

Ambiguity Function and Frame-Theoretic Properties of Periodic Zero-Autocorrelation Waveforms

John J. Benedetto and Jeffrey J. Donatelli

Abstract—Periodic constant-amplitude zero-autocorrelation (CAZAC) waveforms u are analyzed in terms of the discrete periodic ambiguity function A_u . Elementary number-theoretic considerations illustrate that peaks in A_u are not stable under small perturbations in its domain. Further, it is proved that the analysis of vector-valued CAZAC waveforms depends on methods from the theory of frames. Finally, techniques are introduced to characterize the structure of A_u , to compute u in terms of A_u , and to evaluate MSE for CAZAC waveforms.

Index Terms—Constant-amplitude zero-autocorrelation (CAZAC) waveforms, discrete periodic ambiguity function, frames.

I. INTRODUCTION

A. Background

LET $N \geq 1$ be an integer, let \mathbb{Z}_N be the additive group \mathbb{Z} of integers modulo N , and let \mathbb{F} be the field \mathbb{R} of real numbers or the field \mathbb{C} of complex numbers. (\mathbb{Z}_N is also a commutative ring with unit; and it is a field if and only if N is prime.) Let $d \geq 1$ be an integer. We shall construct and analyze N -periodic functions $u : \mathbb{Z}_N \rightarrow \mathbb{F}^d$, which are unimodular and have zero-autocorrelation for each $m \in \mathbb{Z}_N \setminus \{0\}$. The autocorrelation A_u of u is defined by

$$\forall m \in \mathbb{Z}_N, \quad A_u(m) = \frac{1}{N} \sum_{k=0}^{N-1} \langle u(m+k), u(k) \rangle$$

where each $u(k) = (u_1(k), \dots, u_d(k))$, where $u_j(k) \in \mathbb{F}$, $k \in \mathbb{Z}_N$, and $j = 1, \dots, d$, and where the inner product is

$$\langle u(k), u(m) \rangle = \sum_{j=1}^d u_j(k) \overline{u_j(m)}.$$

Thus, the norm of each $u(k)$ is $\|u(k)\| = \langle u(k), u(k) \rangle^{1/2}$, and we say that u is *unimodular* when $\|u\| = 1$.

If $u : \mathbb{Z}_N \rightarrow \mathbb{F}^d$ is unimodular and has zero-autocorrelation for each $m \in \mathbb{Z}_N \setminus \{0\}$, then u is a *Constant-Amplitude Zero-Autocorrelation (CAZAC) waveform* in \mathbb{F}^d of length N . This is

Manuscript received August 24, 2006; revised December 26, 2006. The work of J. J. Donatelli was supported by the University of Maryland VIGRE Grant DMS0240049. This work was supported by ONR Grant N00014-06-1-0002, AFOSR(MURI) Grant FA9550-05-1-0443, and DARPA funding under NRL Grant N00173-06-1-G006. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Muralidhar Rangaswamy.

The authors are with the Norbert Wiener Center, Department of Mathematics, University of Maryland, College Park, MD 20742 USA (e-mail: jjb@math.umd.edu).

Digital Object Identifier 10.1109/JSTSP.2007.897044

a generalization of the usual setting of CAZAC waveforms or codes in which $\mathbb{F} = \mathbb{C}$ and $d = 1$. In this latter case, CAZAC waveforms (and some of their close relatives) are also called by the following names among others: polyphase codes with good periodic or optimum correlation properties, e.g., [44], [41], [27], [16], and [9]; perfect autocorrelation or root-of-unity sequences, e.g., [34], [17], and [21]; bi-unimodular sequences, e.g., [4]–[6], and [25]; bent functions, e.g., [11] and [10]. The literature in this area is extensive, one might say overwhelming. A hint of its breadth and activity in the study of CAZAC waveforms is found in [28]. Fundamental applications are to radar and communications theory, e.g., [32] and [36], [31], respectively. We note that our results are limited to applications to coded CW systems since we have chosen to analyze periodic waveforms.

In this paper, we prove new results for two classes of CAZAC waveforms, which describe the behavior of their discrete periodic ambiguity functions. These are called the Wiener [47] and Milewski classes [33]. We also give first results on our problem of describing vector-valued CAZAC waveforms $u : \mathbb{Z}_N \rightarrow \mathbb{F}^d$, which are also finite-unit norm tight frames (FUNTFs). FUNTFs are a basic model for applications dealing with robust transmission of data over erasure channels such as the internet [22], [7], multiple antenna code design for wireless communications [29], multiple description coding [45], [23], and quantum detection and information [12], [14], [13]. Many of the results invoke elementary number theory for their verification.

In Section I-B, we give requisite definitions and in Section I-C, we describe our results. Our overall goal is to provide several new and useful techniques in waveform design.

We were led to this topic because of three related aspects of our work. These are: waveform design in radar [30]; $\Sigma - \Delta$ quantization for FUNTFs [3] and the potential theoretic characterization of FUNTFs [2]; and our perspective of Norbert Wiener's Generalized Harmonic Analysis [47] *vis à vis* recent, deep work characterizing CAZAC waveforms by Björck and Saffari [4]–[6], [37], [39] and Haagerup [25], [26].

Remark 1.1:

- a) Our emphasis is on $\mathbb{F} = \mathbb{R}$ or $\mathbb{F} = \mathbb{C}$. On the other hand, it is natural to do what we have done for finite extensions of the p -adic rationals, \mathbb{Q}_p , or for the finite fields of p integers under modular addition, where p is prime. It is also natural to conduct our analysis on locally compact, and, hence, complete fields \mathbb{F} . The completeness is essential since every d -dimensional Hilbert space \mathbb{H} over \mathbb{F} is isometric to \mathbb{F}^d ; and so it becomes interesting to investigate our results directly for functions $u : \mathbb{Z}_N \rightarrow \mathbb{H}$, when the intrinsic properties of \mathbb{H} are required as opposed to results valid up to isometries.

b) As we have indicated, this paper deals with *periodic* waveforms. *Aperiodic* waveforms or codes with properties similar to periodic CAZAC waveforms are especially important in modern radar applications, but that is not the subject of this paper.

An aperiodic waveform $u : \mathbb{Z} \rightarrow \mathbb{C}$ is one that is compactly supported. The sequel to the present paper deals with the aperiodic case, focusing on the themes developed herein, but in the context of Golay-Shapiro-Welch codes [19], [20], [43], and [46], which date from 1949, 1951, and 1960, respectively. These closely related and justly famous codes have been reinvented and renamed (alas) in recent years, see [40] for a documentation of this history sometimes repeating itself.

B. Definitions

Gauss was able to construct CAZAC waveforms of any length N , see [6], [38]. In fact, if we let

$$M = \begin{cases} N, & N \text{ odd} \\ 2N, & N \text{ even} \end{cases}$$

then it is elementary to prove that

$$\forall k \in \mathbb{Z}_N, \quad u(k) = e^{2\pi i k^2 / M} \quad (1.1)$$

defines a CAZAC waveform of length N ; see Theorem 3.1. Wiener [47] used such examples as a staple in his theory of Generalized Harmonic Analysis. Because of his deep analysis of autocorrelation in this context, we refer to (1.1) as a *Wiener CAZAC waveform*. When N is odd, a slightly more general Wiener CAZAC waveform, than (1.1), is defined by

$$\forall k \in \mathbb{Z}_N, \quad u(k) = e^{2\pi i (ak^2 + bk) / N}$$

where $a, b \in \mathbb{Z}$ and $(a, N) = 1$, i.e., a and N are relatively prime.

Further, we can use any CAZAC waveform $\{v(k)\}_{k=0}^{M-1}$ to generate a family of CAZAC waveforms of length MN^2 , $N = 2, 3, \dots$. To be precise, let v be a CAZAC waveform of length M , and define the waveform

$$\begin{aligned} \forall k \in \mathbb{Z}_{MN^2}, \quad u(k) &= u(aN + b) = v(a)e^{2\pi i ab / (MN)} \\ k &= aN + b, \\ a &= 0, \dots, MN - 1 \\ b &= 0, \dots, N - 1. \end{aligned} \quad (1.2)$$

This is equivalent to

$$\forall k \in \mathbb{Z}_{MN^2}, \quad u(k) = v \left(\left\lfloor \frac{k}{N} \right\rfloor \bmod M \right) e^{2\pi i \lfloor \frac{k}{N} \rfloor (k \bmod N) / (MN)}$$

where $\lfloor x \rfloor$ is the greatest integer $n_x \leq x$. Milewski [33] verified that u is a CAZAC waveform and, as such, we refer to waveforms u defined by (1.2) as *Milewski CAZAC waveforms* of length MN^2 , see [1] for user-friendly software generating and analyzing Milewski CAZAC waveforms.

A natural generalization of autocorrelation is the discrete periodic ambiguity function, so useful in radar. We shall define it with the following normalization.

Definition 1.2: Let $u : \mathbb{Z}_N \rightarrow \mathbb{C}^d$ be an N -periodic waveform. The *discrete periodic ambiguity function* $A_u : \mathbb{Z}_N \times \mathbb{Z}_N \rightarrow \mathbb{C}$ of u is defined by

$$\begin{aligned} \forall (m, n) &\in \mathbb{Z}_N \times \mathbb{Z}_N, \\ A_u(m, n) &= \frac{1}{N} \sum_{k=0}^{N-1} \langle u(m+k), u(k) \rangle e^{2\pi i kn / N}. \end{aligned}$$

Note that the autocorrelation $A_u(m)$ is $A_u(m, 0)$. Notationally, we shall use j, k, m as ‘‘time’’ variables, and n, q, r as ‘‘frequency’’ variables. Also, $\delta(j) = 0$ if $j \neq 0$ and $\delta(0) = 1$. Further, $a \nmid b$ indicates that the integer a does not divide the integer b ; and $\mathbb{1}_S$ designates the characteristic function of the set S .

CAZAC waveforms can be thought of in terms of FUNTFs as we do in Section V. There is an even more basic relation in terms of tight frames due to the characterization of CAZAC waveforms as circulant Hadamard matrices with complex entries (which can be thought of as tight frames); see [6] for the characterization. As such, we now define finite frames.

Definition 1.3:

- A sequence $\{x_{(j)}\}_{j=1}^N \subseteq \mathbb{F}^d$ is a *finite frame* for \mathbb{F}^d if $\{x_{(j)}\}_{j=1}^N$ spans \mathbb{F}^d .
- Let $\{x_{(j)}\}_{j=1}^N \subseteq \mathbb{F}^d$. The *Bessel (analysis) operator*, $L : \mathbb{F}^d \rightarrow \ell^2(\mathbb{Z}_N)$, for $\{x_{(j)}\}_{j=1}^N$ is defined by

$$\forall x \in \mathbb{F}^d, \quad L(x) = \{ \langle x, x_{(j)} \rangle \}_{j=1}^N$$

where $\ell^2(\mathbb{Z}_N)$, the space of \mathbb{F} -valued functions on \mathbb{Z}_N , can be identified with $\mathbb{F} \times \dots \times \mathbb{F}$ (N -times). L is the $N \times d$ matrix operator $L = (x_{(1)} \dots x_{(N)})^\tau$, where τ designates the (complex) adjoint. The *adjoint (synthesis) operator*, $L^* : \ell^2(\mathbb{Z}_N) \rightarrow \mathbb{F}^d$, of L is characterized by the equation

$$\forall v = \{v_{(j)}\}_{j=1}^N \in \ell^2(\mathbb{Z}_N), \quad L^*(v) = \sum_{j=1}^N v_{(j)} x_{(j)} \in \mathbb{F}^d,$$

where v is considered as an $N \times 1$ vector. L^* is the $d \times N$ matrix operator $L^* = (x_{(1)}, \dots, x_{(N)}) \in \mathbb{F}^d \times \dots \times \mathbb{F}^d$ (N -times).

- Let $\{x_{(j)}\}_{j=1}^N \subseteq \mathbb{F}^d$. $S = L^*L : \mathbb{F}^d \rightarrow \mathbb{F}^d$ is the *frame operator* and $G = LL^* : \ell^2(\mathbb{Z}_N) \rightarrow \ell^2(\mathbb{Z}_N)$ is the *Gram operator* for $\{x_{(j)}\}_{j=1}^N$.

It is straightforward to calculate that

$$\forall x \in \mathbb{F}^d, \quad S(x) = \sum_{j=1}^N \langle x, x_{(j)} \rangle x_{(j)} \in \mathbb{F}^d$$

and

$$\forall v \in \ell^2(\mathbb{Z}_N), \quad G(v) = \sum_{j=1}^N \overline{\langle x_{(k)}, x_{(j)} \rangle} v_{(j)} \in \ell^2(\mathbb{Z}_N).$$

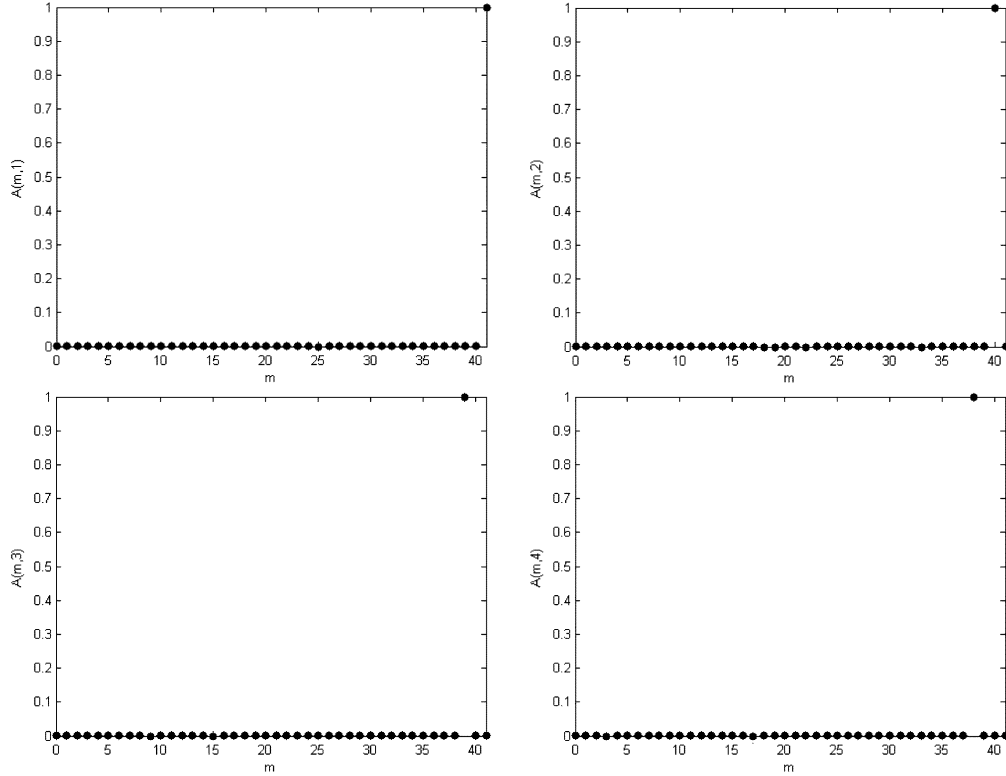


Fig. 1. Ambiguity function modulus $|A_u(\bullet, n)|$, as a function of m , of a length 42 Wiener CAZAC waveform u evaluated at $n = 1, 2, 3, 4$, where $u(k) = \omega^{k^2}$ for $\omega = e^{2\pi i/84}$.

$G = (\overline{\langle x(k), x(j) \rangle})_{k,j=1}^N$ is the $N \times N$ Gram matrix operator.

The following result is well-known, e.g., [2], [8].

Proposition 1.4: Let $\{x(j)\}_{j=1}^N \subseteq \mathbb{F}^d$.

a) $\{x(j)\}_{j=1}^N$ is a frame for \mathbb{F}^d if and only if

$\exists A, B > 0$ such that $\forall x \in \mathbb{F}^d$,

$$A\|x\|^2 \leq \sum_{j=1}^N |\langle x, x(j) \rangle|^2 \leq B\|x\|^2.$$

b) $\{x(j)\}_{j=1}^N$ is a frame for \mathbb{F}^d if and only if S is a bijection on \mathbb{F}^d .

c) If $\{x(j)\}_{j=1}^N$ is a frame for \mathbb{F}^d , then $G : L(\mathbb{F}^d) \rightarrow L(\mathbb{F}^d)$ is a bijection, and

$$\begin{aligned} \forall x \in \mathbb{F}^d, \quad x &= \sum_{j=1}^N \langle x, S^{-1}x(j) \rangle x(j) \\ &= \sum_{j=1}^N \langle x, x(j) \rangle S^{-1}x(j) = L^*G^{-1}(L(x)). \end{aligned}$$

A and B in Proposition 1.4a) are *frame constants*. If $\{x(j)\}_{j=1}^N$ is a frame for \mathbb{F}^d and if $A = B$ in Proposition 1.4a), then $\{x(j)\}_{j=1}^N$ is a *tight* frame. In this case, the decomposition in Proposition 1.4c) can be simplified to

$$\forall x \in \mathbb{F}^d, \quad x = \frac{d}{N} \sum_{j=1}^N \langle x, x(j) \rangle x(j).$$

We shall also use the discrete Fourier transform (DFT).

Definition 1.5: The $N \times N$ DFT matrix D_N is

$$D_N = \left(e^{-2\pi i mn/N} \right)_{m,n=0}^{N-1}.$$

The DFT \hat{v} of $v \in \ell^2(\mathbb{Z}_N)$ is defined by

$$\forall n \in \mathbb{Z}_N, \quad \hat{v}(n) = \sum_{m=0}^{N-1} v(m) e^{-2\pi i mn/N}$$

i.e., $\hat{v} = D_N v$.

C. Results

The results of Section II are well known. They are included for perspective and the fact that our point of view of dealing with the nonabelian group \mathcal{G}_N may be new. Specifically, we want to emphasize that there are many *non-chirp-like* CAZAC waveforms.

Theorem 3.3 and its consequences, Corollary 3.4 and Example 3.5, as well as the accompanying Figs. 1–4 for Wiener waveforms, are new. We note that the zero sets for the discrete periodic ambiguity function in the cases of Figs. 1–4 do not translate in such a pristine way for the aperiodic case. In fact, the aperiodic ambiguity function analysis of Wiener waveforms gives rise to more complex results as is seen by considering the classical integral ambiguity function of pulse waveforms such as

$$\sum_{m=0}^{N-1} u(m) \mathbb{1}_{[m, m+1]}.$$

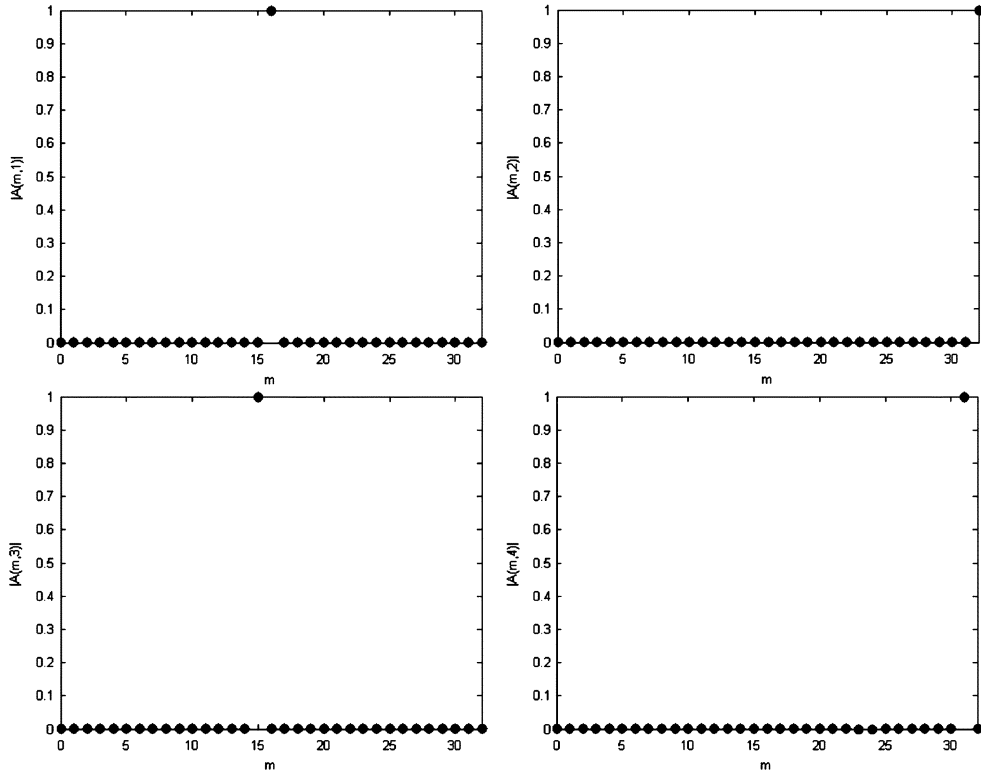


Fig. 2. Ambiguity function modulus $|A_u(\bullet, n)|$, as a function of m , of a length 33 Wiener CAZAC waveform u evaluated at $n = 1, 2, 3, 4$, where $u(k) = \omega^{k^2}$ for $\omega = e^{2\pi i/33}$.

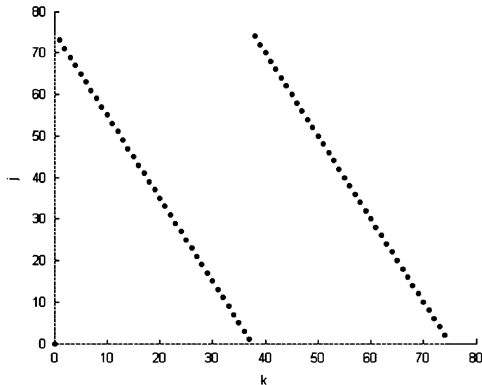


Fig. 3. Ambiguity function domain of a length 75 Wiener CAZAC waveform u , where $|A_u(m, n)| = 1$ for a dot (m, n) and $A_u(m, n) = 0$ otherwise, and where $u(k) = \omega^{k^2}$ for $\omega = e^{2\pi i/75}$.

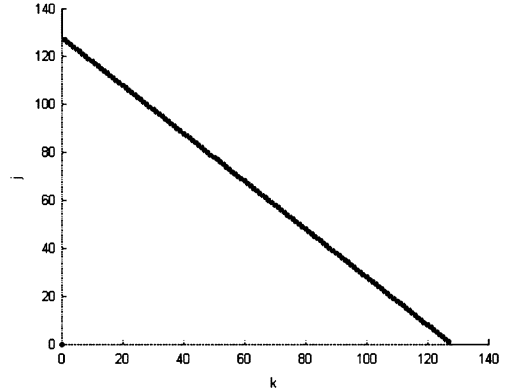


Fig. 4. Ambiguity function domain of a length 128 Wiener CAZAC waveform u , where $|A_u(m, n)| = 1$ for a dot (m, n) and $A_u(m, n) = 0$ otherwise, and where $u(k) = \omega^{k^2}$ for $\omega = e^{2\pi i/256}$.

In any case, the impact of our periodic results is that even chirp-like CAZAC waveforms are not stable under small perturbations in the domain $\mathbb{Z}_N \times \mathbb{Z}_N$ of the discrete periodic ambiguity function. Theorems 4.1, 4.2, and 4.3, as well as the accompanying Figs. 5–8, provide the analogous more complicated behavior of Milewski waveforms.

In Section V, we relate CAZAC waveforms with the theory of frames in a fundamental problem we have posed with an eye to vector-valued and multidimensional waveform design (and emerging applications). Theorems 5.3, 5.4, and 5.5 provide partial solutions to this problem. We should point out that this material was developed with the idea of providing a theoretical basis

for fundamental work being done in acoustic and electromagnetic vector sensing, see [35], cf., results in [24] on multichannel waveform design.

Section VI introduces several applicable techniques to characterize the structure of the discrete periodic ambiguity function matrix (Propositions 6.1, 6.2, 6.3, 6.4, 6.6, and Example 6.8). We also determine the signal u for given A_u data (Theorem 6.5 and Remark 6.7), and compute mean square error (MSE) for ZAC waveforms (Theorem 6.9); see Proposition 2.4.

II. CAZAC WAVEFORMS IN \mathbb{C}

Consider mappings $\alpha : \ell^2(\mathbb{Z}_N) \rightarrow \ell^2(\mathbb{Z}_N)$ of the following form.

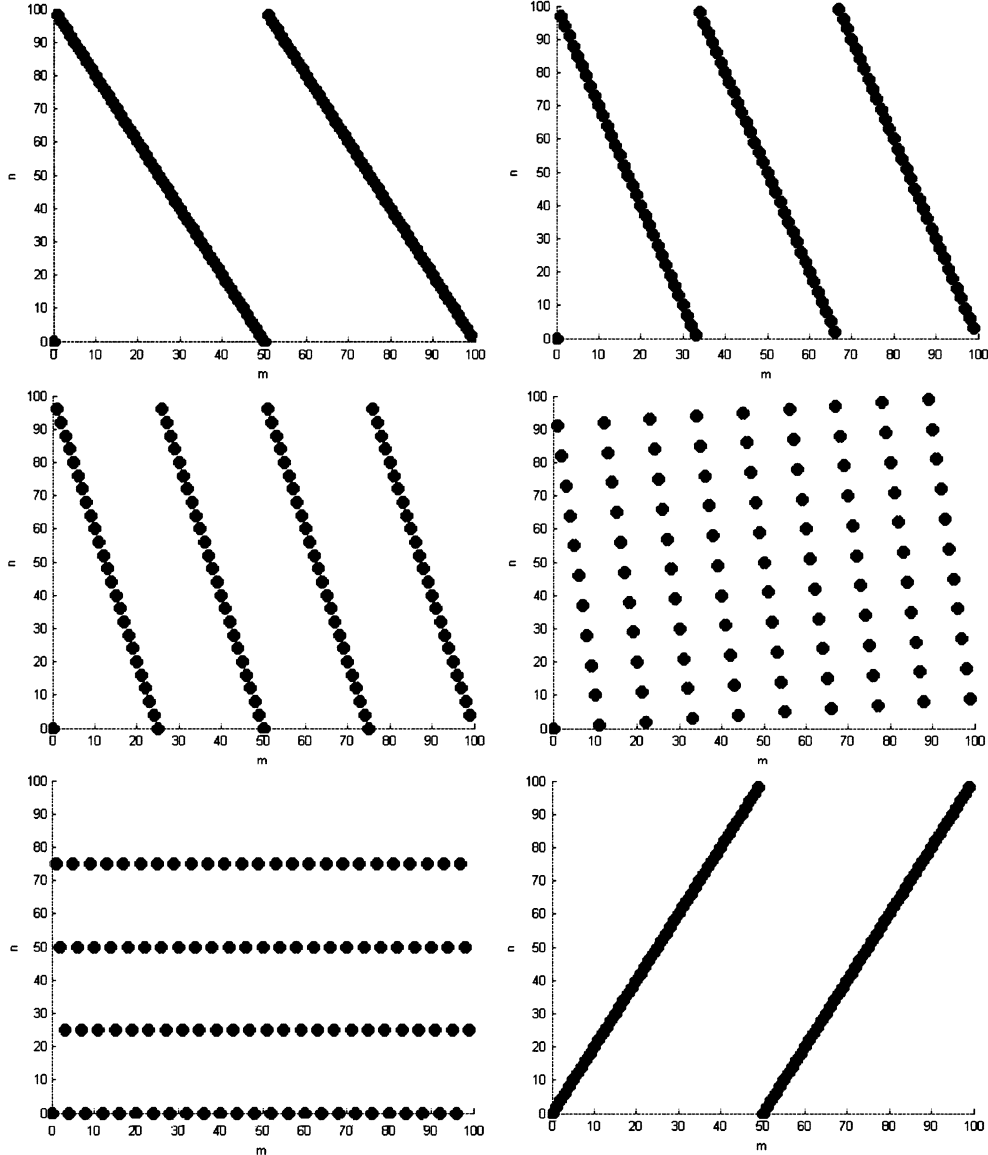


Fig. 5. Ambiguity function domain of a length-100 Wiener CAZAC waveform u , defined in Theorem 3.3 and for $j = 2, 3, 4, 9, 25, 98$.

- Rotation $\rho_a(u) = au$ by $a \in \mathbb{C}$, $|a| = 1$.
- Translation (cyclic shift) $\tau_{-j}(u)$ of $u \in \ell^2(\mathbb{Z}_N)$ by $j \in \mathbb{Z}$, defined as $\tau_{-j}(u)(k) = u(k + j)$.
- Decimation (permutation subgroup) $\pi_j(u)$ of $u \in \ell^2(\mathbb{Z}_N)$ by $j \in \mathbb{Z}$, $(j, N) = 1$, defined as $\pi_j(u)(k) = u(jk)$.
- Linear frequency modulation $\mu_{q,\omega}(u)$ of $u \in \ell^2(\mathbb{Z}_N)$ by $q \in \mathbb{Z}$ and any N th root of unity ω , defined as $\mu_{q,\omega}(u)(k) = \omega^{kq}u(k)$.
- Conjugation $\kappa(u) = \bar{u}$.

We have

$$A_{\rho_a(u)}(m) = A_u(m) \quad (2.1)$$

$$A_{\tau_{-j}(u)}(m) = A_u(m) \quad (2.2)$$

$$A_{\pi_j(u)}(m) = A_u(jm), \quad (j, N) = 1 \quad (2.3)$$

$$A_{\mu_{q,\omega}(u)}(m) = \omega^{mq}A_u(m) \quad (2.4)$$

$$A_{\kappa(u)}(m) = \overline{A_u(m)} = A_u(-m) = A_u(N - m) \quad (2.5)$$

where jm and $N - m$ are evaluated mod N . Equation (2.3) is a

consequence of the fact that \mathbb{Z}_N is identified with $\{kj : 0 \leq k \leq N - 1\}$ in the case $(j, N) = 1$.

Theorem 2.1 is an elementary extension of (2.1)–(2.5) to the discrete periodic ambiguity function.

Theorem 2.1: Let $u : \ell^2(\mathbb{Z}_N) \rightarrow \ell^2(\mathbb{Z}_N)$ and let $m, n \in \mathbb{Z}_N$.

- If $|a| = 1$, then $A_{\rho_a(u)}(m, n) = A_u(m, n)$.
- If $j \in \mathbb{Z}$, then $A_{\tau_{-j}(u)}(m, n) = e^{-2\pi i j n / N} A_u(m, n)$.
- Let $1 \leq j \leq N - 1$. If $(j, N) = 1$, then the multiplicative inverse $j^{-1} \in \mathbb{Z}_N$ exists and $A_{\pi_j(u)}(m, n) = A_u(jm, n/j)$, where jm and n/j are evaluated mod N .
- If $q \in \mathbb{Z}$ and ω is an N th root of unity, then $A_{\mu_{q,\omega}(u)}(m, n) = \omega^{mq}A_u(m, n)$.
- $A_{\kappa(u)}(m, n) = \overline{A_u(m, -n)} = e^{-2\pi i m n / N} A_u(-m, n) = e^{-2\pi i m n / N} A_u(N - m, n)$.

Definition 2.2: Let $u, v \in \ell^2(\mathbb{Z}_N)$. u and v are *equivalent* if v can be obtained from u by a finite composition (finite succession) α of the mappings $\rho_a, \tau_{-j}, \pi_j, \mu_{q,\omega}$, and κ . The set of all such finite compositions α is denoted by \mathcal{G}_N .

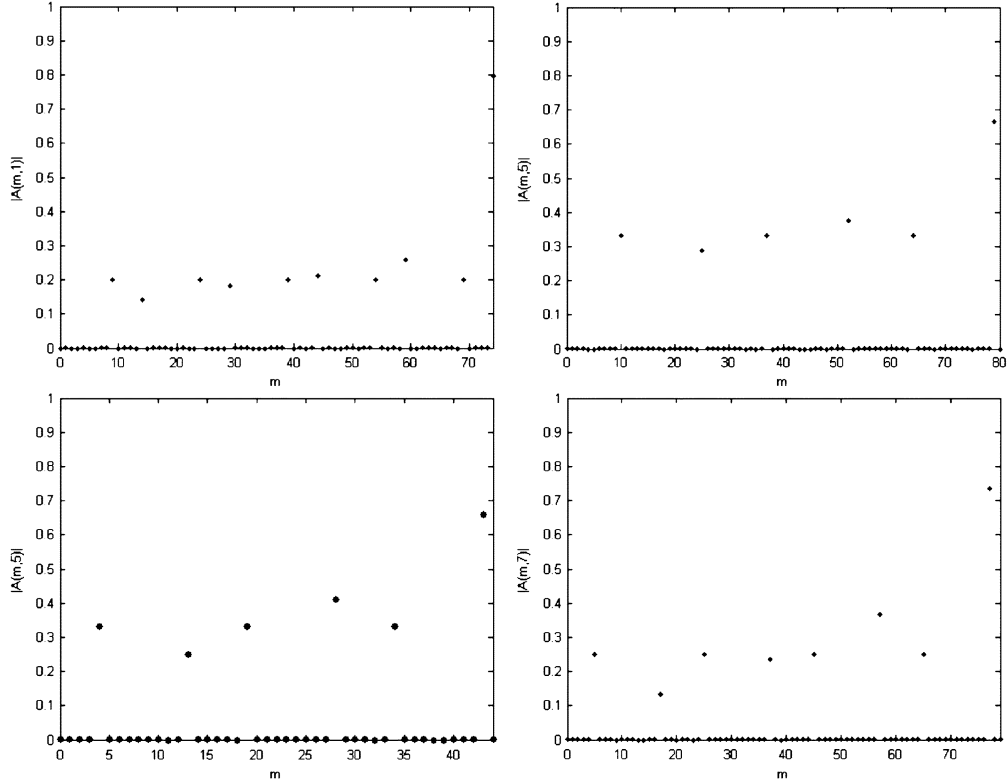


Fig. 6. Ambiguity function modulus $|A_u(\bullet, n)|$, as a function of m , of length 3×5^2 , 9×3^2 , 5×3^2 , and 5×4^2 Milewski CAZAC waveforms evaluated at $n = 1, 5, 5$, and 7 , respectively.

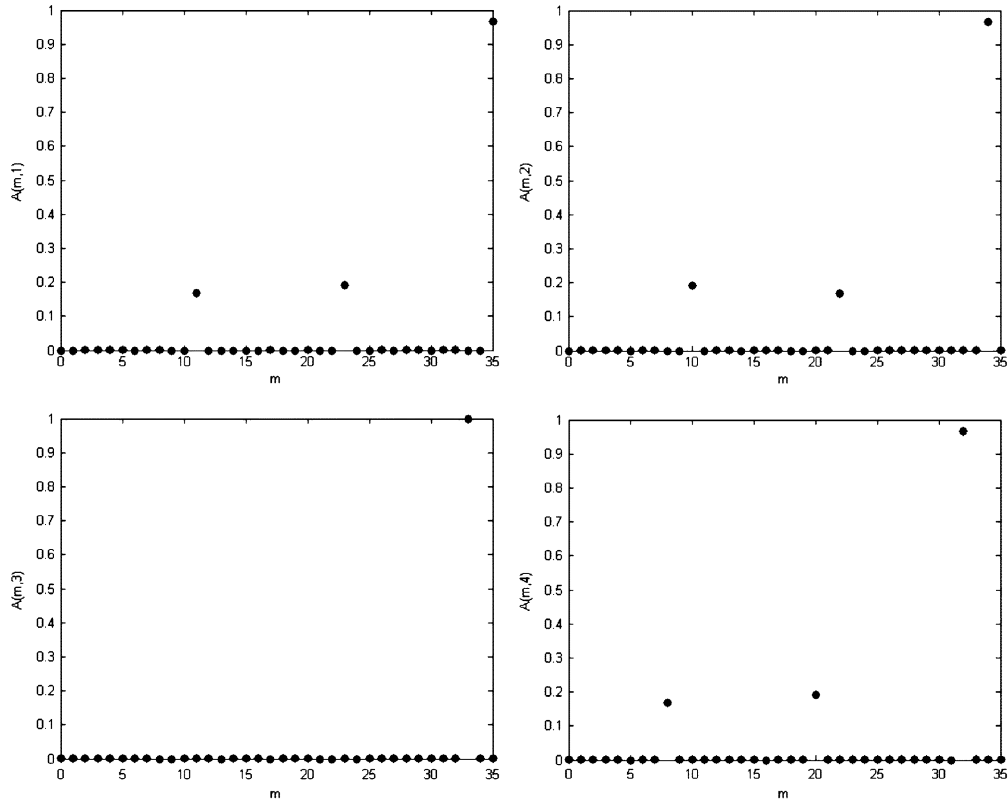


Fig. 7. Ambiguity function modulus $|A_u(\bullet, n)|$, as a function of m , of a length 4×3^2 Milewski CAZAC waveform evaluated at $n = 1, 2, 3, 4$.

This notion of *equivalence* defines an *equivalence relation* $R \subseteq \ell^2(\mathbb{Z}_N) \times \ell^2(\mathbb{Z}_N)$ on $\ell^2(\mathbb{Z}_N)$; and \mathcal{G}_N is a nonabelian group which is the focus of a sequel by the authors.

Remark 2.3: Define the partition, $\{X_{\rho,u} : u \in \ell^2(\mathbb{Z}_N)\}$, by the rule that $X_{\rho,u} = \{v \in \ell^2(\mathbb{Z}_N) : \exists |a| = 1 \text{ such that } v = au\}$. The assertion that $\{X_{\rho,u}\}$ is a *partition* means that the sets

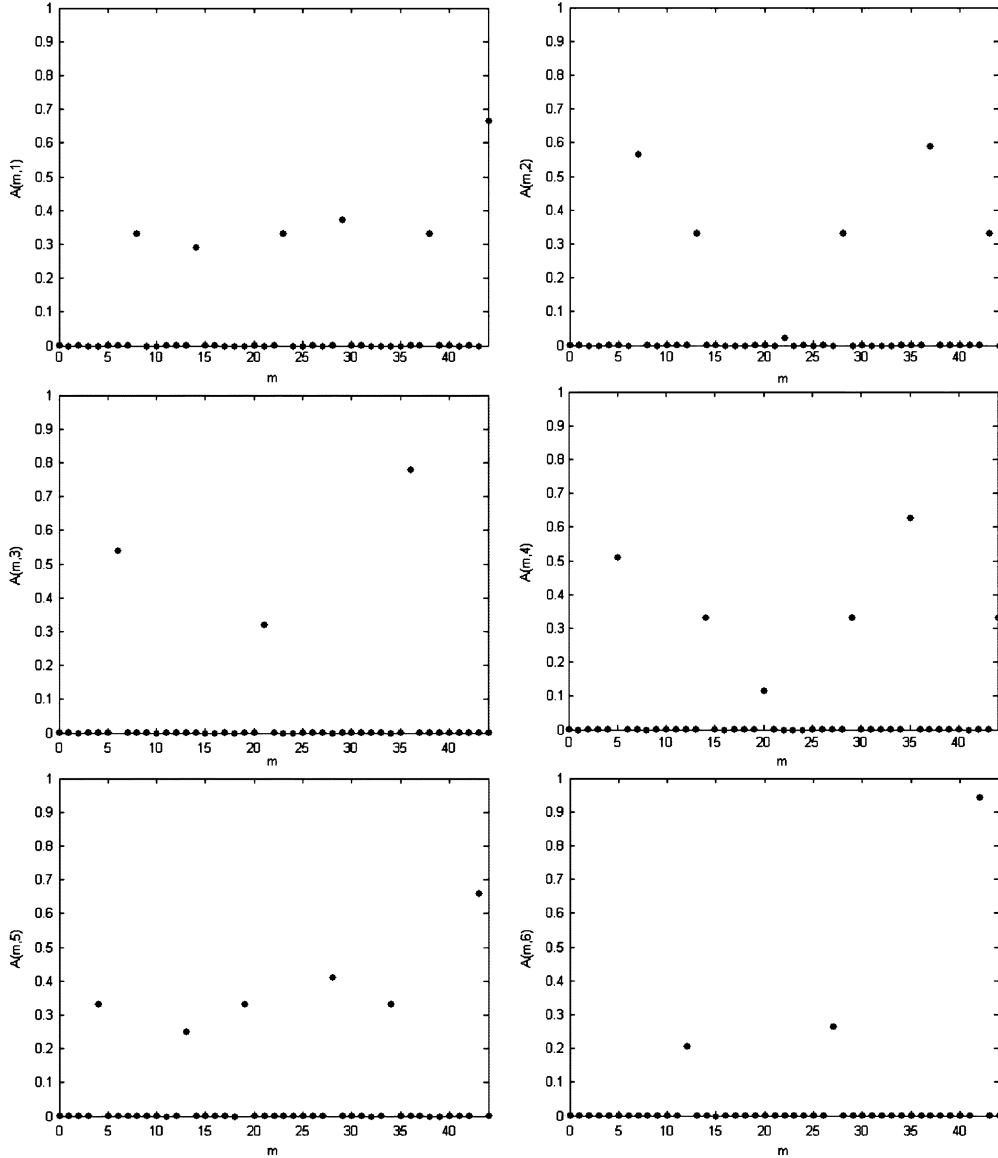


Fig. 8. Ambiguity function modulus $|A_u(\bullet, n)|$, as a function of m , of a length 5×3^2 Milewski CAZAC waveform, generated by a length-5 Wiener CAZAC waveform and evaluated at $n = 1, 2, 3, 4, 5, 6$.

$X_{\rho, u}, u \in \ell^2(\mathbb{Z}_N)$, are disjoint and their union over u is $\ell^2(\mathbb{Z}_N)$. $\{X_{\rho, u}\}$ defines an equivalence relation $R_\rho \subseteq \ell^2(\mathbb{Z}_N) \times \ell^2(\mathbb{Z}_N)$ whose equivalence classes $X_{\rho, u}$ satisfy

$$X_{\rho, u} \subseteq X_{R, u} = \{v : \exists \alpha \in \mathcal{G}_N \text{ such that } \alpha(u) = v\}$$

where $\{X_{R, u}\}$ is the partition of $\ell^2(\mathbb{Z}_N)$ defined by the equivalence relation R .

There is the following compelling problem for R_ρ , and therefore associated with the notion of equivalence in Definition 2.2: for a given N , compute or estimate the number of nonequivalent CAZAC waveforms. The problem has been investigated by Gabidulin [17], [18]. Björck and Saffari [6] proved that if $N = MK^2$ then there are infinitely many nonequivalent CAZAC waveforms, e.g., $N = 8, 9$, or 12 . (The case $N = 4$ is straightforward). On the other hand, Haagerup [26] has given a

complete mathematical proof that if N is prime, then there are only finitely many nonequivalent CAZAC waveforms.

The following two propositions are well known and elementary to verify.

Proposition 2.4: If $\{u(k)\}_{k=0}^{N-1} \subseteq \mathbb{C}$ has constant amplitude (CA) on \mathbb{Z}_N , e.g., if u is unimodular, then its DFT has the zero-autocorrelation property (ZAC), i.e., $A_u(m) = \delta(m)$ for $m \in \mathbb{Z}_N$. If $\{u(k)\}_{k=0}^{N-1}$ has the zero autocorrelation property (ZAC), then its DFT has CA. Thus, $\{u(k)\}_{k=0}^{N-1}$ is a CAZAC waveform if and only if the normalized DFT $(1/\sqrt{N})\hat{u}$ is a CAZAC waveform.

Proposition 2.5: Let $(N_1, N_2) = 1$ and let $u : \mathbb{Z}_{N_1} \rightarrow \mathbb{C}$ and $v : \mathbb{Z}_{N_2} \rightarrow \mathbb{C}$ be CAZAC waveforms. Then $w = uv : \mathbb{Z}_N \rightarrow \mathbb{C}, N = N_1N_2$ is a CAZAC waveform.

This method of making new longer CAZAC waveforms from given CAZAC waveforms is *not* the same as the Milewski method.

Example 2.6:

- Let N be odd. Binary CAZAC waveforms $u : \mathbb{Z}_N \rightarrow \{\pm 1\}$ can not exist. In fact, if u is constant, then $A_u = 1$ on \mathbb{Z}_N . If u is not constant, then $\sum_{k=0}^{N-1} u(m+k)u(k)$ is a sum with N terms, each taking the value ± 1 ; as such $A_u(m) \neq 0$ for $m \in \mathbb{Z}_N \setminus \{0\}$. It is easy to see that $A_u(m) \neq 0$ for $m \in \mathbb{Z}_N \setminus \{0\}$. Even more, it is elementary to verify that $A_u(m)$ is odd for $m \in \mathbb{Z}_N \setminus \{0\}$.
- Let N be arbitrary. It is well known that if $u : \mathbb{Z}_N \rightarrow \{\pm 1\}$, then $A_u(m) = N \pmod{4}$. Thus, if $A_u(m)$ has zeros, and, in particular, if u is a CAZAC waveform, then 4 divides N .
- Let N be arbitrary. The only known binary CAZAC waveform $u : \mathbb{Z}_N \rightarrow \{\pm 1\}$, up to any translation and multiplication by -1 , is $\{1, 1, 1, -1\}$. Also, it is clear that any Milewski waveform generated by $\{1, 1, 1, -1\}$ is not binary. However, there do exist periodic complex binary sequences, not ± 1 , which are CAZAC waveforms, e.g., Björck (1985) [4], [5] and Golomb (1992) [21], cf., [25]. In fact, Saffari [37], [39] was able to find all such complex binary sequences.

III. AMBIGUITY FUNCTION ANALYSIS OF WIENER CAZACS

As indicated in Section I-B, the Wiener waveforms defined in (1.1) have long been known to be CAZAC waveforms. This assertion can be also stated in terms of primitive roots of unity, which we do in Theorem 3.1; and the proof is elementary, and, hence, omitted. Since this extension of (1.1) in terms of primitive roots is so natural, we shall also refer to such functions as *Wiener waveforms*.

Theorem 3.1: Given $N \geq 1$. Let

$$M = \begin{cases} N, & N \text{ odd} \\ 2N, & N \text{ even} \end{cases}$$

and let ω be a primitive M th root of unity. Define the Wiener waveform $u : \mathbb{Z}_N \rightarrow \mathbb{C}$ by $u(k) = \omega^{k^2}$, $0 \leq k \leq N-1$. Then u is a CAZAC waveform.

Remark 3.2: Periodic waveforms similar to Wiener waveforms have long been used in engineering, e.g., in continuous wave (CW) radar (see [32, ch. 10]). Such waveforms go back to Frank (1953) with significant subsequent contributions through the 1970s by Heimiller (1961) [27], Frank and Zadoff (1962) [16], Schroeder (1970) [42], Chu (1972) [9], and Frank (1973) [15].

Theorem 3.3: Let $j \in \mathbb{Z}$. Define $u_j : \mathbb{Z}_N \rightarrow \mathbb{C}$ 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

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

Proof: Let N be even, and set $u_j(k) = e^{\pi i j k^2 / N}$. We calculate

$$\begin{aligned} A_{u_j}(m, n) &= \frac{1}{N} \sum_{k=0}^{N-1} u_j(m+k) \overline{u_j(k)} e^{2\pi i k n / N} \\ &= \frac{1}{N} \sum_{k=0}^{N-1} e^{(\pi i / N)(j m^2 + 2j k m + 2k n)} \\ &= e^{\pi i j m^2 / N} \frac{1}{N} \sum_{k=0}^{N-1} e^{2\pi i k (j m + n) / N}. \end{aligned}$$

If $jm + n \equiv 0 \pmod{N}$, then

$$\frac{1}{N} \sum_{k=0}^{N-1} e^{2\pi i k (j m + n) / N} = 1.$$

Otherwise, we have

$$\frac{1}{N} \sum_{k=0}^{N-1} e^{2\pi i k (j m + n) / N} = \frac{e^{(2\pi i (j m + n) / N) N} - 1}{e^{2\pi i (j m + n) / N} - 1} = 0.$$

Let N be odd, and set $u(k) = e^{2\pi i k^2 / N}$. We calculate

$$\begin{aligned} A_{u_j}(m, n) &= \frac{1}{N} \sum_{k=0}^{N-1} u_j(m+k) \overline{u_j(k)} e^{2\pi i k n / N} \\ &= \frac{1}{N} \sum_{k=0}^{N-1} e^{(2\pi i / N)(j m^2 + 2j k m + k n)} \\ &= e^{2\pi i j m^2 / N} \frac{1}{N} \sum_{k=0}^{N-1} e^{2\pi i k (2j m + n) / N}. \end{aligned}$$

If $2jm + n \equiv 0 \pmod{N}$, then

$$\frac{1}{N} \sum_{k=0}^{N-1} e^{2\pi i k (2j m + n) / N} = 1.$$

Otherwise, we have

$$\frac{1}{N} \sum_{k=0}^{N-1} e^{2\pi i k (2j m + n) / N} = \frac{e^{2\pi i (2j m + n) / N} - 1}{e^{2\pi i (2j m + n) / N} - 1} = 0.$$

□

The discrete periodic ambiguity function, A_u , of a Wiener CAZAC waveform $u : \mathbb{Z}_N \rightarrow \mathbb{C}$, as given in Theorem 3.1, 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 $A_u(\bullet, n)$ as a function of m consists of a single peak, see Figs. 1 and 2. In fact, we have the following consequence of Theorem 3.3.

Corollary 3.4: Let $\{u(k)\}_{k=0}^{N-1}$ be a Wiener CAZAC waveform as given in Theorem 3.1. (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

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

Example 3.5:

a) Let N be odd and let $\omega = e^{2\pi i/N}$. Then, $u(k) = \omega^{k^2}$, $0 \leq k \leq N-1$, is a CAZAC waveform. By Corollary 3.4, $|A_u(m, n)| = |\omega^{m^2}| = 1$ if $2m+n = l_{m,n}N$ for some $l_{m,n} \in \mathbb{Z}$ 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 $2m+n = l_{m,n}N$ for some $l_{m,n} \in \mathbb{Z}$, we have the following phenomenon. If $0 \leq m \leq (N-1/2)$ and $2m+n = l_{m,n}N$ for some $l_{m,n} \in \mathbb{Z}$, then n is odd; and if $(N+1/2) \leq m \leq N-1$ and $2m+n = l_{m,n}N$ for some $l_{m,n} \in \mathbb{Z}$, 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 $0 \leq m \leq (N-1/2)$ has odd function values n ; and the line whose domain is $(N+1/2) \leq m \leq N-1$ has even function values n , see Fig. 3, cf., Fig. 4.

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

Let $u : \mathbb{Z}_N \rightarrow \mathbb{C}$ be a Wiener waveform. Thus, $u(k) = \omega^{k^2}$, $0 \leq k \leq N-1$, and $\omega = e^{2\pi i j/M}$, $(j, M) = 1$, where M is defined in terms of N in Theorem 3.1. By Corollary 3.4, for each fixed $n \in \mathbb{Z}_N$, the function $A_u(\bullet, n)$ of m vanishes everywhere except for a *unique* value $m_n \in \mathbb{Z}_N$ for which $|A_u(m_n, n)| = 1$.

The hypotheses of Theorem 3.3 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 , $A_u(\bullet, n)$ will be identically 0 and, for certain values of n , $|A_u(\bullet, n)| = 1$ will have several solutions, see Fig. 5, cases $j = 2, 4, 25, 98$. For example, if $N = 100$ and $j = 2$, then, for each odd n , $A_u(\bullet, n) = 0$ as a function of m . If $N = 100$ and $j = 3$, then $(100, 3) = 1$ so 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 $m \neq m_n$.

IV. AMBIGUITY FUNCTION ANALYSIS OF MILEWSKI CAZACS

The following theorem shows that for a fixed value of n , the discrete periodic ambiguity function, $A_u(m, n)$, of a Milewski CAZAC waveform is well behaved in the sense that it vanishes for a large set of values of m ; see Fig. 6.

Theorem 4.1: Let $\{u(k)\}_{k=1}^{MN^2}$ be a Milewski CAZAC waveform generated by a CAZAC waveform $v : \mathbb{Z}_M \rightarrow \mathbb{C}$. If $m, n \in \mathbb{Z}$ have the property that $N \nmid (m+n)$, then $A_u(m, n) = 0$.

Proof: We first write A_u as follows:

$$\begin{aligned} A_u(m, n) &= \frac{1}{MN^2} \sum_{k=0}^{MN^2-1} u(m+k) \overline{u(k)} e^{2\pi i kn/(MN^2)} \\ &= \frac{1}{MN^2} \sum_{k=0}^{MN^2-1} v\left(\left\lfloor \frac{m+k}{N} \right\rfloor \pmod{M}\right) \\ &\quad \times v\left(\overline{\left\lfloor \frac{k}{N} \right\rfloor \pmod{M}}\right) e^\eta \end{aligned}$$

where $\eta = (2\pi i/MN)(\lfloor (m+k/N) \rfloor (m+k \pmod{N}) - \lfloor (k/N) \rfloor (k \pmod{N}) + (kl/N))$. Next, write each k as $k = \gamma + sMN$, where $\gamma = 0, 1, \dots, MN-1$ and $s = 0, 1, \dots, N$. Then

$$\begin{aligned} A_u(m, n) &= \frac{1}{MN^2} \sum_{\gamma=0}^{MN-1} \sum_{s=0}^{N-1} v\left(\left\lfloor \frac{m+\gamma+sMN}{N} \right\rfloor \pmod{M}\right) \\ &\quad \times v\left(\overline{\left\lfloor \frac{\gamma+sMN}{N} \right\rfloor \pmod{M}}\right) e^\eta \\ &= \frac{1}{MN^2} \sum_{\gamma=0}^{MN-1} \sum_{s=0}^{N-1} v\left(\left\lfloor \frac{m+\gamma}{N} \right\rfloor \pmod{M}\right) \\ &\quad \times v\left(\overline{\left\lfloor \frac{\gamma}{N} \right\rfloor \pmod{M}}\right) e^\eta, \end{aligned}$$

where

$$\begin{aligned} \eta &= \frac{2\pi i}{MN} \left(\left\lfloor \frac{m+\gamma+sMN}{N} \right\rfloor \right. \\ &\quad \times (m+\gamma+sMN \pmod{N}) \\ &\quad \left. - \left\lfloor \frac{\gamma+sMN}{N} \right\rfloor (\gamma+sMN \pmod{N}) \right. \\ &\quad \left. + \frac{(\gamma+sMN)n}{N} \right) \\ &= \frac{2\pi i}{MN} \left(\left(\left\lfloor \frac{m+\gamma}{N} \right\rfloor + sM \right) (m+\gamma \pmod{N}) \right. \\ &\quad \left. - \left(\left\lfloor \frac{\gamma}{N} \right\rfloor + sM \right) (\gamma \pmod{N}) + \frac{\gamma n}{N} + sMn \right) \\ &= \frac{2\pi i}{MN} \left(\left\lfloor \frac{m+\gamma}{N} \right\rfloor (m+\gamma \pmod{N}) \right. \\ &\quad \left. - \left\lfloor \frac{\gamma}{N} \right\rfloor (\gamma \pmod{N}) + \frac{\gamma n}{N} \right. \\ &\quad \left. + sM(m+\gamma \pmod{N} - \gamma \pmod{N} + n) \right) \end{aligned}$$

$$\begin{aligned} \beta(m, n, \gamma) &= v\left(\left\lfloor \frac{m+\gamma}{N} \right\rfloor \pmod{M}\right) \\ &\quad \times v\left(\overline{\left\lfloor \frac{\gamma}{N} \right\rfloor \pmod{M}}\right) e^{\delta(m, n, \gamma)} \end{aligned}$$

and

$$\begin{aligned} \delta(m, n, \gamma) &= \frac{2\pi i}{MN} \left(\left\lfloor \frac{m+\gamma}{N} \right\rfloor (m+\gamma \pmod{N}) \right. \\ &\quad \left. - \left\lfloor \frac{\gamma}{N} \right\rfloor (\gamma \pmod{N}) + \frac{\gamma n}{N} \right). \end{aligned}$$

Therefore

$$\begin{aligned} A_u(m, n) &= \frac{1}{MN^2} \sum_{\gamma=0}^{MN-1} \beta(m, n, \gamma) \\ &\quad \times \sum_{s=0}^{N-1} \left(e^{\frac{2\pi i}{N}((m+\gamma) \pmod{N} - \gamma \pmod{N} + n)} \right)^s. \end{aligned}$$

If $N \nmid (m + \gamma \bmod N - \gamma \bmod N + n)$, i.e., $N \nmid (m + n)$, then

$$A_u(m, n) = \frac{1}{MN^2} \sum_{\gamma=0}^{MN-1} \beta(m, n, \gamma) \times \frac{\left(e^{\frac{2\pi i}{N}((m+\gamma) \bmod N - \gamma \bmod N + n)} \right)^N - 1}{e^{\frac{2\pi i}{N}((m+\gamma) \bmod N - \gamma \bmod N + n)} - 1} = 0.$$

□

The graphs of the discrete periodic ambiguity function of Milewski CAZAC waveforms are periodic. The precise nature of this periodicity is the content of the following result.

Theorem 4.2: Let $\{u(k)\}_{k=1}^{MN^2}$ be a Milewski CAZAC waveform generated by a CAZAC waveform $v : \mathbb{Z}_M \rightarrow \mathbb{C}$, and let $s \in \mathbb{Z}$. Then

$$\forall (m, n) \in \mathbb{Z}_N \times \mathbb{Z}_N, \quad |A_u(m, n)| = |A_u(m - sMN, n + sMN)|.$$

Proof: By definition

$$\begin{aligned} A_u(m - sMN, n + sMN) &= \frac{1}{MN^2} \sum_{k=0}^{MN^2-1} u(m - sMN + k) \overline{u(k)} e^{\frac{2\pi i}{MN^2} k(n+sMN)} \\ &= \frac{1}{MN^2} \sum_{k=0}^{MN^2-1} v\left(\left[\frac{m+k}{N}\right] \bmod M\right) \overline{v\left(\left[\frac{k}{N}\right]\right)} e^{\eta'} \end{aligned}$$

where

$$\begin{aligned} \eta' &= \frac{2\pi i}{MN} \left(\left[\frac{m - sMN + k}{N} \right] \right. \\ &\quad \times (m - sMN + k \bmod N) \\ &\quad \left. - \left[\frac{k}{N} \right] (k \bmod N) + \frac{k(n + sMN)}{N} \right) \\ &= \frac{2\pi i}{MN} \left(\left(\left[\frac{m+k}{N} \right] - sM \right) (m + k \bmod N) \right. \\ &\quad \left. - \left[\frac{k}{N} \right] (k \bmod N) + \frac{kn}{N} + sMk \right) \\ &= \frac{2\pi i}{MN} \left(\left[\frac{m+k}{N} \right] (m + k \bmod N) \right. \\ &\quad \left. - \left[\frac{k}{N} \right] (k \bmod N) + \frac{kn}{N} \right) \\ &\quad + \frac{2\pi i}{MN} (-sM(m + k \bmod N) + sMk). \end{aligned}$$

We can write η' as

$$\begin{aligned} \eta' &= \eta + \frac{2\pi i}{N} (k - (m + k \bmod N)) \\ &= \eta + \frac{2\pi i}{N} (k - m - r(k)N) \\ &= \eta - \frac{2\pi i s m}{N} + 2\pi i s r(k) \end{aligned}$$

for some integer $r(k)$ which depends on k , and where

$$\eta = \frac{2\pi i}{MN} \left(\left[\frac{m + \gamma + sMN}{N} \right] (m + \gamma + sMN \bmod N) - \left[\frac{\gamma + sMN}{N} \right] (\gamma + sMN \bmod N) + \frac{(\gamma + sMN)n}{N} \right).$$

Therefore

$$e^{\eta'} = e^{\eta} e^{2\pi i s m / N} e^{2\pi i r(k)} = e^{\eta} e^{-2\pi i s m / N}.$$

Now

$$\begin{aligned} |A_u(m - sMN, n + sMN)| &= \left| \frac{1}{MN^2} \sum_{k=0}^{MN^2-1} v\left(\left[\frac{m+k}{N}\right] \bmod M\right) \right. \\ &\quad \left. \times v\left(\left[\frac{k}{N}\right] \bmod M\right) e^{\eta} e^{-\frac{2\pi i s m}{N}} \right| \\ &= |e^{-\frac{2\pi i s m}{N}} A_u(m, n)| = |A_u(m, n)|. \end{aligned}$$

□

Let $K = MN^2$. We would like to be able to say that

$$\forall m, n \in \mathbb{Z}, \quad MN \nmid (m + n) \Rightarrow A_u(m, n) = 0 \quad (4.1)$$

and

$$\forall m, n, s \in \mathbb{Z}, \quad |A_u(m, n)| = |A_u(m - sN, n + sN)|. \quad (4.2)$$

The reason (4.1) and (4.2) are attractive is that they say the following. The quantity $|A_u(m, n)|$ is N -periodic as a function of n , i.e., there are at most N different graphs of $|A_u(m, n)|$. Also, for a fixed n , the values of m in which $|A_u(m, n)|$ may be non-zero are MN periodic, i.e., the non-zero points of the graph of $|A_u(m, n)|$ are separated by MN values of m . (4.1) and (4.2) do hold for a large number of CAZAC waveforms, see Fig. 7. However, this is not always the case, see Fig. 8. In fact, we have the following result.

Theorem 4.3: Let $\{u(k)\}_{k=0}^{MN^2-1}$ be a Milewski CAZAC waveform generated by an M -periodic Wiener CAZAC waveform. Then (4.1) and (4.2) are valid if M is even.

Proof: Part (4.1). Let M be even. Assume M divides $m + n$. Then, by the proof of Theorem 4.1,

$$A_u(m) = \frac{1}{MN} \sum_{\gamma=0}^{MN-1} e^{\tau}$$

where

$$\begin{aligned} \tau &= \frac{\pi i}{M} \left[\left(\left[\frac{m + \gamma}{N} \right] \bmod M \right)^2 \right. \\ &\quad \left. - \left(\left[\frac{\gamma}{N} \right] \bmod M \right)^2 + \frac{2}{N} \left[\frac{m + \gamma}{N} \right] (m + \gamma \bmod N) \right. \\ &\quad \left. - \frac{2}{N} \left[\frac{\gamma}{N} \right] (\gamma \bmod N) + \frac{2\gamma n}{N^2} \right]. \end{aligned}$$

Write each $\gamma = \nu + rN$, where $\nu = 0, \dots, N-1$ and $r = 0, \dots, M-1$. We compute (modulo $2\pi i$)

$$\begin{aligned}
\tau &= \frac{\pi i}{M} \left[\left(\left\lfloor \frac{m+\nu}{N} \right\rfloor + r \bmod M \right)^2 \right. \\
&\quad - \left. \left(\left\lfloor \frac{\nu}{N} \right\rfloor + r \bmod M \right)^2 \right. \\
&\quad + \frac{2}{N} \left(\left\lfloor \frac{m+\nu}{N} \right\rfloor + r \right) (m + \nu \bmod N) \\
&\quad - \left. \frac{2}{N} \left(\left\lfloor \frac{\nu}{N} \right\rfloor + r \right) (\nu \bmod N) + \frac{2\nu n}{N^2} + \frac{2nr}{N} \right] \\
&= \frac{\pi i}{M} \left[\left(\left\lfloor \frac{m+\nu}{N} \right\rfloor + r - c(r)M \right)^2 \right. \\
&\quad - r^2 + \frac{2}{N} \left(\left\lfloor \frac{m+\nu}{N} \right\rfloor + r \right) (m + \nu \bmod N) \\
&\quad - \left. \frac{2r\nu}{N} + \frac{2\nu n}{N^2} + \frac{2nr}{N} \right] \\
&= \frac{\pi i}{M} \left[\left(\left\lfloor \frac{m+\nu}{N} \right\rfloor + r \right)^2 \right. \\
&\quad - 2 \left(\left\lfloor \frac{m+\nu}{N} \right\rfloor + r \right) c(r)M + c^2(r)M^2 - r^2 \\
&\quad + \frac{2}{N} \left(\left\lfloor \frac{m+\nu}{N} \right\rfloor + r \right) (m + \nu \bmod N) \\
&\quad - \left. \frac{2r\nu}{N} + \frac{2\nu n}{N^2} + \frac{2nr}{N} \right] \\
&= \frac{\pi i}{M} \left[\left\lfloor \frac{m+\nu}{N} \right\rfloor^2 + 2r \left\lfloor \frac{m+\nu}{N} \right\rfloor \right. \\
&\quad + \frac{2}{N} \left(\left\lfloor \frac{m+\nu}{N} \right\rfloor + r \right) (m + \nu \bmod N) \\
&\quad - \left. \frac{2r\nu}{N} + \frac{2\nu n}{N^2} + \frac{2nr}{N} \right] \\
&= \frac{2\pi i r}{MN} \left[N \left\lfloor \frac{m+\nu}{N} \right\rfloor + (m + \nu \bmod N) \right. \\
&\quad - \left. \nu + n \right] + \alpha(m, n, \nu) \\
&= \frac{2\pi i}{M} \left(\frac{(m+n)r}{N} \right) + \alpha(m, n, \nu)
\end{aligned}$$

where $\alpha(m, n, \nu)$ is a constant independent of r and $c(r)$ whose value depends on r . If $M \nmid (m+n)$, then

$$\begin{aligned}
A_u(m, n) &= \frac{1}{MN} \sum_{\nu=0}^{N-1} e^{\alpha(m, n, \nu)} \sum_{r=0}^{M-1} e^{2\pi i \frac{m+n}{N} r/M} \\
&= \frac{1}{MN} \sum_{\nu=0}^{N-1} e^{\alpha(m, n, \nu)} \frac{e^{(2\pi i \frac{m+n}{N} / M)M} - 1}{e^{2\pi i (m+n)/M} - 1} \\
&= 0.
\end{aligned}$$

Part (4.2). If $MN \nmid (m+n)$, then we are done by (4.1) since $m - sN + l + sN = m + l$. Assume $MN \mid (m+n)$. Then, by the proof of part (4.1), we have

$$A_u(m, n) = \frac{1}{N} \sum_{\nu=0}^{N-1} e^{\lambda}$$

where

$$\begin{aligned}
\lambda &= \frac{\pi i}{M} \left[\left\lfloor \frac{m+\nu}{N} \right\rfloor^2 \right. \\
&\quad + \left. \frac{2}{N} \left\lfloor \frac{m+\nu}{N} \right\rfloor (m + \nu \bmod N) + \frac{2\nu n}{N^2} \right].
\end{aligned}$$

We calculate

$$|A_u(m - sN, n + sN)| = \left| \frac{1}{N} \sum_{\nu=0}^{N-1} e^{\lambda'} \right|$$

where

$$\begin{aligned}
\lambda' &= \frac{\pi i}{M} \left[\left\lfloor \frac{m - sN + \nu}{N} \right\rfloor^2 \right. \\
&\quad + \frac{2}{N} \left\lfloor \frac{m - sN + \nu}{N} \right\rfloor (m - sN + \nu \bmod N) \\
&\quad + \left. \frac{2\nu n + sN}{N^2} \right] \\
&= \frac{\pi i}{M} \left[\left\lfloor \frac{m+\nu}{N} \right\rfloor^2 + \frac{2}{N} \left\lfloor \frac{m+\nu}{N} \right\rfloor (m + \nu \bmod N) \right. \\
&\quad + \left. \frac{2\nu n}{N^2} - 2s \left\lfloor \frac{m+\nu}{N} \right\rfloor \right. \\
&\quad + \left. s^2 - \frac{2s}{N} (m + \nu \bmod N) + \frac{2\nu s}{N} \right] \\
&= \lambda + \frac{\pi i}{M} \left[s^2 - \frac{2s}{N} \left(N \left\lfloor \frac{m+\nu}{N} \right\rfloor \right. \right. \\
&\quad + \left. \left. (m + \nu \bmod N) \right) + \frac{2\nu s}{N} \right] \\
&= \lambda + \frac{\pi i}{M} \left[s^2 - \frac{2s(m+\nu)}{N} \right. \\
&\quad + \left. \frac{2\nu s}{N} \right] = \lambda + \frac{\pi i}{M} \left[s^2 - \frac{2sm}{N} \right].
\end{aligned}$$

Therefore, we have that

$$\begin{aligned}
|A_u(m - sN, n + sN)| &= \left| e^{\frac{\pi i}{M} (s^2 - \frac{2sm}{N})} \frac{1}{N} \sum_{\nu=0}^{N-1} e^{\lambda} \right| \\
&= |A_u(m, n)|.
\end{aligned}$$

V. VECTOR VALUED CAZAC WAVEFORMS AND FRAMES

Our results in this section rely on the following two well known facts, e.g., see [2] and [8].

Proposition 5.1: Let $\{x_{(k)}\}_{k=1}^N \subseteq \mathbb{F}^d$, with corresponding Bessel operator $L : \mathbb{F}^d \rightarrow \ell^2(\mathbb{Z}_N)$, $x \mapsto \{(x, x_{(k)})\}_{k=1}^N$. Then $\{x_{(k)}\}_{k=1}^N \subseteq \mathbb{F}^d$ is a tight frame for \mathbb{F}^d with frame constant C if and only if $L^*L = CI_d$, where I_d is the $d \times d$ identity matrix.

Proposition 5.2: Let $\{x_{(k)}\}_{k=1}^N \subseteq \mathbb{F}^d$ be a FUNTF for \mathbb{F}^d , then its frame constant is (N/d) .

It is desirable to generate tight frames which also have the properties of CAZAC waveforms. We are able to generate such sequences in \mathbb{C}^d , which, in fact, provide a new class of FUNTFs.

Theorem 5.3: Let $u = \{u(k)\}_{k=1}^N$ be a CAZAC waveform in \mathbb{C} . Define

$\forall k = 1, \dots, N$,

$$v_{(k)} = v(k) = \frac{1}{\sqrt{d}}(u(k)u(k+1)\cdots u(k+d-1)).$$

Then $v = \{v(k)\}_{k=1}^N \subseteq \mathbb{C}^d$ is a CAZAC waveform in \mathbb{C}^d and $\{v_{(k)}\}_{k=1}^N$ is a FUNTF for \mathbb{C}^d with frame constant (N/d) .

Proof: (CAZAC) Clearly

$$\begin{aligned} \|v(j)\| &= \left(\sum_{k=j}^{k+d-1} |u(k)/\sqrt{d}|^2 \right)^{1/2} \\ &= \left(\sum_{k=j}^{j+d-1} 1/d \right)^{1/2} = 1. \end{aligned}$$

Consider $A_v(m)$, where $m \not\equiv 0 \pmod N$

$$\begin{aligned} A_v(m) &= \frac{1}{N} \sum_{k=0}^{N-1} \langle v_{(m+k)}, v_{(k)} \rangle \\ &= \frac{1}{N} \sum_{k=0}^{N-1} \sum_{h=0}^{d-1} u(m+h+k) \overline{u(h+k)} \\ &= \frac{1}{N} \sum_{h=0}^{d-1} \sum_{k=0}^{N-1} u(m+h+k) \overline{u(h+k)} \\ &= \sum_{h=0}^{d-1} A_u(m) = 0. \end{aligned}$$

(FUNTF) Consider the operator L^*L , defined by the Bessel operator $L : \mathbb{C}^d \rightarrow \mathbb{C}^N$, $x \mapsto \{\langle x, x_{(k)} \rangle\}_{k=1}^N$. Using the corresponding matrix operator [Definition 1.3b)] and the definition of $v_{(k)}$, $k = 1, \dots, N$, we have the calculation shown at the bottom of the page, which depends on the periodicity of u : Thus, we invoke Proposition 5.2 to complete the proof. \square

The following result provides a method for generating non-trivial vector valued CAZAC waveforms. By nontrivial, we mean that the elements in each row do not form a CAZAC waveform themselves. This could also allow for the possibility of discovering different families of CAZAC waveforms in \mathbb{C} if the appropriate tight frame and vector valued CAZAC waveform is chosen. This is a consequence of Theorem 5.5.

Theorem 5.4: Let $\{x_{(k)}\}_{k=1}^N \subseteq \mathbb{C}^d$ be a FUNTF for \mathbb{C}^d , with frame constant C and with associated Bessel map $L : \mathbb{C}^d \rightarrow$

$\ell^2(\mathbb{Z}_N)$; and let $u = \{u(j)\}_{j=1}^M \subseteq \mathbb{C}^d$ be a CAZAC waveform in \mathbb{C}^d ($u : \mathbb{Z}_M \rightarrow \mathbb{C}^d$). Then $L(u(j)) \in \ell^2(\mathbb{Z}_N)$, $j = 1, \dots, M$, and $\{(1/\sqrt{C})L(u(j))\}_{j=1}^M \subseteq \mathbb{C}^N (= \ell^2(\mathbb{Z}_N))$ is a CAZAC waveform in \mathbb{C}^N .

Proof: Let $L_j = L(u(j)) \in \mathbb{C}^N$, $j = 1, \dots, M$ and let $L_j = (L_{j1}, L_{j2}, \dots, L_{jN})$, so that $L_{jk} = \langle u(j), x_{(k)} \rangle$.

(CA) Using the hypothesis that $\{x_{(k)}\}_{k=1}^N$ is a FUNTF, we calculate the $\ell^2(\mathbb{Z}_N)$ -norm of each $L(u(j))$, $j = 1, \dots, M$

$$\begin{aligned} \|L(u(j))\|^2 &= \|L_j\|^2 = \sum_{k=1}^N |L_{jk}|^2 \\ &= \sum_{k=1}^N |\langle u(j), x_{(k)} \rangle|^2 = C\|u(j)\|^2 = C. \end{aligned}$$

(ZAC) Also, we compute

$$\begin{aligned} A_{\frac{1}{\sqrt{C}}L \circ u}(m) &= \frac{1}{CM} \sum_{j=0}^{M-1} \langle L(u(m+j)), L(u(j)) \rangle \\ &= \frac{1}{CM} \sum_{j=0}^{M-1} \langle u(m+j), L^*L(u(j)) \rangle \\ &= \frac{C}{CM} \sum_{j=0}^{M-1} \langle u(m+j), u(j) \rangle \\ &= A_u(m) = \delta(m) \end{aligned}$$

where $L^*L = CI_d$ by Proposition 5.2 and where the last step follows by the CAZAC hypothesis on u . \square

Theorem 5.5: Let $\{x_{(k)}\}_{k=1}^N \subseteq \mathbb{C}^d$ be a FUNTF for \mathbb{C}^d , with frame constant C and with associated Bessel map $L : \mathbb{C}^d \rightarrow \ell^2(\mathbb{Z}_N)$; and let $u = \{u(j)\}_{j=1}^M \subseteq \mathbb{C}^N$ be a CAZAC waveform in \mathbb{C}^N for which $\{u(j)\}_{j=1}^M \subseteq L(\mathbb{C}^d)$. Then $L^*(u(j)) \in \ell^2(\mathbb{Z}_d)$, $j = 1, \dots, M$, and $\{(1/\sqrt{C})L^* \circ u(j)\}_{j=1}^M \subseteq \mathbb{C}^d (= \ell^2(\mathbb{Z}_d))$ is a CAZAC waveform in \mathbb{C}^d .

Proof: For each $j = 1, \dots, M$, let $u(j) = (u(j)_1, \dots, u(j)_N)$. Since $u(j) \in \text{Range}(L)$, there is $y_j \in \mathbb{C}^d$ such that $L(y_j) = u(j) \in \mathbb{C}^N$ and each $u(j)_k = \langle y_j, x_{(k)} \rangle$, $k = 1, \dots, N$. Therefore, for each $j = 1, \dots, M$

$$\begin{aligned} \|L^*(u(j))\|^2 &= \left\| \sum_{k=1}^N \langle y_j, x_{(k)} \rangle x_{(k)} \right\|^2 = \|Cy_j\|^2 \\ &= C \sum_{k=1}^N |\langle y_j, x_{(k)} \rangle|^2 = C\|u(j)\|^2 = C \end{aligned}$$

$$\begin{aligned} L^*L &= \frac{1}{d} \begin{pmatrix} u(1) & u(2) & \cdots & u(N) \\ u(2) & u(3) & \cdots & u(N+1) \\ \vdots & \vdots & \ddots & \vdots \\ u(d) & u(d+1) & \cdots & u(N+d-1) \end{pmatrix} \begin{pmatrix} \overline{u(1)} & \overline{u(2)} & \cdots & \overline{u(d)} \\ \overline{u(2)} & \overline{u(3)} & \cdots & \overline{u(d+1)} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{u(N)} & \overline{u(N+1)} & \cdots & \overline{u(N+d-1)} \end{pmatrix} \\ &= \frac{1}{d} \begin{pmatrix} NA_u(0) & NA_u(1) & \cdots & NA_u(d-1) \\ NA_u(-1) & NA_u(0) & \cdots & NA_u(d-2) \\ \vdots & \vdots & \ddots & \vdots \\ NA_u(-d+1) & NA_u(-d+2) & \cdots & NA_u(0) \end{pmatrix} = \frac{N}{d} I_d. \end{aligned}$$

where we have used the tight frame hypothesis once and the unit norm condition once.

Since $L^*L = CI_d$ on \mathbb{C}^d (Proposition 5.2), we obtain $LL^* = CI_N$ on $L(\mathbb{C}^d) \subseteq \mathbb{C}^N$ by taking $c \in L(\mathbb{C}^d)$, choosing $y_c \in \mathbb{C}^d$ for which $L(y_c) = c$, and computing $LL^*(c) = L(Cx_c) = Cc$.

We use $LL^* = CI_N$ on $L(\mathbb{C}^d)$ in the following calculation:

$$\begin{aligned} & A_{\frac{1}{\sqrt{C}}L^*o_u}(m) \\ &= \frac{1}{CM} \sum_{j=0}^{M-1} \langle L^*(u(m+j)), L^*(u(j)) \rangle \\ &= \frac{1}{CM} \sum_{j=0}^{M-1} \langle LL^*(u(m+j)), u(j) \rangle \\ &= \frac{1}{M} \sum_{j=0}^{M-1} \langle u(m+j), u(j) \rangle = \delta(m). \end{aligned}$$

VI. STATISTIC, INVERSION OF A_u , AND RMS ERROR

Propositions 6.1, 6.2, and 6.3 can be used to devise statistics to analyze Doppler [30].

Proposition 6.1: Let $u = \{u(k)\}_{k=0}^{N-1} \subseteq \mathbb{C}$ be a CAZAC waveform. Then

$$\forall n \in \mathbb{Z}, \quad \sum_{m=0}^{N-1} |A_u(m, n)|^2 = 1.$$

Proof: Fix $n \in \mathbb{Z}$. We compute

$$\begin{aligned} & \sum_{m=0}^{N-1} |A_u(m, n)|^2 \\ &= \sum_{m=0}^{N-1} \left(\frac{1}{N} \sum_{k=0}^{N-1} u(m+k) \overline{u(k)} e^{2\pi i kn/N} \right) \\ & \quad \times \overline{\left(\frac{1}{N} \sum_{j=0}^{N-1} u(m+j) \overline{u(j)} e^{2\pi i jn/N} \right)} \\ &= \frac{1}{N^2} \sum_{m=0}^{N-1} \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} u(m+k) \\ & \quad \times \overline{u(k)u(m+j)u(j)} e^{2\pi i n(k-j)/N} \\ &= \frac{1}{N^2} \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} u(j) \overline{u(k)} e^{2\pi i n(k-j)/N} \\ & \quad \times \sum_{m=0}^{N-1} u(m+k) \overline{u(m+j)} \\ &= \frac{1}{N^2} \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} u(j) \overline{u(k)} e^{2\pi i n(k-j)/N} N A_u(k-j) \\ &= \frac{1}{N^2} \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} u(j) \overline{u(k)} e^{2\pi i n(k-j)/N} N \delta(k-j) \\ &= \frac{1}{N} \sum_{k=0}^{N-1} u(k) \overline{u(k)} = 1. \end{aligned}$$

Similarly, but more simply, we can verify the following result, which does not require u to be a CAZAC waveform.

Proposition 6.2: Let $u = \{u(k)\}_{k=0}^{N-1} \subseteq \mathbb{C}$. Then

$$\forall m \in \mathbb{Z}, \quad \sum_{n=0}^{N-1} |A_u(m, n)|^2 = 1.$$

Proposition 6.3: Let $\{u(k)\}_{k=0}^{N-1} \subseteq \mathbb{C}$. Then

a)

$$\forall n \in \mathbb{Z}_N, \quad \sum_{m=0}^{N-1} A_u(m, n) = \frac{1}{N} \left(\sum_{k=0}^{N-1} u(k) \right) \overline{\hat{u}(n)}$$

b)

$$\forall m \in \mathbb{Z}_N, \quad \sum_{n=0}^{N-1} A_u(m, n) = u(m) \overline{u(0)}.$$

Proof:

a)

$$\begin{aligned} \sum_{m=0}^{N-1} A_u(m, n) &= \frac{1}{N} \sum_{m=0}^{N-1} \sum_{k=0}^{N-1} u(m+k) \overline{u(k)} e^{2\pi i kn/N} \\ &= \frac{1}{N} \sum_{k=0}^{N-1} \overline{u(k)} e^{2\pi i kn/N} \sum_{m=0}^{N-1} u(m+k) \\ &= \frac{1}{N} \sum_{k=0}^{N-1} \overline{u(k)} e^{2\pi i kn/N} \sum_{m=0}^{N-1} u(m) \\ &= \frac{1}{N} \left(\sum_{m=0}^{N-1} u(m) \right) \overline{\hat{u}(n)}. \end{aligned}$$

b)

$$\begin{aligned} \sum_{n=0}^{N-1} A_u(m, n) &= \frac{1}{N} \sum_{n=0}^{N-1} \sum_{k=0}^{N-1} u(m+k) \overline{u(k)} e^{2\pi i kn/N} \\ &= \frac{1}{N} \sum_{k=0}^{N-1} u(m+k) \overline{u(k)} \sum_{n=0}^{N-1} e^{2\pi i kn/N} \\ &= \frac{1}{N} \sum_{k=0}^{N-1} u(m+k) \overline{u(k)} N \delta(k) = u(m) \overline{u(0)}. \end{aligned}$$

□

The following result is a consequence of Proposition 6.3.

Proposition 6.4: Let $u = \{u(k)\}_{k=0}^{N-1} \subseteq \mathbb{C}$.

a) u is a ZAC waveform if and only if

$$\forall n \in \mathbb{Z}_N, \quad \left| \sum_{m=0}^{N-1} A_u(m, n) \right| = 1$$

;

b) u is a CA waveform if and only if

$$\forall m \in \mathbb{Z}_N, \quad \left| \sum_{n=0}^{N-1} A_u(m, n) \right| = 1.$$

Theorem 6.5 is clear by matrix multiplication. It is useful because it says that a signal's discrete periodic ambiguity function

□

data, which can be recorded in radar, allows us to compute the signal.

Theorem 6.5: Let $u : \mathbb{Z}_N \rightarrow \mathbb{C}^d$ and let A_u be its discrete periodic ambiguity function matrix defined in Definition 1.2. Define the $N \times N$ matrix $U = (U_{i,j})$, where $U_{i,j} = \langle u(i+j), u(j) \rangle$. Then $U = A_u D_N$.

Proposition 6.6: Let $u = \{u(k)\}_{k=0}^{N-1} \subseteq \mathbb{C}$ and let A_u be its discrete periodic ambiguity function matrix. Then u is a ZAC waveform if and only if A_u has an eigenvalue of 1 with corresponding eigenvector $[1 \ 0 \ 0 \ \dots \ 0]$.

Remark 6.7:

- 1) Let $u : \mathbb{Z}_N \rightarrow \mathbb{C}$ and consider the matrix U of Theorem 6.5. Note that $U_{k,0} = u(k)u(0)$. Hence, if we know the values of the discrete periodic ambiguity function, and, thus, the discrete periodic ambiguity function matrix A_u , then Theorem 6.5 allows us to retrieve the sequence u , which generates it, as long as $u(0) \neq 0$. In fact, if $u(0) = 1$, then $u(k) = (A_u D_N)(k, 0)$.
- 2) Theorem 6.5 establishes a bijection between $\ell^2(\mathbb{Z}_N)$ and a subset of the set of complex $N \times N$ matrices $\mathbb{C}^{N \times N}$. This allows us to convert a problem about sequences into a matrix problem. In particular, we may define an equivalence relation on $\mathbb{C}^{N \times N}$ by saying that $A \in \mathbb{C}^{N \times N}$ and $B \in \mathbb{C}^{N \times N}$ are *equivalent* if the entries of A may be obtained from B by applying a finite succession of the operations derived in Theorem 2.1 a)–e). Therefore, equivalent discrete periodic ambiguity function matrices correspond to equivalent sequences. Thus, finding the number of nonequivalent discrete periodic ambiguity function matrices will determine the number of nonequivalent sequences. In fact, by utilizing the restrictions imposed by Propositions 6.1, 6.2, 6.3, 6.4, and 6.6, this method is successful at finding all nonequivalent sequences for small values of n .
- 3) Theorem 6.5 may also be used to construct new equivalence classes of CAZAC waveforms by choosing an appropriate matrix to serve as the discrete periodic ambiguity function matrix. Note that an arbitrary matrix may not be the discrete periodic ambiguity function matrix of some CAZAC waveform, or even any complex sequence. Propositions 6.2 and 6.3 place restrictions on the structure of a matrix in order for it to be a discrete periodic ambiguity function matrix. Propositions 6.1, 6.4, and 6.6 provide analogous restrictions in the CAZAC and ZAC cases.

Example 6.8: In practice, given a sequence $u = \{u(k)\}_{k=0}^{N-1}$, a fixed $n \in \mathbb{Z}$, and the values of its discrete periodic ambiguity function $A_u(m, n)$ for all $m \in \mathbb{Z}_N$, one may wish to find n , which can be thought of as an observable quantity, e.g., related to a Doppler shift. If u is a Wiener CAZAC waveform then Corollary 3.4 allows us to calculate $n \bmod N$. If we can use several different waveforms, then the following observation allows for an alternative method for calculating $n \bmod N$.

Let $n \in \mathbb{Z}$ and let $\{\{u_j(k)\}_{k=0}^{N_j-1}\}_{j=1}^M$ be a sequence of Wiener CAZAC waveforms $u_j : \mathbb{Z}_{N_j} \rightarrow \mathbb{C}$ with mutually relatively prime lengths N_j and with corresponding discrete periodic ambiguity function values $\{\{A_{u_j}(m, n)\}_{m=0}^{N_j-1}\}_{j=1}^M$. Using Corollary 3.4 for each $j = 1, \dots, M$ we can calculate

$n \bmod N_j$. Consequently, we can use the Chinese Remainder Theorem to find $n \bmod \prod_{j=1}^M N_j$.

Let $N = \prod_{j=1}^M p_j^{a_j}$ be the prime decomposition of N . Given $n \in \mathbb{Z}$ and a Wiener CAZAC waveform $\{u(k)\}_{k=0}^{N-1}$, Corollary 3.4 allows us to calculate $n \bmod N$ using $N^2 = \prod_{j=1}^M p_j^{2a_j}$ inner product operations. Alternatively, the Chinese Remainder Theorem method allows us to calculate $n \bmod N$ using only $\sum_{j=1}^M p_j^{2a_j}$ inner product operations.

Theorem 6.9: Let $x : \mathbb{Z}_K \rightarrow \mathbb{C}$ be a ZAC waveform. Suppose $2J+1 < K = 2L+1$ and let $Z(J) = \{-J, \dots, J\}$. Consider the set BL of all waveforms $z : \mathbb{Z}_K \rightarrow \mathbb{C}$ with the property that $\text{supp}(\hat{z}) \subseteq Z(J)$. The mean-square-error (MSE), $\|z - x\|$, for $z \in BL$ has a minimum value of $(2(L - J))^{1/2}$, and this minimum value is attained by $y = x * d_J \in BL$, where $d_J = \mathbb{1}_{Z(J)}$, i.e.,

$$\forall z \in BL, \quad (2(L - J))^{1/2} = \|y - x\| \leq \|z - x\|.$$

Proof: Let $y = x * d_J$. Then $\text{supp}(\hat{y}) \subseteq Z(J)$. We compute

$$\begin{aligned} \|y - x\|^2 &= \|\hat{y} - \hat{x}\|^2 = \sum_{k=-L}^L |\hat{y}(k) - \hat{x}(k)|^2 \\ &= \sum_{J < |k| \leq L} |\hat{x}(k)|^2 \\ &\quad + \sum_{k=-J}^J (\hat{y}(k) - \hat{x}(k)) \overline{(\hat{y}(k) - \hat{x}(k))} \\ &= \sum_{J < |k| \leq L} |\hat{x}(k)|^2. \end{aligned}$$

This clearly minimizes $\|y - x\|$. Since x is a ZAC waveform, \hat{x} is a CA waveform. Hence, we have

$$\|y - x\| = \left(\sum_{J < |k| \leq L} |\hat{x}(k)|^2 \right)^{1/2} = (2(L - J))^{1/2}. \quad \square$$

ACKNOWLEDGMENT

The authors wish to thank Dr. D. Cochran and Dr. B. Saffari and the following scientists at the Norbert Wiener Center: Drs. M. Dellomo, A. Kebo, I. Konstantinidis, and J. Sieracki. Finally, they appreciate the thoughtful critique by the referees.

REFERENCES

- [1] J. J. Benedetto, J. Donatelli, and J. Ryan, *Software Package for Milewski CAZAC Code Generators and Doppler Shift Analysis* 2004 [Online]. Available: www.math.umd.edu~jjb/cazac
- [2] J. J. Benedetto and M. Fickus, "Finite normalized tight frames," *Adv. Comput. Math.*, vol. 18, pp. 357–385, 2003.
- [3] J. J. Benedetto, A. Powell, and Ö. Yilmaz, "Sigma-Delta quantization and finite frames," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 1990–2005, May 2006.
- [4] G. Björck, "Functions of modulus 1 on \mathbb{Z}_p , whose Fourier transforms have constant modulus," in *Proc. A. Haar Memorial Conf., Colloq. Math János Bolyai*, Budapest, Hungary, 1985, vol. 9, pp. 193–197.
- [5] G. Björck, *Functions of Modulus 1 on \mathbb{Z}_N Whose Fourier Transforms have Constant Modulus, and "Cyclic n-Roots"*. Norwell, MA: Kluwer, 1990, vol. 315, pp. 131–140, NATO-ASI.

- [6] G. Björck and B. Saffari, "New classes of finite unimodular sequences with unimodular transforms. Circular Hadamard matrices with complex entries," in *C.R. Acad. Sci.*, Paris, 1995, vol. 320, pp. 319–324.
- [7] P. Casazza and J. Kovačević, "Equal-norm tight frames with erasures," *Adv. Comput. Math.*, vol. 18, pp. 387–430, 2003.
- [8] O. Christensen, *An Introduction to Frames and Riesz Bases*. Boston, MA: Birkhäuser, 2003.
- [9] D. C. Chu, "Polyphase codes with good periodic correlation properties," *IEEE Trans. Inf. Theory*, vol. IT-18, pp. 531–532, 1972.
- [10] H. Chung and P. V. Kumar, "A new general construction for generalized bent functions," *IEEE Trans. Inf. Theory*, vol. 35, pp. 206–209, 1989.
- [11] J. Dillon, "Elementary Hadamard Difference Sets," Ph.D. dissertation, Univ. Maryland, College Park, 1974.
- [12] Y. Eldar and H. Bölcskei, "Geometrically uniform frames," *IEEE Trans. Inf. Theory*, vol. 49, pp. 993–1006, 2003.
- [13] Y. Eldar and G. D. Forney, "On quantum detection and the square-root measurement," *IEEE Trans. Inf. Theory*, vol. 47, pp. 858–872, 2001.
- [14] Y. Eldar and A. Oppenheim, "Quantum signal processing," in *Signal Process. Mag.*, 2002, vol. 19, pp. 12–32.
- [15] R. L. Frank, "Comments on polyphase codes with good correlation properties," *IEEE Trans. Inf. Theory*, vol. IT-19, 1973, 244.
- [16] R. L. Frank and S. A. Zadoff, "Phase shift codes with good periodic correlation properties," *IRE Trans. Inform. Theory*, vol. 8, pp. 381–382, 1962.
- [17] E. M. Gabidulin, "On classification of sequences with the perfect periodic autocorrelation functions," in *Proc. 3rd Int. Colloq. Coding Theory*, Sept. 25– Oct. 2 1990, pp. 24–30.
- [18] E. M. Gabidulin, "There are only finitely many perfect autocorrelation polyphase sequences of prime length," in *Proc. IEEE Int. Symp. Information Theory*, Trondheim, Norway, 1994, pp. 282–.
- [19] M. J. E. Golay, "Multislit spectroscopy," *J. Opt. Soc. Amer.*, vol. 39, pp. 437–444, 1949.
- [20] M. J. E. Golay, "Complementary series," *IRE Trans. Inform. Theory*, vol. 7, pp. 82–87, 1961.
- [21] S. W. Golomb, "Two-valued sequences with perfect periodic autocorrelation," *IEEE Trans. Aerosp. Electro. Syst.*, vol. 28, pp. 383–386, 1992.
- [22] V. K. Goyal, J. A. Kelner, and J. Kovačević, "Quantized frame expansions with erasures," *Appl. Comput. Harmon. Anal.*, vol. 10, pp. 203–233, 2001.
- [23] V. K. Goyal, J. Kovačević, and M. Vetterli, "Multiple description transform coding: Robustness to erasures using tight frame expansions," in *Proc. IEEE Int. Symp. Information Theory*, Cambridge, MA, 1998, 408.
- [24] J.-C. Guey and M. R. Bell, "Diversity waveform sets for delay-doppler imaging," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1504–1522, 1998.
- [25] U. Haagerup, *Orthogonal Maximal Abelian*-Subalgebras of the $n \times n$ Matrices and Cyclic n -Roots*. Odense, Denmark: Institut for Matematik, Univ. Southern Denmark, 1996, preprints no. 4.
- [26] U. Haagerup, T. Erdelyi, B. Saffari, and G. Tenenbaum, Eds., "Cyclic p -roots and bi-unimodular sequences of prime lengths," in *Topics on the Interface Between Harmonic Analysis and Number Theory*. Boston, MA: Birkhäuser, 2008, to be published.
- [27] R. C. Heimiller, "Phase shift pulse codes with good periodic correlation properties," *IRE Trans. Inform. Theory*, vol. 7, pp. 254–257, 1961.
- [28] T. Helleseth and P. V. Kumar, V. S. Pless and W. C. Huffman, Eds., "Sequences with low correlation," in *Handbook of Coding Theory*. Amsterdam, The Netherlands: Elsevier, 1998, pp. 1765–1853.
- [29] B. M. Hochwald, T. L. Marzetta, T. J. Richardson, W. Sweldens, and R. L. Urbanke, "Systematic design of unitary space-time constellations," *IEEE Trans. Inf. Theory*, vol. 46, 2000, 1962–1973.
- [30] I. Konstantinidis, A. Kebo, J. Benedetto, M. Dellomo, and J. Sieracki, "Ambiguity and sidelobe behavior of CAZAC coded waveforms," in *Proc. IEEE Radar Conf.*, Boston, MA, Apr. 17–22, 2007.
- [31] J. S. Lee and L. E. Miller, *CDMA Systems Engineering Handbook*. Norwood, MA: Artech House, 1998.
- [32] N. Levanon and E. Mozeson, *Radar Signals*. New York: Wiley-Interscience/ IEEE Press, 2004.
- [33] A. Milewski, "Periodic sequences with optimal properties for channel estimation and fast start-up equalization," *IBM J. Res. Develop.*, vol. 27, pp. 426–431, 1983.
- [34] W. H. Mow, "A new unified construction of perfect root-of-unity sequences," in *Proc. IEEE 4th Int. Symp. Spread Spectrum Techniques and Applications*, Germany, Sep. 1996, pp. 955–959.
- [35] A. Nehorai and E. Paldi, *Electromagnetic Vector-Sensor Array Processing*. Boca Raton, FL: CRC Press, 1998, pp. 65.1–65.26.
- [36] J. G. Proakis, *Digital Communications*, 4th ed. New York: McGraw-Hill, 2004.
- [37] B. Saffari, "Some polynomial extremal problems which emerged in the twentieth century," in *Twentieth Century Harmonic Analysis*. Norwell, MA: Kluwer, 2001, vol. 33, pp. 201–233, NATO-ASI.
- [38] B. Saffari, *Personal Commun.*, 2006.
- [39] B. Saffari, T. Erdelyi, B. Saffari, and G. Tenenbaum, Eds., "Bi-unimodular (CAZAC) sequences," in *Topics on the Interface Between Harmonic Analysis and Number Theory*. Boston, MA: Birkhäuser, 2008, to appear in.
- [40] B. Saffari, T. Erdelyi, B. Saffari, and G. Tenenbaum, Eds., "History of shapiro polynomials and golay complementary sequences," in *Topics on the Interface Between Harmonic Analysis and Number Theory*. Boston, MA: Birkhäuser, 2008, to appear in.
- [41] R. A. Scholtz and L. R. Welch, "Group characters: Sequences with good correlation properties," *IEEE Trans. Inform. Theory*, vol. 24, pp. 537–545, 1978.
- [42] M. R. Schroeder, "Synthesis of low-peak factor signals and binary sequences with low autocorrelation," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 85–89, 1970.
- [43] H. Shapiro, "Extremal Problems for Polynomials and Power Series," M.Sc. thesis, MIT, Cambridge, MA, 1951.
- [44] D. A. Shedd and D. V. Sarwate, "Construction of sequences with good correlation properties," *IEEE Trans. Inf. Theory*, vol. IT-25, pp. 94–97, 1979.
- [45] T. Strohmer and R. W. Heath, Jr., "Grassmanian frames with applications to coding and communication," *Appl. Comput. Harmon. Anal.*, vol. 14, pp. 257–275, 2003.
- [46] G. R. Welty, "Quaternary codes for pulsed radar," *IRE Trans. Inform. Theory*, vol. 6, pp. 400–408, 1960.
- [47] N. Wiener, "Generalized harmonic analysis," *Acta Mathematica*, vol. 55, pp. 117–258, 1930.



John J. Benedetto received the B.A. degree from Boston College, Boston, MA, in 1960, the M.A. degree from Harvard University, Cambridge, MA, in 1962, and the Ph.D. degree from the University of Toronto, Toronto, ON, Canada, in 1964, all in mathematics.

He is a Professor of Mathematics, the Director of the Norbert Wiener Center in the Department of Mathematics, a Distinguished Scholar-Teacher, and a Senior Fulbright-Hays Scholar, all at the University of Maryland, College Park. He has published 150 research papers in harmonic analysis and its applications, has directed 43 doctoral dissertations, and consulted for The MITRE Corporation from 1987 to 1996. His recent research in harmonic analysis, theoretically based in wavelets, time-frequency analysis, the uncertainty principle, and frames, has dealt with the following topics: health monitoring of jet engines, epileptic seizure prediction, sigma-delta quantization for finite frames, radar waveform design, MRI reconstruction associated with fast imaging from spectral data on spirals, (patented) auditory modelling, quantum detection, wavelet sets, and number-theoretic wavelet theory.

Dr. Benedetto is the Founding Editor-in-Chief and Executive Editor of the *Journal of Fourier Analysis and Applications*, and the Series Editor of Birkhäuser's *Applied and Numerical Harmonic Analysis* book series, as well as Associate Editor of several other journals.



J. Donatelli received the B.S. degree in mathematics (with high honors) from the University of Maryland at College Park in May 2007. He is currently working toward the Ph.D. degree in mathematics at the University of California Berkeley.

His research interests include operator algebras, harmonic analysis, and mathematical physics.