dots, N-1, \\ 0, & \text{otherwise.} \end{cases}$$

• The discrete periodic ambiguity function $A_p(u) : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{C}$ of u is defined by

$$A_p(u)(m,n) = \frac{1}{N} \sum_{k=0}^{N-1} u_p[m+k] \overline{u_p[k]} e^{-2\pi i k n/N}$$

• The discrete aperiodic ambiguity function $A_a(u) : \mathbb{Z} \times \mathbb{Z} \to \mathbb{C}$ of u is defined by

$$A_{a}(u)(m,n) = \frac{1}{N} \sum_{k=0}^{N-1} u_{a}[m+k]\overline{u_{a}[k]}e^{-2\pi i kn/N}.$$

Note that if $0 \le m \le N-1$ and $n \in \mathbb{Z}$, then

$$A_a(u)(m,n) = \frac{1}{N} \sum_{k=0}^{N-1-m} u[m+k]\overline{u[k]}e^{-2\pi i kn/N}$$

Example 1 (Shapiro – Rudin polynomials and Golay pairs): The Shapiro–Rudin polynomials, P_n , Q_n , $n = 0, 1, \ldots$, are defined recursively as follows for $t \in \mathbb{R}/\mathbb{Z}$:

-

$$P_0(t) = Q_0(t) = 1$$
$$P_{n+1}(t) = P_n(t) + e^{2\pi i 2^n t} Q_n(t),$$
$$Q_{n+1}(t) = P_n(t) - e^{2\pi i 2^n t} Q_n(t).$$

Two finite sequences, p and q, of length N, are a Golay complementary pair if

$$A_a(p)(0,0) + A_a(q)(0,0) \neq 0, \text{ and}$$

$$A_a(p)(m,0) + A_a(q)(m,0) = 0$$

for $1 \le m \le N-1$. It is interesting and not difficult to prove that, for each $n \ge 1$, the $N = 2^n$ coefficients for each of P_n and Q_n combine to form a Golay complementary pair, see [Ben] for a survey of this subject as well as [Cla] in this issue for radar applications.

QMF (CMF)

$$|P_n(t)|^2 + |Q_n(t)|^2 = 2^{n+1}$$

IV. CAZAC SEQUENCES

A. Historical background from engineering

A function $u : \mathbb{Z}_N \to \mathbb{C}$ is a Constant Amplitude Zero Autocorrelation (CAZAC) sequence if

(CA)
$$|u[m]| = 1, \quad 0 \le m \le N - 1,$$

and

(ZAC)
$$A_p(u)(m,0) = 0, \quad 1 \le m \le N-1.$$

There is an extensive literature on CAZACs because of the importance of such sequences in communications, coding theory, cryptology, and radar, e.g., [Kla60a], [Kla60b], [Hei61], [Fra62], [Tur68], [Sch70], [Chu72], [Fra73], [Mil83], [Roh92], [Lee98], [Hel98], [Lev04], [Pro04], [Gol05]

CAZAC waveforms (and some of their close relatives) are also called by the following names among others: polyphase sequences with good periodic or optimum correlation properties, e.g., [Hei61], [Fra62], [Chu72], [Sch78], [She79], [Kum85]; constant amplitude optimal sequences, e.g. [Ng98]; perfect auto-correlation or root-of-unity sequences, e.g., [Mow96], [Gab91], [Gol92]; generalized chirp-like polyphase sequences, e.g., [Pop92]; bi-unimodular sequences, e.g., [Bjo90], [Bjo95], [Haa96]; bent functions, e.g., [Dil74], [Chu89]; constant amplitude all pass sequences. As mentioned in the Introduction, the literature in this area is extensive, one might say overwhelming, see [Hel98].

Example 2 (Quadratic phase CAZAC sequences): A *quadratic phase* CAZAC sequence $u : \mathbb{Z}_N \to \mathbb{C}$ is defined by

$$u[k] = e^{\pi i P(k)/N}, \quad 0 \le k \le N - 1,$$

where P(k) is a quadratic polynomial in k. The following are specific examples from the aforementioned literature.

- Chu sequences: P(k) = k(k-1), N odd,
- P4 sequences: P(k) = k(k N),

The set of quadratic phase sequences is actually much richer than the classical nickname, chirps, implies. We shall quantify this assertion in Section IV-C, but set the stage with the following definition.

Definition 1: Given N > 1, and let M = N if N is odd, M = 2N if N is even. Assume that ω is a primitive M-th root of unity, i.e., $\omega = e^{2\pi i k/M}$, where k and M are relatively prime, denoted by (k, M) = 1. The function $u : \mathbb{Z}_N \to \mathbb{C}$ defined by

$$u[m] = \omega^{m^2}, \quad 0 \le m \le N - 1,$$

is a Wiener sequence, see [Ben07].

It is not difficult to prove that Wiener sequences are CAZAC sequences.

The discrete Fourier transform (DFT) of a function $u: \mathbb{Z}_N \to \mathbb{C}$ is defined by

$$\hat{u}[n] = \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} u[m] e^{-2\pi i m n/N}$$

The following facts are elementary to verify:

- $u \text{ CA} \iff \text{DFT of } u \text{ is ZAC.}$
- $u \text{ CAZAC} \iff \text{DFT of } u \text{ is CAZAC}.$

• If u is CA, then \hat{u} can have zeros.

B. Mathematical problems

We have defined CAZAC sequences in terms of functions $u : \mathbb{Z}_N \to \mathbb{C}$. Of course, such a function can be identified with a point $(u[0], \ldots, u[N-1]) \in \mathbb{C}^N$. Thus, the set of all CAZAC sequences defines a subset of \mathbb{C}^N . The periodicity inherent in \mathbb{Z}^N and the fact that \mathbb{C}^N consists of N-tuples leads us to consider *circulant matrices*, i.e., $N \times N$ matrices A_u whose first row is $u[0], \ldots, u[N-1]$, whose second row is $u[N-1], u[0], \ldots, u[N-2]$, etc., where each $u[m] \in \mathbb{C}$. A circulant matrix H_u is called a *Hadamard matrix* if $H_u H_u^* = N Id$, where H_u^* is the Hermitian conjugate of H_u and Id is the $N \times N$ identity matrix.

We begin this section with the following well known fact.

Proposition 1: A function $u : \mathbb{Z}_N \to \mathbb{C}$ is a CAZAC sequence if and only if A_u is a Hadamard matrix. We shall say that two CAZAC sequences u and $v : \mathbb{Z}_N \to \mathbb{C}$ are *equivalent* if v = cu for some $c \in \mathbb{C}$ for which |c| = 1. There are other equivalence relations one can impose on the category of CAZAC sequences from which one can pose problems related to natural non-abelian groups which arise, see [Ben07];

• Shifts: $\forall n = 0, \dots, N-1$ and $m \in \mathbb{Z}$,

$$u[n] = (\tau_m v)[n] = v[m+n].$$

• Cyclic permutations: for k with gcd(k, N) = 1,

$$u[n] = (\sigma_k v)[n] = v[kn].$$

• Multiplication by powers of N-th roots of unity: for ζ with $\zeta^N = 1$,

$$u[n] = v[n]\zeta^n.$$

In all these cases, u is a CAZAC sequence if v is also CAZAC.

There is the following compelling problem. For a given N, compute or estimate the number of non-equivalent CAZAC sequences. The problem has been investigated by Gabidulin [Gab91], [Gab94]. Björck and Saffari [Bjo95] proved that if $N = MK^2$, then there are infinitely many non-equivalent CAZAC sequences, e.g., N = 4, 8, 9, or 12. On the other hand, Haagerup [Haa96] has given a complete mathematical proof that if N is prime, then there are only finitely many non-equivalent CAZAC sequences.

Remark 4: Haagerup's theorem, as well as Gabidulin's work, uses a refinement of Chebotorev's theorem (1924) that if p is prime, then all square submatrices of the $p \times p$ DFT matrix are non-singular.

Such refinements, with intermediate contributions by Dieudonné, as well as Donoho and Stark, and a recent formulation by Tao, are critical in compressive sampling and especially the theory of Candès, Romberg, and Tao, see [SPM08].

Example 3: a. Let N be odd. Binary CAZAC waveforms $u : \mathbb{Z}_N \to \{\pm 1\}$ can not exist.

b. Let N be arbitrary. It is well known that if $u : \mathbb{Z}_N \to \{\pm 1\}$, then $A(u)(m, 0) \equiv N \pmod{4}$. Thus, if A(u)(m, 0) has zeros, and, in particular, if u is a CAZAC sequence, then 4 divides N.

c. Let N be arbitrary. The only known binary CAZAC sequence $u : \mathbb{Z}_N \to \{\pm 1\}$, up to any translation and multiplication by -1, is $\{1, 1, 1, -1\}$. However, there do exist periodic complex binary sequences, not ± 1 , which are CAZAC sequences, e.g., Björck [Bjo90] and Golomb (1992) [Gol92], cf., [Haa96] and see Section IV-D. In fact, Saffari [Saf01] was able to determine all such complex binary sequences.

C. The discrete periodic ambiguity function of Wiener CAZAC sequences

We begin this section with the following computation.

Theorem 1: Let $j \in \mathbb{Z}$. Define $u_j : \mathbb{Z}_N \to \mathbb{C}$ by $u_j(k) = e^{2\pi i j k^2/M}$, where M = 2N if N is even and M = N if N is odd. If N is even, then

$$A(u_j)(m,n) = \begin{cases} e^{2\pi i j m^2/(2N)}, & jm+n \equiv 0 \pmod{N}, \\ 0, & \text{otherwise.} \end{cases}$$

If N is odd, then

$$A(u_j)(m,n) = \begin{cases} e^{2\pi i j m^2/N}, & 2jm+n \equiv 0 \pmod{N}, \\ 0, & \text{otherwise.} \end{cases}$$

The discrete periodic ambiguity function, A(u), of a Wiener CAZAC sequence $u : \mathbb{Z}_N \to \mathbb{C}$ has a simple behavior since, for any fixed value of n, A(u)(m, n) is zero for all except one value of m. That is, for each fixed n, the graph of $A(u)(\cdot, n)$ as a function of m consists of a single peak. In fact, we have the following consequence of Theorem 1.

Corollary 1: Let u be a Wiener CAZAC sequence. (In particular, ω is a primitive M-th root of unity.) If N is even, then

$$A(u)(m,n) = \begin{cases} \omega^{m^2}, & m \equiv -n \pmod{N}, \\ 0, & \text{otherwise.} \end{cases}$$

If N is odd, then

$$A(u)(m,n) = \begin{cases} \omega^{m^2}, & m \equiv -n(N+1)/2 \pmod{N}, \\ 0, & \text{otherwise.} \end{cases}$$



Figure 1. Discrete periodic ambiguity plot for Wiener sequences of length N = 101 and j = 49, 4, resp.

Example 4: a. Let N be odd and let $\omega = e^{2\pi i/N}$. Then, $u(k) = \omega^{k^2}$, $0 \le k \le N - 1$, is a CAZAC sequence. By Corollary 1, $|A(u)(m,n)| = |\omega^{m^2}| = 1$ if $2m + n = \ell_{m,n}N$ for some $\ell_{m,n} \in \mathbb{Z}$ and |A(u)(m,n)| = 0 otherwise, i.e., A(u)(m,n) = 0 on $\mathbb{Z}_N \times \mathbb{Z}_N$ unless $2m + n \equiv 0 \pmod{N}$. In the case $2m + n = \ell_{m,n}N$ for some $\ell_{m,n} \in \mathbb{Z}$, we have the following phenomenon. If $0 \le m \le \frac{N-1}{2}$ and $2m + n = \ell_{m,n}N$ for some $\ell_{m,n} \in \mathbb{Z}$, then n is odd; and if $\frac{N+1}{2} \le m \le N-1$ and $2m + n = \ell_{m,n}N$ for some $\ell_{m,n} \in \mathbb{Z}$, then n is even. Thus, the values (m, n) in the domain of the discrete periodic ambiguity function A(u), for which A(u)(m, n) = 0, appear as two parallel discrete lines. The line whose domain is $0 \le m \le \frac{N-1}{2}$ has odd function values n; and the line whose domain is $\frac{N+1}{2} \le m \le N-1$ has even function values n.

b. The behavior observed in part a has extensions for primitive and nonprimitive roots of unity.

Let $u : \mathbb{Z}_N \to \mathbb{C}$ be a Wiener sequence. Thus, $u[k] = \omega^{k^2}$, $0 \le k \le N - 1$, and $\omega = e^{2\pi i j/M}$, (j, M) = 1, where M is defined in terms of N in Definition 1. By Corollary 1, for each fixed $n \in \mathbb{Z}_N$, the function $A(u)(\cdot, n)$ of m vanishes everywhere except for a *unique* value $m_n \in \mathbb{Z}_N$ for which $|A(u)(m_n, n)| = 1$. See Figure 1, where N = 101 and j = 49, 4, resp.

c. The hypotheses of Theorem 1 do not assume that $e^{2\pi i j/M}$ is a primitive M-th root of unity. In fact, in the case that $e^{2\pi i j/M}$ is *not* primitive, then, for certain values of n, $A(u)(\cdot, n)$ will be identically 0 and, for certain values of n, $|A(u)(\cdot, n)| = 1$ will have several solutions. For example, if N = 100 and j = 2, then, for each odd n, $A(u)(\cdot, n) = 0$ as a function of m. If N = 100 and j = 3, then (100, 3) = 1so that $e^{2\pi i 3/100}$ is a primitive 100th root of unity; and, in this case, for each $n \in \mathbb{Z}_N$ there is a *unique* $m_n \in \mathbb{Z}_N$ such that $|A(u)(m_n, n)| = 1$ and A(u)(m, n) = 0 for each $m \neq m_n$.

D. Björck sequences

We shall now define a class of CAZAC sequences which are not equivalent to Wiener CAZAC sequences, where equivalence was defined in Section 1. This result came as a surprise in several fields, and proves false the conjectures of Popa and Enflo, see [Haa96]. This subsection presents a breif summary of Bjorck's results.

Let N = p be prime. The Legendre symbol $\left(\frac{k}{p}\right)$ is defined by

$$\begin{pmatrix} \frac{k}{p} \end{pmatrix} = \begin{cases} 0, & \text{if } k \equiv 0 \pmod{p}, \\ 1, & \text{if } k \equiv n^2 \pmod{p} & \text{for some } n \in \mathbb{Z}, n \neq 0 \pmod{p} \\ -1, & \text{if } k \neq n^2 \pmod{p} & \text{for all } n \in \mathbb{Z}, \end{cases}$$

Example 5: Let p = 7, noting that $7 \equiv -1 \pmod{4}$. Then $\binom{k}{7} = -1$ for k = 3, 5, 6. Björck made the remarkable discovery that $u : \mathbb{Z}_7 \to \mathbb{C}$, defined by

$$u[0] = u[1] = u[2] = u[4] = 1,$$

 $u[3] = u[5] = u[6] = e^{i\theta},$

where $\theta = \arccos(-3/4)$, is a CAZAC sequence!

Definition 2: Given N = p, a prime. The function $u : \mathbb{Z}_p \to \mathbb{C}$ defined by

$$u[m] = e^{i\theta_p[m]}, \quad 0 \le m \le p - 1,$$

is a Björck sequence if,

• for $p \equiv 1 \pmod{4}$, we have

$$\theta_p[m] = \left(\frac{m}{p}\right) \arccos\left(\frac{1}{1+\sqrt{p}}\right)$$

• for $p \equiv -1 \pmod{4}$, we have

$$\theta_p[m] = \begin{cases} \arccos\left(\frac{1-p}{1+p}\right), & \text{if } \left(\frac{m}{p}\right) = -1\\ 0, & \text{else,} \end{cases}$$

Björck (1985) went on to prove the following theorem, see [Bjo90], [Bjo95], [Saf01].

Theorem 2: Björck sequences are CAZAC sequences.

Two-valued CAZACs have been classified by Saffari [Saf01] in terms of Hadamard–Paley and Hadamard– Menon difference sets. The result of Saffari states that two-valued CAZACs exist for lengths $N \ge 3$ if and only if $N \equiv 3 \pmod{4}$ and there exists a Hadamard–Paley difference set of length N or $N \equiv 0 \pmod{4}$ and there exists a Hadamard–Menon difference set of length N. In either case, explicit formulas are provided



Figure 2. Discrete periodic ambiguity plot (in dB) for a Björck sequence of length N = 101.

for the construction of the CAZAC sequence. A similar classification exists for two-level autocorrelation Legendre sequences [Gol05], with several results relating to the existence of Hadamard–Paley difference sets. Existence of Hadamard–Menon sets is rather more difficult to prove, as it relates to the Hadamard circulant conjecture. It follows that two-valued CAZACs cannot exist for lengths $K \equiv 1 \pmod{4}$. However, note that in this case Björck CAZAC sequences are *almost* two-valued.

V. PHASE CODED WAVEFORMS

CAZAC sequences are important in waveform design because of their defining properties: CA ensures optimal transmission efficiency while ZAC provides tight time localization at zero Doppler. In Section IV we focused on their characterization in terms of the discrete *periodic* ambiguity function A_p . By definition, all CAZAC sequences have the same *periodic autocorrelation* $A_p(u)(\cdot, 0)$, but we have shown that they exhibit significant diversity of behavior once the full time–frequency landscape is considered, see Figure 2. Periodic autocorrelation is also referred to as cyclic autocorrelation, which permits computation by loading finite sequences into a circular register and rotating the register.

In the aperiodic case, of course, ZAC is unattainable, and sidelobes appear. In order to quantify this behavior, we utilize two measures of sidelobe magnitude, that capture various aspects of the *aperiodic autocorrelation* $A_a(u)(\cdot, 0)$

Definition 3: The Peak Sidelobe Level (PSL) of a sequence u is defined by

$$PSL(u) = \frac{1}{|A_a(u)(0,0)|} \sup_{1 \le m \le N-1} |A_a(u)(m,0)|$$



Figure 3. Effect of cyclic shifts τ_m on the discrete aperiodic autocorrelation $A_a(u)(\cdot, 0)$ of different equivalence classes of CAZAC sequences; PSL(u) (in dB) vs. shift length m. Red x: Björck (N=101), Blue triangles: Milewski (N = 100), Green squares: Wiener (N=101).

The Integrated Sidelobe Level (ISL) of a sequence u is defined by

$$ISL(u) = \frac{1}{|A_a(u)(0,0)|^2} \sum_{m=1}^{N-1} |A_a(u)(m,0)|^2$$

Both the PSL and the ISL differ within the equivalence classes of CAZAC sequences, and across classes. This is analogous to results obtained for Legendre sequences [B93], [Bor01]. Figure 3 illustrates this effect on PSL with respect to shifts τ_m . Note that Wiener CAZACs are not affected at all, whereas Björck sequences exhibit the most variability. Similar results arise when one considers other measures, such as ISL.

The variability in sidelobe behavior for Björck CAZACs is not limited to their energy levels. As Figure 4 shows, shifting also affects sidelobe location.

Example 6: By averaging the autocorrelation $A_a(\tau_k u)(\cdot, 0)$ of several different shifts m of the same basis sequence u, we can obtain an overall lowering of the energy levels off of the main lobe. In this example, we present the noncoherent average over two selected shifts, i.e.

$$|A_a(\tau_{40}u)(\cdot,0)| + |A_a(\tau_{41}u)(\cdot,0)|,$$

which have complementary sidelobes near the origin. Note that we can improve over the shift that achieves the lowest PSL globally (shift by 28).

Example 7: The same averaging technique can be used with the discrete aperiodic ambiguity functions of shifted sequences $A_a(\tau_k u)$. Figures 6(a–c) plot the discrete aperiodic ambiguity functions of shifts of the Björck CAZAC of length 29 (by zero, 7, and 12, respectively), with a threshold of -10dB. The area



Figure 4. Discrete aperiodic autocorrelation for Björck sequences of length N = 19. Three shifts τ_m , with m = 0, 4, and 9, respectively.



Figure 5. Effect of cyclic shifts on the aperiodic autocorrelation function of Björck CAZAC sequences; Plot of absolute value (dB) in the area of the main lobe for two different shifts (by 40 and 41), and their average. Also plotted for reference is the shift that achieves the lowest PSL globally.

plotted is centered at the origin. We observe that the peak locations vary, and by averaging all three we obtain Figure 6(d).

- Waveforms associated to Chu-Zadoff and P4 CAZACs are known for their low sidelobes at zero Doppler shift, but their ambiguity functions exhibit strong coupling in the time-frequency plane.
- Waveforms associated to Björck CAZACs can more effectively decouple the effect of time and frequency shifts. However, at zero Doppler shift, their sidelobe behavior is less desirable than quadratic phase CAZACs.
- These differences led to our concatenation idea.



Figure 6. Plot of the discrete aperiodic ambiguity function of shifts of the Björck CAZAC of length 29, thresholded at -10dB; darker color denotes higher value. a) zero shift, b) shift by 7, c) shift by 12, and d) their average.



• A concatenation of partial CAZACs u and v is w = Mix(r%, u, v) defined as

$$w[m] = u[m], \text{ if } m = 0, \dots, M$$

and

$$w[m] = v[m], \text{ if } m = M + 1, \dots, N - 1,$$

where M is the nearest integer to $r \times N/100$.

• We show how the ambiguity function can be improved by concatenation of partial CAZACs belonging to two different families. The best choice is obtained with r = 50.

VI. Epilogue

The purpose of this paper was to observe the complexity of CAZAC sequences, resulting in diverse periodic and aperiodic ambiguity behavior. Although we restricted ourselves to two special cases, viz., Wiener and Björck sequences, we ultimately want to fathom the depth of all non–equivalent CAZAC sequences. The supporting mathematical theory must be developed significantly to achieve this goal, and the engineering criteria, particularly in communications, coding, and radar, must interleave with the mathematics to ensure relevance and focus.

Even with these mathematical and engineering challenges to understanding and quantifying the ambiguity function diversity rooted in the mysteries surrounding non–equivalent CAZAC sequences $u : \mathbb{Z}_N \to \mathbb{C}$, there is also the next level of generalization which must be addressed. In fact, one can envision a theory of *ambiguity vector fields* to deal with multidimensional and vector–valued problems, e.g., in light of vector sensor and MIMO settings and capabilities. Some contemporary work [Ben07], [Ben08], [Mat03] illustrate the role of the theory of frames for ambiguity or Wigner ditribution analysis, fitting in with its use in a host of recent applications, e.g., [Kov07], [Ben03]

FUN-TFs are surprisingly applicable. They have arisen in dealing with the robust transmission of data over erasure channels such as the internet [Cas03], [Goy01], [Hol04], and in both multiple antenna code design for wireless communications [Hoc00] as well as multiple description coding [Str03], [Goy98], [Goy99]. There are also recent applications of FUN-TFs in quantum detection, $\Sigma - \Delta$ quantization, and Grassmanian "min-max" waveforms, e.g., [Ben04]. Frames give redundant signal representation to compensate for machine imperfections, to ensure numerical stability, and to minimize the effects of noise.

REFERENCES

[Aus90] L. Auslander and I. Gertner, *Wide–band ambiguity functions and the ax+b group*, volume 22, pp. 1–12, IMA Volumes in Math. and Appl., 1990.

- [B93] L. Bömer and M. Antweiler, "Optimizing the aperiodic merit factor of binary arrays," in *Signal Processing*, volume 30, no. 1, pp. 1–13, 1993.
- [Bel88] M. R. Bell, Information theory and radar : mutual information and the design and analysis of radar waveforms and systems, Ph.D. thesis, California Institute of Technology, 1988.
- [Bel93] M. R. Bell, "Information theory and radar waveform design," in *IEEE Transactions on Information Theory*, volume 39, no. 5, pp. 1578–1597, 1993.
- [Bel98] M. R. Bell, "Diversity waveform sets for delay-doppler imaging," in *IEEE Transactions on Information Theory*, volume 44, no. 4, 1998.
- [Bel02] M. R. Bell and S. Monrocq, "Diversity waveform signal processing for delay-doppler measurement and imaging," in *Digital Signal Processing*, volume 12, no. 2/3, 2002.
- [Ben] J. Benedetto and J. Sugar-Moore, "Geometric properties of shapiro-rudin polynomials," .
- [Ben97] J. Benedetto, Harmonic Analysis and Applications, CRC Press Inc., Boca Raton, FL, 1997.
- [Ben03] J. J. Benedetto and M. Fickus, "Finite normalized tight frames," in Adv. Comp. Math., volume 18, no. 2-4, pp. 357–385, 2003.
- [Ben04] J. J. Benedetto, A. Powell, and O. Yilmaz, " $\Sigma \Delta$ quantization and finite frames," in *IEEE Trans. Inform. Theory*, 2004, submitted.
- [Ben07] J. Benedetto and J. Donatelli, "Ambiguity function and frame-theoretic properties of periodic zero-autocorrelation waveforms," in *Selected Topics in Signal Processing, IEEE Journal of*, volume 1, no. 1, pp. 6–20, June 2007.
- [Ben08] J. Benedetto and J. Donatelli, "Frames and a vector-valued ambiguity function," 2008.
- [Bjo90] G. Bjorck, Functions of modulus 1 on \mathbb{Z}_N whose Fourier transforms have constant modulus, and "cyclic n-roots", volume 315, pp. 131–140, Kluwer Academic Publishers, NATO-ASI, 1990.
- [Bj095] G. Bjorck and B. Saffari, "New classes of finite unimodular sequences with unimodular transforms. Circular Hadamard matrices with complex entries," in C.R. Acad. Sci., Paris, volume 320, pp. 319–324, 1995.
- [Blu06] S. D. Blunt and K. R. Gerlach, "Multistatic adaptive pulse compression," in *IEEE Transactions on Aerospace and Electronic Systems*, volume 42, no. 3, pp. 891–903, 2006.
- [Bor01] P. Borwein, S. Choi, and S. Yazdani, "Extremal property of fekete polynomials," in *Proceedings of the American Mathematical Society*, volume 129, pp. 19–27, 2001.
- [Cas03] P. Casazza and J. Kovačević, "Equal-norm tight frames with erasures," in Adv. Comput. Math., volume 18, no. 2–4, pp. 387–430, 2003.
- [Chu72] D. C. Chu, "Polyphase codes with good periodic correlation properties," in *IEEE Trans. Inform. Theory*, volume IT-18, pp. 531–532, July 1972.
- [Chu89] H. Chung and P. V. Kumar, "A new general construction for generalized bent functions," in *IEEE Transactions on Information Theory*, volume 35, no. 1, p. 206, 1989.
- [Cla] R. Claderbank, S. Howard, and W. Moran, in Signal Processing Magazine, IEEE.
- [Coo67] C. Cook and M. Bernfeld, *Radar Signals: An Introduction to Theory and Application*, Academic Press, New York, 1967.
- [Dil74] J. Dillon, Elementary Hadamard difference sets, Ph.D. Thesis, University of Maryland, College Park, 1974.
- [Fra62] R. L. Frank and S. A. Zadoff, "Phase shift codes with good periodic correlation properties," in *IRE Trans. Inform. Theory*, volume 8, pp. 381–382, 1962.

- [Fra73] R. L. Frank, "Comments on polyphase codes with good correlation properties," in *IEEE Trans. Inform. Theory*, volume 19, p. 244, March 1973.
- [Gab91] E. M. Gabidulin, "On classification of sequences with the perfect periodic autocorrelation functions," in *Proceedings* of the Third International Colloquium on Coding Theory, pp. 24–30, Yerevan, Sept 25 - Oct 2, 1990 1991.
- [Gab94] E. M. Gabidulin, "There are only finitely many perfect autocorrelation polyphase sequences of prime length," in *Proc. IEEE Int. Symp. Inform. Theory*, p. 282, Trondheim, Norway, 1994.
- [Gol92] S. W. Golomb, "Two-valued sequences with perfect periodic autocorrelation," in *IEEE Transactions on Aerospace and Electronic Systems*, volume 28, pp. 383–386, April 1992.
- [Gol05] S. Golomb and G. Gong, Signal Design for Good Correlation, Cambridge University Press, 2005.
- [Goy98] V. K. Goyal, J. Kovačević, and M. Vetterli, "Multiple description transform coding: Robustness to erasures using tight frame expansions," in *Proc. IEEE Int. Symp. on Inform. Theory*, p. 408, 1998.
- [Goy99] V. K. Goyal, J. Kovačević, and M. Vetterli, "Quantized frame expansions as source-channel codes for erasure channels," in *Proc. IEEE Data Compression Conf.*, pp. 326–335, 1999.
- [Goy01] V. K. Goyal, J. Kovačević, and J. A. Kelner, "Quantized frame expansions with erasures," in Appl. Comput. Harmon. Anal., volume 10, no. 3, pp. 203–233, 2001.
- [Gro01] K. Grochenig, Foundations of Time-Frequency Analysis, Birkhäuser, Boston, MA, 2001.
- [Haa96] U. Haagerup, "Orthogonal maximal abelian *-subalgebras of the n×n matrices and cyclic n-roots," Preprints No. 4, Institut for Matematik, U. of Southern Denmark, 1996.
- [Hei61] R. C. Heimiller, "Phase shift pulse codes with good periodic correlation properties," in *IRE Trans. Inform. Theory*, volume 7, pp. 254–257, October 1961.
- [Hel98] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in V. S. Pless and W. C. Huffman (editors), *Handbook of Coding Theory*, chapter 21, pp. 1765–1853, Elsevier, Amsterdam, 1998.
- [Hoc00] B. M. Hochwald, T. L. Marzetta, T. J. Richarson, W. Sweldens, and R. L. Urbanke, "Systematic design of unitary space-time constellations," in *IEEE Trans. Inform. Theory*, volume 46, no. 6, pp. 1962–1973, 2000.
- [Hol04] R. B. Holmes and V. I. Paulsen, "Optimal frames for erasures," in *Linear Algebra Appl.*, volume 377, pp. 31–51, 2004.
- [Jam99] P. Jaming, "Phase retrieval techniques for radar ambiguity problems," in J. of Fourier Analysis Appl., 1999.
- [Kla60a] J. R. Klauder, "The design of radar signals having both high range resolution and high velocity resolution," in *Bell System Technical Journal*, volume 39, pp. 809–820, 1960.
- [Kla60b] J. R. Klauder, A. C. Price, S. Darlington, and W. J. Albersheim, "The theory and design of chirp radars," in *Bell System Technical Journal*, volume 39, pp. 745–808, 1960.
- [Kov07] J. Kovačević and A. Chebira, "Life beyond bases: The advent of frames (Part I)," in Signal Processing Magazine, IEEE, volume 24, no. 4, pp. 86–104, July 2007.
- [Kum85] P. Kumar, R. Scholtz, and L. Welch, "Generalized bent functions and their properties," in J. Combin. Theory, volume A, no. 40, pp. 90–107, 1985.
- [Lee98] J. S. Lee and L. E. Miller, CDMA Systems Engineering Handbook, Artech House Publications, 1998.
- [Lev04] N. Levanon and E. Mozeson, Radar Signals, Wiley-Interscience, IEEE Press, New York, 2004.
- [Mat03] G. Matz and F. Hlawatsch, "Wigner distributions (nearly) everywhere: time-frequency analysis of signals, systems, random processes, signal spaces, and frames," in *Signal Processing*, pp. 1355–1378, 2003.
- [Mil83] A. Milewski, "Periodic sequences with optimal properties for channel estimation and fast start-up equalization," in *IBM J. Res. Develop.*, volume 27, no. 5, pp. 426–431, 1983.

- [Mow96] W. H. Mow, "A new unified construction of perfect root-of-unity sequences," in *Proc. IEEE 4th International Symposium on Spread Spectrum Techniques and Applications*, pp. 955–959, Germany, September 1996.
- [Ng98] J. C. Ng, K. B. Letaief, and R. D. Murch, "Complex optimal sequences with constant magnitude for fast channel estimation initialization," in *IEEE Transactions on Communications*, volume 46, no. 3, pp. 305–308, 1998.
- [Pop92] B. Popović, "Generalized chirp-like polyphase sequences with optimum correlation properties," in *IEEE Transactions on Information Theory*, volume 38, no. 4, pp. 1406–1409, 1992.
- [Pro04] J. G. Proakis, Digital Communications, McGraw-Hill Book Co., NY, 4th edition, 2004.
- [Roh92] U. H. Rohrs and L. P. Linde, "Some unique properties and applications of perfect squares minimum phase cazac sequences," in *Proc. South African Symp. on Communications and Signal Processing*, pp. 155–160, 1992.
- [Saf01] B. Saffari, "Some polynomial extremal problems which emerged in the twentieth century," in *in: Twentieth Century Harmonic Analysis*, volume 33, pp. 201–233, Kluwer Academic Publishers, NATO-ASI, 2001.
- [Sch70] M. R. Schroeder, "Synthesis of low-peak factor signals and binary sequences with low autocorrelation," in *IEEE Trans. Inform. Theory*, volume 16, pp. 85–89, January 1970.
- [Sch78] R. A. Scholtz and L. R. Welch, "Group characters: sequences with good correlation properties," in *IEEE Trans. Inform. Theory*, volume 24, pp. 537–545, September 1978.
- [She79] D. A. Shedd and D. V. Sarwate, "Construction of sequences with good correlation properties," in *IEEE Trans. Inform. Theory*, volume 25, pp. 94–97, January 1979.
- [SPM08] "Sensing, sampling, and compression," in Signal Processing Magazine, IEEE, volume 25, no. 2, March 2008.
- [Str03] T. Strohmer and R. W. J. Heath, "Grassmannian frames with applications to coding and communication," in *Appl. Comp. Harmon. Anal.*, volume 14, no. 3, pp. 257–275, 2003.
- [Tsa97] T. Tsao, M. Slamani, P. Varshney, D. Weiner, H. Schwarzlander, and S. Borek, "Ambiguity function for a bistatic radar," in *IEEE Transactions on Aerospace and Electronic Systems*, volume 33, no. 3, pp. 1041–1051, 1997.
- [Tur68] R. Turyn, Sequences with small correlations, pp. 195–228, John Wiley & Sons, Inc., New York, 1968.
- [Vak68] D. Vakman, Sophisticated Signals and the Uncertainty Principle in Radar, Springer Verlag, New York, 1st edition, 1968.
- [VT68] H. Van Trees, Detection, Estimation and Modulation Theory, volume 3, John Wiley and Sons, New York, 1968.
- [Wie30] N. Wiener, "Generalized harmonic analysis," in Acta Mathematica, volume 55, pp. 117-258, 1930.
- [Woo53a] P. Woodward, Probability and information theory, with applications to radar, Pergamon Press, London, UK, 1953.
- [Woo53b] P. Woodward, "Theory of radar information," in *IEEE Transactions on Information Theory*, volume 1, no. 1, pp. 108–113, 1953.