AMBIGUITY FUNCTION AND FRAME THEORETIC PROPERTIES OF PERIODIC ZERO AUTOCORRELATION WAVEFORMS

JOHN J. BENEDETTO AND JEFFREY J. DONATELLI
NORBERT WIENER CENTER
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF MARYLAND, COLLEGE PARK 20742
JJB@MATH.UMD.EDU

ABSTRACT. Constant Amplitude Zero Autocorrelation (CAZAC) waveforms u are analyzed in terms of the ambiguity function A_u. Elementary number theoretic considerations illustrate that peaks in A_u are not stable under small pertubations 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.

1. INTRODUCTION

1.1. **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 $u : \mathbb{Z}_N \to \mathbb{F}^d$, which are unimodular and have 0-autocorrelation for each $m \in \mathbb{Z}_N \setminus \{0\}$. The *autocorrelation* A_u of u is defined by

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

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

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

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

If $u : \mathbb{Z}_N \to \mathbb{F}^d$ is unimodular and has 0-autocorrelation for each $m \in \mathbb{Z}_N \setminus \{0\}$, then u is a CAZAC (*Constant Amplitude Zero Autocorrelation) waveform in* $\mathbb{F}^d$ of length N. This is 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., [42], [39], [26], [16], [9]; perfect autocorrelation or root-of-unity sequences, e.g., [33], [17], [21]; bi-unimodular sequences, e.g., [4], [5], [6], [24]; bent functions, e.g., [11], [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 [27]. Fundamental applications are to radar and communications theory, e.g., [31] and [34], [30], respectively.

In this paper we prove new results for two classes of CAZAC waveforms, which describe the behavior of their ambiguity functions. These are called the Wiener [45] and Milewski classes [32]. We also give first results on our problem of describing vector-valued CAZAC waveforms $u : \mathbb{Z}_N \to \mathbb{F}^d$, 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 [28], multiple description coding [43], [23], and quantum detection and information [12], [14], [13]. Many of the results invoke elementary number theory for their verification.

In Subsection 1.2 we give requisite definitions and in Subsection 1.3 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 [29]; $\Sigma-\Delta$ quantization for FUNTFs [3] and the potential theoretic characterization of FUNTFs [2]; and our perspective of Norbert Wiener's Generalized Harmonic Analysis [45] vis à vis recent, deep work characterizing CAZAC waveforms by Björck and Saffari [4], [5], [6], [35], [37] and Haagerup [24], [25].

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 $u : \mathbb{Z}_N \to \mathbb{H}$, 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 many modern applications. An aperiodic waveform $u : \mathbb{Z} \to \mathbb{C}$ 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-Welti codes [19], [20], [41], and [44], 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 [38] for a documentation of this history sometimes repeating itself.

1.2. **Definitions.** Gauss was able to construct CAZAC waveforms of any length N, see [6], [36]. 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

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

defines a CAZAC waveform of length N, see Theorem 3.1. Wiener [45] 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, $N = 2, 3, \ldots$. To be precise, let v be a CAZAC waveform of length M, and define the waveform

(1.2)

$$\forall k \in \mathbb{Z}_{MN^2}, \quad u(k) = u(aN+b) = v(a)e^{2\pi iab/(MN)}, k = aN+b, a = 0, \ldots, MN-1, b = 0, \ldots, N-1.$$

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 [32] 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 ambiguity function, so useful in radar. We shall define it with the following normalization.

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

$$\forall (m,n) \in \mathbb{Z}_N \times \mathbb{Z}_N,\ A_u(m,n) = \frac{1}{N} \sum_{k=0}^{N-1} < u(m+k), u(k) > e^{2\pi i k n/N}.$$

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 $j = 0$ and $\delta(0) = 1$. Further, $a \not| b$ 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 5. 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.* 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 $\mathbb{F}^d$.

b. Let $\{x_{(j)}\}_{j=1}^N \subseteq \mathbb{F}^d$. The *Bessel (analysis) operator,* $L : \mathbb{F}^d \to \ell^2(\mathbb{Z}_N)$, for $\{x_{(j)}\}_{j=1}^N$ is defined by

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

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

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

It is straightforward to calculate that

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

and

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

$G = \left(\overline{< x_{(k)}, x_{(j)} >}\right)_{k,j=1}^{N}$ 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

$$\exists\ A, B > 0 \text{ such that } \quad \forall x \in \mathbb{F}^d, \quad A||x||^2 \leq \sum_{j=1}^{N} | < x, x_{(j)} > |^2 \leq B||x||^2.$$

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 $G : L(\mathbb{F}^d) \to L(\mathbb{F}^d)$ is a bijection, and

$$\forall x \in \mathbb{F}^d, \quad x = \sum_{j=1}^{N} < x, S^{-1}x_{(j)} > x_{(j)} = \sum_{j=1}^{N} < x, x_{(j)} > S^{-1}x_{(j)} = L^*G^{-1}(L(x)).$$

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

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

We shall also use the Discrete Fourier Transform (DFT).

Definition 1.5. The $N \times N$ DFT *matrix* D_N is

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

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

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

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

1.3. **Results.** The results of Section 2 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 Figures 1–4 for Wiener waveforms, are new. The impact of these results is that even chirp-like CAZAC waveforms are not stable under small pertubations in the domain $\mathbb{Z}_N \times \mathbb{Z}_N$ of the ambiguity function. Theorems 4.1, 4.2, and 4.3, as well as the accompanying Figures 5–8, provide the

analogous more compliacted behavior of Milewski waveforms.

In Section 5 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.

Section 6 introduces several applicable techniques to characterize the structue of the 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.

2. CAZAC waveforms in $\mathbb{C}$

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

a. Rotation $\rho_a(u) = au$ by $a \in \mathbb{C},\ |a| = 1$;

b. Translation (cyclic shift) $\tau_{-j}(u)$ of $u \in \ell^2(\mathbb{Z}_N)$ by $j \in \mathbb{Z}$, defined as $\tau_{-j}(u)(k) = u(k+j)$;

c. Decimation (permutation subgroup) $\pi_j(u)$ of $u \in \ell^2(\mathbb{Z}_N)$ by $j \in \mathbb{Z}$, $(j, N) = 1$, defined as $\pi_j(u)(k) = u(jk)$;

d. Linear frequency modulation $\mu_{q,\omega}(u)$ of $u \in \ell^2(\mathbb{Z}_N)$ by $q \in \mathbb{Z}$ and any Nth root of unity ω, defined as $\mu_{q,\omega}(u)(k) = \omega^{kq}u(k)$;

e. Conjugation $\kappa(u) = \overline{u}$.

Clearly, we have

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

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

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

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

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

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 $\{kj : 0 \le k \le N-1\}$ in the case $(j, N) = 1$.

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

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

a. If $|a| = 1$, then $A_{\rho_a(u)}(m, n) = A_u(m, n)$.

b. If $j \in \mathbb{Z}$, then $A_{\tau_{-j}(u)}(m, n) = e^{-2\pi ijn/N} A_u(m, n)$.

c. 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.

d. If $q \in \mathbb{Z}$ and ω is an Nth root of unity, then $A_{\mu_{q,\omega}(u)}(m, n) = \omega^{mq} A_u(m, n)$.

e. $A_{\kappa(u)}(m, n) = \overline{A_u(m, -n)} = e^{-2\pi imn/N} A_u(-m, n) = e^{-2\pi imn/N} A_u(N - m, n)$.

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 $\mathcal{G}_N$.

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 $X_{\rho,u}$, $u \in \ell^2(\mathbb{Z}_N)$, 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 [25] 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 constant amplitude (CA). Thus, $\{u(k)\}_{k=0}^{N-1}$ is a CAZAC waveform if and only if its DFT $\hat{u}$ is a CAZAC waveform.

Proposition 2.5. Let $(N_1, N_2) = 1$ and let $u : \mathbb{Z}_{N_1} \to \mathbb{C}$ and $v : \mathbb{Z}_{N_2} \to \mathbb{C}$ be CAZAC waveforms. Then $w = uv : \mathbb{Z}_N \to \mathbb{C}$, $N = N_1 N_2$ 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. *a.* Let N be odd. Binary CAZAC waveforms $u : \mathbb{Z}_N \to \{\pm 1\}$ 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 $m \in \mathbb{Z}_N \setminus \{0\}$.

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

c. Let N be arbitrary. The only known binary CAZAC waveform $u : \mathbb{Z}_N \to \{\pm 1\}$, 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., [24]. In fact, Saffari [35], [37] was able to find all such complex binary sequences.

3. Ambiguity function analysis of Wiener CAZACs

As indicated in Subsection 1.2, 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 Mth root of unity. Define the Wiener waveform $u : \mathbb{Z}_N \to \mathbb{C}$ 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 Chapter 10 of [31]). Such waveforms go back to Frank

(1953) with signifigant subsequent contributions through the 1970s by Heimiller (1961) [26], Frank and Zadoff (1962) [16], Schroeder (1970) [40], Chu (1972) [9], and Frank (1973) [15].

Theorem 3.3. Let $j \in \mathbb{Z}$. Define $u : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{C}$ 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

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

If N is odd

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

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

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

If $jm + n \equiv 0 \bmod N$, then

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

Otherwise, we have

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

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

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

If $2jm + n \equiv 0 \bmod N$, then

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

Otherwise, we have

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

□

The ambiguity function, A_u, of a Wiener CAZAC waveform $u : \mathbb{Z}_N \to \mathbb{C}$, 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 Figures 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

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

If N is odd, then

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

Example 3.5. a. Let N be odd and let $\omega = e^{2\pi i/N}$. Then, $u(k) = \omega^{k^2}$, $0 \le k \le N-1$, 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 $2m+n \equiv 0 \bmod N$. In the case $2m+n = l_{m,n}N$ for some $l_{m,n} \in \mathbb{Z}$, we have the following phenomenon. If $0 \le m \le \frac{N-1}{2}$ and $2m+n = l_{m,n}N$ for some $l_{m,n} \in \mathbb{Z}$, then n is odd; and if $\frac{N+1}{2} \le m \le N-1$ 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 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, see Figure 3, cf., Figure 4.

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 waveform. Thus, $u(k) = \omega^{k^2}$, $0 \le k \le N-1$, and $\omega = e^{2\pi ij/M}$, $(j,M) = 1$, 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 $e^{2\pi ij/M}$ is a primitive Mth root of unity. In fact, in the case that $e^{2\pi ij/M}$ 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 Figure 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 $m \neq m_n$.

4. Ambiguity function analysis of Milewski CAZACs

The following theorem shows that for a fixed value of n, the 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 Figure 6.

Theorem 4.1. Let $\{u(k)\}_{k=1}^{MN^2}$ be a Milewski CAZAC waveform generated by a CAZAC waveform $v : \mathbb{Z}_M \to \mathbb{C}$. If $m, n \in \mathbb{Z}$ have the property that $N \not| (m + n)$, then $A_u(m, n) = 0$.

Proof. We first write A_u as follows:

$$A_u(m,n) = \frac{1}{MN^2} \sum_{k=0}^{MN^2-1} u(m+k)\overline{u(k)} e^{2\pi i k n/(MN^2)}$$

$$= \frac{1}{MN^2} \sum_{k=0}^{MN^2-1} v\left(\left\lfloor \frac{m+k}{N} \right\rfloor \bmod M\right) \overline{v\left(\left\lfloor \frac{k}{N} \right\rfloor \bmod M\right)} e^{\eta},$$

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

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

$$= \frac{1}{MN^2} \sum_{\gamma=0}^{MN-1} \sum_{s=0}^{N-1} v(\left\lfloor \frac{m+\gamma}{N} \right\rfloor \bmod M)\overline{v(\left\lfloor \frac{\gamma}{N} \right\rfloor \bmod M)} e^{\eta},$$

where

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

$$= \frac{2\pi i}{MN}\left(\left(\left\lfloor \frac{m+\gamma}{N} \right\rfloor + sM\right)(m+\gamma \bmod N) - \left(\left\lfloor \frac{\gamma}{N} \right\rfloor + sM\right)(\gamma \bmod N) = \frac{\gamma n}{N} + sMn\right)$$

$$= \frac{2\pi i}{MN}\left(\left\lfloor \frac{m+\gamma}{N} \right\rfloor (m+\gamma \bmod N) - \left\lfloor \frac{\gamma}{N} \right\rfloor (\gamma \bmod N) + \frac{\gamma n}{N} + sM\,(m+\gamma \bmod N - \gamma \bmod N + n)\right),$$

$$\beta(m,n,\gamma) = v\left(\left\lfloor \frac{m+\gamma}{N} \right\rfloor \bmod M\right)\overline{v\left(\left\lfloor \frac{\gamma}{N} \right\rfloor \bmod M\right)}e^{\delta(m,n,\gamma)},$$

and

$$\delta(m,n,\gamma) = \frac{2\pi i}{MN}\left(\left\lfloor \frac{m+\gamma}{N} \right\rfloor (m+\gamma \bmod N) - \left\lfloor \frac{\gamma}{N} \right\rfloor (\gamma \bmod N) + \frac{\gamma n}{N}\right).$$

Therefore,

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

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

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

□

The graphs of the 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 $v : \mathbb{Z}_M \to \mathbb{C}$, 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,

$$A_u(m - sMN, n + sMN) = \frac{1}{MN^2}\sum_{k=0}^{MN^2-1} u\,(m - sMN + k)\,\overline{u(k)}e^{\frac{2\pi i}{MN^2}k(n+sMN)}$$

$$= \frac{1}{MN^2}\sum_{k=0}^{MN^2-1} v\left(\left\lfloor \frac{m+k}{N} \right\rfloor \bmod M\right)\overline{v\left(\left\lfloor \frac{k}{N} \right\rfloor\right)}e^{\eta'},$$

where

$$\eta' = \frac{2\pi i}{MN}\left(\left\lfloor \frac{m - sMN + k}{N} \right\rfloor (m - sMN + k \bmod N) - \left\lfloor \frac{k}{N} \right\rfloor (k \bmod N) + \frac{k(n+sMN)}{N}\right)$$

$$= \frac{2\pi i}{MN}\left(\left(\left\lfloor \frac{m+k}{N} \right\rfloor - sM\right)(m+k \bmod N) - \left\lfloor \frac{k}{N} \right\rfloor (k \bmod N) + \frac{kn)}{N} + sMk\right)$$

$$= \frac{2\pi i}{MN}\left(\left\lfloor \frac{m+k}{N} \right\rfloor (m+k \bmod N) - \left\lfloor \frac{k}{N} \right\rfloor (k \bmod N) + \frac{kn}{N}\right) + \frac{2\pi i}{MN}\left(-sM(m+k \bmod N) + sMk\right).$$

We can write η' as

$$\eta' = \eta + \frac{2\pi i}{N}\left(k - (m + k \bmod N)\right)$$
$$= \eta + \frac{2\pi i}{N}(k - m - r(k)N) = \eta - \frac{2\pi ism}{N} + 2\pi isr(k)$$

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

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

Therefore,

$$e^{\eta'} = e^{\eta}e^{2\pi ism/N}e^{2\pi ir(k)} = e^{\eta}e^{-2\pi ism/N}.$$

Now,

$$|A_u(m - sMN, n + sMN)| = \left| \frac{1}{MN^2}\sum_{k=0}^{MN^2-1} v\left(\left\lfloor \frac{m+k}{N}\right\rfloor \bmod M\right)\overline{v\left(\left\lfloor \frac{k}{N}\right\rfloor \bmod M\right)}e^{\eta}e^{\frac{-2\pi ism}{N}}\right|$$

$$= |e^{\frac{-2\pi ism}{N}}A_u(m,n)| = |A_u(m,n)|.$$

□

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

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

and

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

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 Figure 7. However, this is not always the case, see Figure 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

$$\tau = \frac{\pi i}{M}\left[\left(\left\lfloor \frac{m+\gamma}{N}\right\rfloor \bmod M\right)^2 - \left(\left\lfloor \frac{\gamma}{N}\right\rfloor \bmod M\right)^2 + \frac{2}{N}\left\lfloor \frac{m+\gamma}{N}\right\rfloor (m+\gamma \bmod N) - \frac{2}{N}\left\lfloor \frac{\gamma}{N}\right\rfloor (\gamma \bmod N) + \frac{2\gamma n}{N^2}\right].$$

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

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

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

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

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

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

We calculate

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

where

$$\lambda' = \frac{\pi i}{M}\left[\left\lfloor\frac{m-sN+\nu}{N}\right\rfloor^2 + \frac{2}{N}\left\lfloor\frac{m-sN+\nu}{N}\right\rfloor(m-sN+\nu \bmod N) + \frac{2\nu n+sN}{N^2}\right]$$

$$= \frac{\pi i}{M}\left[\left\lfloor\frac{m+\nu}{N}\right\rfloor^2 + \frac{2}{N}\left\lfloor\frac{m+\nu}{N}\right\rfloor(m+\nu \bmod N) + \frac{2\nu n}{N^2} - 2s\left\lfloor\frac{m+\nu}{N}\right\rfloor + s^2 - \frac{2s}{N}(m+\nu \bmod N) + \frac{2\nu s}{N}\right]$$

$$= \lambda + \frac{\pi i}{M}\left[s^2 - \frac{2s}{N}\left(N\left\lfloor\frac{m+\nu}{N}\right\rfloor + (m+\nu \bmod N)\right) + \frac{2\nu s}{N}\right]$$

$$= \lambda + \frac{\pi i}{M}\left[s^2 - \frac{2s(m+\nu)}{N} + \frac{2\nu s}{N}\right] = \lambda + \frac{\pi i}{M}\left[s^2 - \frac{2sm}{N}\right].$$

Therefore, we have that

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

□

5. Vector valued CAZAC waveforms and frames

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

Proposition 5.1. Let $\{x_{(k)}\}_{k=1}^N \subseteq \mathbb{F}^d$, with corresponding Bessel operator $L : \mathbb{F}^d \to \ell^2(\mathbb{Z}_N)$, $x \mapsto \{< x, x_{(k)} >\}_{k=1}^N$. 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 $\frac{N}{d}$.

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

$$\forall\ k = 1, \ldots, N, \quad v_{(k)} = v(k) = \frac{1}{\sqrt{d}}\left(u(k)\ u(k+1)\ \ldots\ u(k+d-1)\right).$$

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 $\frac{N}{d}$.

Proof. (CAZAC) Clearly,

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

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

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

(FUNTF) Consider the operator L^*L, defined by the Bessel operator $L : \mathbb{C}^d \to \mathbb{C}^N$, $x \mapsto \{< x, x_{(k)} >\}_{k=1}^N$. Using the corresponding matrix operator (Definition 1.3b) and the definition of $v_{(k)}$, $k = 1, \ldots, N$, we have the following calculation, which depends on the periodicity of u:

$$L^*L = \frac{1}{d}\begin{pmatrix} u(1) & u(2) & \ldots & u(N) \\ u(2) & u(3) & \ldots & u(N+1) \\ \vdots & \vdots & \ddots & \vdots \\ u(d) & u(d+1) & \ldots & u(N+d-1) \end{pmatrix}\begin{pmatrix} \overline{u(1)} & \overline{u(2)} & \ldots & \overline{u(d)} \\ \overline{u(2)} & \overline{u(3)} & \ldots & \overline{u(d+1)} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{u(N)} & \overline{u(N+1)} & \ldots & \overline{u(N+d-1)} \end{pmatrix}$$

$$= \frac{1}{d}\begin{pmatrix} NA_u(0) & \overline{NA_u(1)} & \ldots & \overline{NA_u(d-1)} \\ \overline{NA_u(-1)} & NA_u(0) & \ldots & \overline{NA_u(d-2)} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{NA_u(-d+1)} & \overline{NA_u(-d+2)} & \ldots & NA_u(0) \end{pmatrix} = \frac{N}{d} I_d.$$

Thus, we invoke Proposition 5.2 to complete the proof. □

The following result provides a method for generating nontrivial 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 $L : \mathbb{C}^d \to \ell^2(\mathbb{Z}_N)$; and let $u = \{u(j)\}_{j=1}^M \subseteq \mathbb{C}^d$ be a CAZAC waveform in $\mathbb{C}^d$ ($u : \mathbb{Z}_M \to \mathbb{C}^d$). Then $L(u(j)) \in \ell^2(\mathbb{Z}_N)$, $j = 1, \ldots, M$, and $\{\frac{1}{\sqrt{C}} L(u(j))\}_{j=1}^M \subseteq \mathbb{C}^N (= \ell^2(\mathbb{Z}_N))$ is a CAZAC waveform in $\mathbb{C}^N$.

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

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

$L(u(j)),\ j = 1, \ldots, M$:

$$||L(u(j))||^2 = ||L_j||^2 = \sum_{k=1}^{N} |L_{jk}|^2 = \sum_{k=1}^{N} | < u(j), x_{(k)} > |^2 = C||u(j)||^2 = C.$$

(ZAC) Also, we compute

$$A_{\frac{1}{\sqrt{C}}L\circ u}(m) = \frac{1}{CM} \sum_{j=0}^{M-1} < L(u(m+j)), L(u(j)) >$$

$$= \frac{1}{CM} \sum_{j=0}^{M-1} < u(m+j), L^*L(u(j)) >= \frac{C}{CM} \sum_{j=0}^{M-1} < u(m+j), u(j) >$$

$$= A_u(m) = \delta(m),$$

where $L^*L = CI_d$ by Proposition 5.1 and where the last step follows by the CAZAC hypothesis on u. □

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 $L : \mathbb{C}^d \to \ell^2(\mathbb{Z}_N)$; 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 $L^*(u(j)) \in \ell^2(\mathbb{Z}_d)$, $j = 1, \ldots, M$, and $\{\frac{1}{\sqrt{C}}L^* \circ u(j)\}_{j=1}^M \subseteq \mathbb{C}^d (= \ell^2(\mathbb{Z}_d))$ is a CAZAC waveform in $\mathbb{C}^d$.

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

$$||L^*(u(j))||^2 = ||\sum_{k=1}^{N} < y_j, x_{(k)} > x_{(k)}||^2 = ||Cy_j||^2 = C\sum_{k=1}^{N} | < y_j, x_{(k)} > |^2 = C||u(j)||^2 = C,$$

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 5.1), 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.

$$A_{\frac{1}{\sqrt{C}}L^*\circ u}(m) = \frac{1}{CM} \sum_{j=0}^{M-1} < L^*(u(m+j)), L^*(u(j)) >$$

$$= \frac{1}{CM} \sum_{j=0}^{M-1} < LL^*(u(m+j)), u(j) >$$

$$= \frac{1}{M} \sum_{j=0}^{M-1} < u(m+j), u(j) >= \delta(m).$$

□

6. 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 [29].

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

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

□

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.

$$\sum_{m=0}^{N-1} A_u(m,n) = \frac{1}{N}\sum_{m=0}^{N-1}\sum_{k=0}^{N-1} u(m+k)\overline{u(k)}e^{2\pi ikn/N}$$

$$= \frac{1}{N}\sum_{k=0}^{N-1}\overline{u(k)}e^{2\pi ikn/N}\sum_{m=0}^{N-1} u(m+k) = \frac{1}{N}\sum_{k=0}^{N-1}\overline{u(k)}e^{2\pi ikn/N}\sum_{m=0}^{N-1} u(m) = \frac{1}{N}\left(\sum_{m=0}^{N-1} u(m)\right)\overline{\hat{u}(n)}.$$

b.

$$\sum_{n=0}^{N-1} A_u(m,n) = \frac{1}{N}\sum_{n=0}^{N-1}\sum_{k=0}^{N-1} u(m+k)\overline{u(k)}e^{2\pi ikn/N}$$

$$= \frac{1}{N}\sum_{k=0}^{N-1} u(m+k)\overline{u(k)}\sum_{n=0}^{N-1} e^{2\pi ikn/N} = \frac{1}{N}\sum_{k=0}^{N-1} u(m+k)\overline{u(k)}N\delta(k) = u(m)\overline{u(0)}.$$

□

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

Theorem 6.5. Let $u : \mathbb{Z}_N \to \mathbb{C}^d$ and let A_u be its ambiguity function matrix defined in Definition 1.2. Define the $N \times N$ matrix $U = (U_{i,j})$, where $U_{i,j} =< u(i+j), u(j) >$. 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 ambiguity function matrix. Then u is a ZAC waveform if and only if A_u has an eigenvalue of 1 with corresponding eigenvector $[1\ 0\ 0\ \ldots\ 0]$.

Remark 6.7. a. Let $u : \mathbb{Z}_N \to \mathbb{C}$ and consider the matrix U of Theorem 6.5. Note that $U_{k,0} = u(k)\overline{u(0)}$. Hence, if we know the values of the ambiguity function, and, thus, the 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 $u(k) = (A_u D_N)(k, 0)$.

b. 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 ambiguity function matrices correspond to equivalent sequences. Thus, finding the number of nonequivalent 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.

c. Theorem 6.5 may also be used to construct new equivalence classes of CAZAC waveforms by choosing an appropriate matrix to serve as the ambiguity function matrix. Note that an arbitrary matrix may not be the ambigutiy 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 an 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 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 mod N. If we can use several different waveforms, then the following observation allows for an alternative method for calculating n mod 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 $u_j : \mathbb{Z}_{N_j} \to \mathbb{C}$ with mutually relatively prime lengths N_j and with corresponding ambiguity function values $\{\{A_{u_j}(m, n)\}_{m=0}^{N_j-1}\}_{j=1}^{M}$. Using Corollary 3.4 for each $j = 1, \ldots, M$ we can calculate n mod N_j. Consequently, we can use the Chinese Remainder Theorem to find n mod $\prod_{j=1}^{M} N_j$.

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 mod 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 mod N using only $\sum_{j=1}^{M} p_j^{2a_j}$ inner product operations.

Theorem 6.9. Let $x : \mathbb{Z}_K \to \mathbb{C}$ be a ZAC waveform. Suppose $2J + 1 < K = 2L + 1$ and let $Z(J) = \{-J, \ldots, J\}$. Consider the set BL of all waveforms $z : \mathbb{Z}_K \to \mathbb{C}$ with the property that supp $(\hat{z}) \subseteq \mathbb{Z}(\mathrm{J})$. 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 $\hat{d}_J = \mathbb{1}_{\mathbb{Z}(J)}$, i.e.,

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

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

$$||y-x||^2 = ||\hat{y}-\hat{x}||^2 = \sum_{k=-L}^{L} |\hat{y}(k)-\hat{x}(k)|^2$$

$$= \sum_{J<|k|\leq L} |\hat{x}(k)|^2 + \sum_{k=-J}^{J} (\hat{y}(k)-\hat{x}(k))\overline{(\hat{y}(k)-\hat{x}(k))}$$

$$= \sum_{J<|k|\leq L} |\hat{x}(k)|^2.$$

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

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

□

Acknowledgements

The authors wish to thank Drs. Douglas Cochran and Bahman Saffari and the following scientists at the Norbert Wiener Center: Drs. Michael Dellomo, Andrew Kebo, Ioannis Konstantinidis, and Jeffrey Sieracki. We are also grateful for support from the University of Maryland VIGRE Grant DMS0240049 for the second named author, as well as from ONR Grant N00014-06-1-0002, AFOSR(MURI) Grant FA9550-05-1-0443, and DARPA funding under NRL Grant N00173-06-1-G006.

References

1. J. J. Benedetto, J. Donatelli, and J. Ryan, *Software package for Milewski CAZAC code generators and Doppler shift analysis*, www.math.umd.edu/˜jjb/cazac, 2004.
2. J. J. Benedetto and M. Fickus, *Finite normalized tight frames*, Adv. Comput. Math. **18** (2003), 357–385.
3. J. J. Benedetto, A. Powell, and Ö Yilmaz, *Sigma-Delta quantization and finite frames*, IEEE Trans. Inform. Theory **52** (2006), 1990–2005.
4. G. Björck, *Functions of modulus 1 on $\mathbb{Z}_p$, whose Fourier transforms have constant modulus*, Proc. of A. Haar Memorial Conference, Budapest, 1985, Colloq. Math János Bolyai (Budapest), vol. 9, 1985, pp. 193–197.
5. G. Björck, *Functions of modulus 1 on $\mathbb{Z}_N$ whose Fourier transforms have constant modulus, and "cyclic n-roots"*, vol. 315, pp. 131–140, Kluwer Academic Publishers, NATO-ASI, 1990.

6. G. Björck and B. Saffari, *New classes of finite unimodular sequences with unimodular transforms. Circular Hadamard matrices with complex entries*, C.R. Acad. Sci., Paris **320** (1995), 319–324.
7. P. Casazza and J. Kovačecić, *Equal-norm tight frames with erasures*, Adv. Comput. Math. **18** (2003), 387–430.
8. O. Christensen, *An Introduction to Frames and Riesz Bases*, Birkhäuser, Boston, 2003.
9. D. C. Chu, *Polyphase codes with good periodic correlation properties*, IEEE Trans. Inform. Theory **IT-18** (1972), 531–532.
10. H. Chung and P. V. Kumar, *A new general constuction for generalized bent functions*, IEEE Trans. Inform. Theory **35** (1989), 206–209.
11. J. Dillon, *Elementary Hadamard difference sets*, Ph.D. Thesis, University of Maryland, College Park, 1974.
12. Y. Eldar and H. Bölcskei, *Geometrically uniform frames*, IEEE Trans. Inform. Theory **49** (2003), 993–1006.
13. Y. Eldar and G .D. Forney, *On quantum detection and the square-root measurement*, IEEE Trans. Inform. Theory **47** (2001), 858–872.
14. Y. Eldar and A. Oppenheim, *Quantum signal processing*, Signal Processing Mag. **19** (2002), 12–32.
15. R. L. Frank, *Comments on polyphase codes with good correlation properties*, IEEE Trans. Inform. Theory **19** (1973), 244.
16. R. L. Frank and S. A. Zadoff, *Phase shift codes with good periodic correlation properties*, IRE Trans. Inform. Theory **8** (1962), 381–382.
17. E. M. Gabidulin, *On classification of sequences with the perfect periodic autocorrelation functions*, Proceedings of the Third International Colloquium on Coding Theory, Sept 25 - Oct 2, 1990 1991, pp. 24–30.
18. E. M. Gabidulin, *There are only finitely many perfect autocorrelation polyphase sequences of prime length*, Proc. IEEE Int. Symp. Inform. Theory (Trondheim, Norway), 1994, p. 282.
19. M. J. E. Golay, *Multislit spectroscopy*, Journal of the Optical Society of America **39** (1949), 437–444.
20. M. J. E. Golay, *Complementary series*, IRE Trans. Inform. Theory **7** (1961), 82–87.
21. S. W. Golomb, *Two-valued sequences with perfect periodic autocorrelation*, IEEE Transactions on Aerospace and Electronic Systems **28** (1992), 383–386.
22. V. K. Goyal, J. A. Kelner, and J. Kovačević, *Quantized frame expansions with erasures*, Appl. Comput. Harmon. Anal. **10** (2001), 203–233.
23. V. K. Goyal, J. Kovačević, and M. Vetterli, *Multiple description transform coding: Robustness to erasures using tight frame expansions*, Proc. IEEE Int. Symp. on Information Th. (Cambridge, MA) (1998), 408.
24. 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.
25. U. Haagerup, *Cyclic p-roots and bi-unimodular sequences of prime lengths*, to appear in Topics on the Interface between Harmonic Analysis and Number Theory (T. Erdelyi, B. Saffari, and G. Tenenbaum, eds.), Birkhäuser, Boston, 2008.
26. R. C. Heimiller, *Phase shift pulse codes with good periodic correlation properties*, IRE Trans. Inform. Theory **7** (1961), 254–257.
27. T. Helleseth and P. V. Kumar, *Sequences with low correlation*, Handbook of Coding Theory (V. S. Pless and W. C. Huffman, eds.), Elsevier, Amsterdam, 1998, pp. 1765–1853.

28. B. M. Hochwald, T. L. Marzetta, T. J. Richardson, W. Sweldens, and R. L. Urbanke, *Systematic design of unitary space-time constellations*, IEEE Trans. Inform. Theory **46** (2000), 1962 – 1973.
29. I. Konstantinidis, A. Kebo, J. Benedetto, M. Dellomo, and J. Sieracki, *Ambiguity and sidelobe behavior of CAZAC coded waveforms*, IEEE Radar Conference (Boston), 17 - 22 April, 2007.
30. J. S. Lee and L. E. Miller, *CDMA Systems Engineering Handbook*, Artech House Publications, 1998.
31. N. Levanon and E. Mozeson, *Radar Signals*, Wiley-Interscience, IEEE Press, 2004.
32. A. Milewski, *Periodic sequences with optimal properties for channel estimation and fast start-up equalization*, IBM J. Res. Develop. **27** (1983), 426–431.
33. W. H. Mow, *A new unified construction of perfect root-of-unity sequences*, Proc. IEEE 4th International Symposium on Spread Spectrum Techniques and Applications (Germany), September 1996, pp. 955–959.
34. J. G. Proakis, *Digital Communications*, 4th ed., McGraw-Hill Book Co., NY, 2004.
35. B. Saffari, *Some polynomial extremal problems which emerged in the twentieth century*, in: Twentieth Century Harmonic Analysis, vol. 33, Kluwer Academic Publishers, NATO-ASI, 2001, pp. 201–233.
36. B. Saffari, *Personal communication*, 2006.
37. B. Saffari, *Bi-unimodular (CAZAC) sequences*, to appear in Topics on the Interface between Harmonic Analysis and Number Theory (T. Erdelyi, B. Saffari, and G. Tenenbaum, eds.), Birkhäuser, Boston, 2008.
38. B. Saffari, *History of Shapiro polynomials and Golay complementary sequences*, to appear in Topics on the Interface between Harmonic Analysis and Number Theory (T. Erdelyi, B. Saffari, and G. Tenenbaum, eds.), Birkhäuser, Boston, 2008.
39. R. A. Scholtz and L. R. Welch, *Group characters: sequences with good correlation properties*, IEEE Trans. Inform. Theory **24** (1978), 537–545.
40. M. R. Schroeder, *Synthesis of low-peak factor signals and binary sequences with low autocorrelation*, IEEE Trans. Inform. Theory **16** (1970), 85–89.
41. H. Shapiro, *Extremal problems for polynomials and power series*, M.Sc. Thesis, MIT, 1951.
42. D. A. Shedd and D. V. Sarwate, *Construction of sequences with good correlation properties*, IEEE Trans. Inform. Theory **25** (1979), 94–97.
43. T. Strohmer and R.W. Heath Jr., *Grassmanian frames with applications to coding and communication*, Appl. Comput. Harmon. Anal. **14** (2003), 257–275.
44. G. R. Welti, *Quaternary codes for pulsed radar*, IRE Trans. Inform. Theory **6** (1960), 400–408.
45. N. Wiener, *Generalized harmonic analysis*, Acta Mathematica **55** (1930), 117–258.

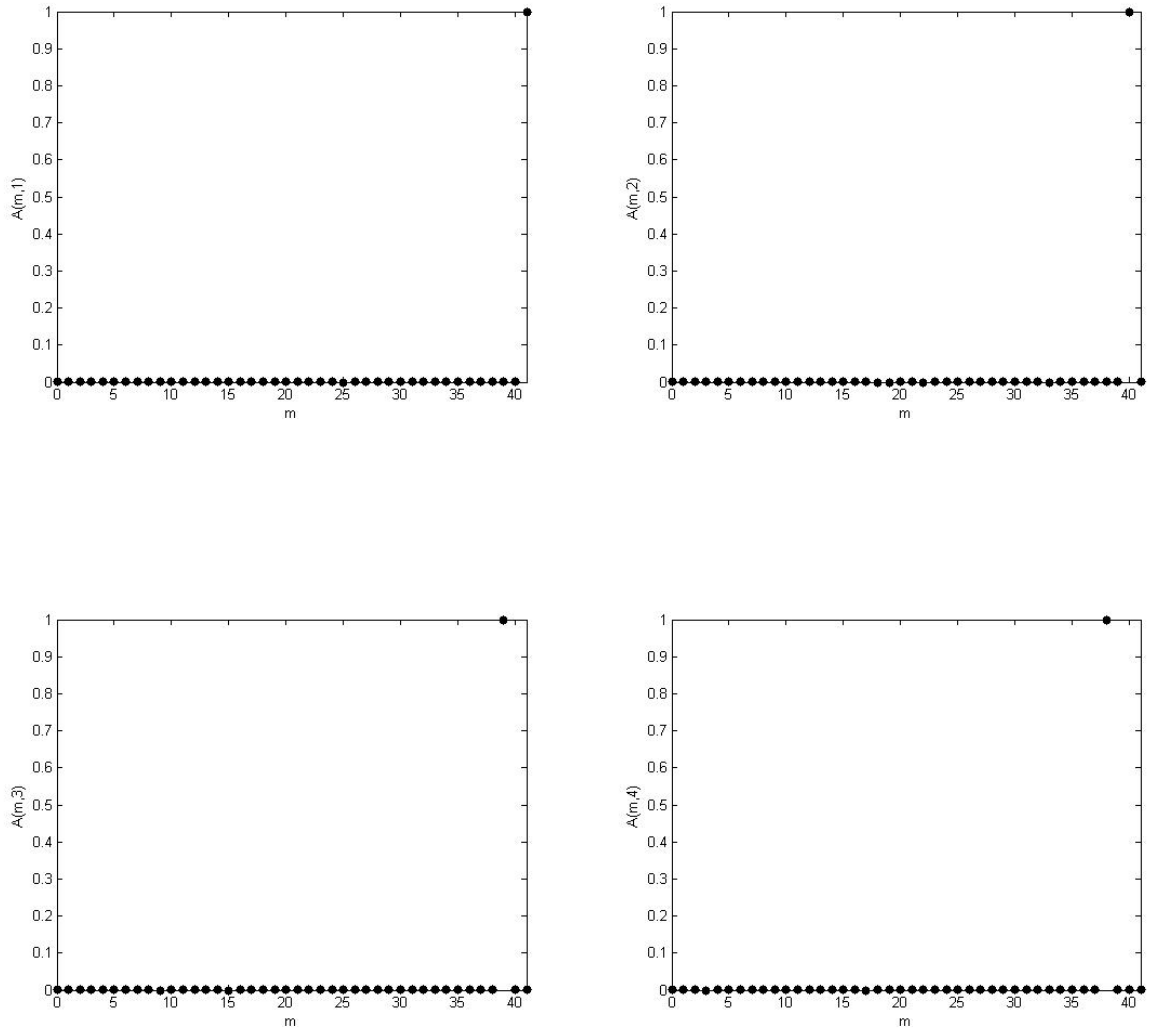

FIGURE 1. Ambiguity function modulus $|A_u(\bullet, n)|$, as a function of m, of a length 42 Wiener CAZAC waveform u evaluated at n = 1,2,3,4, where $u(k) = \omega^{k^2}$ for $\omega = e^{2\pi i/84}$.

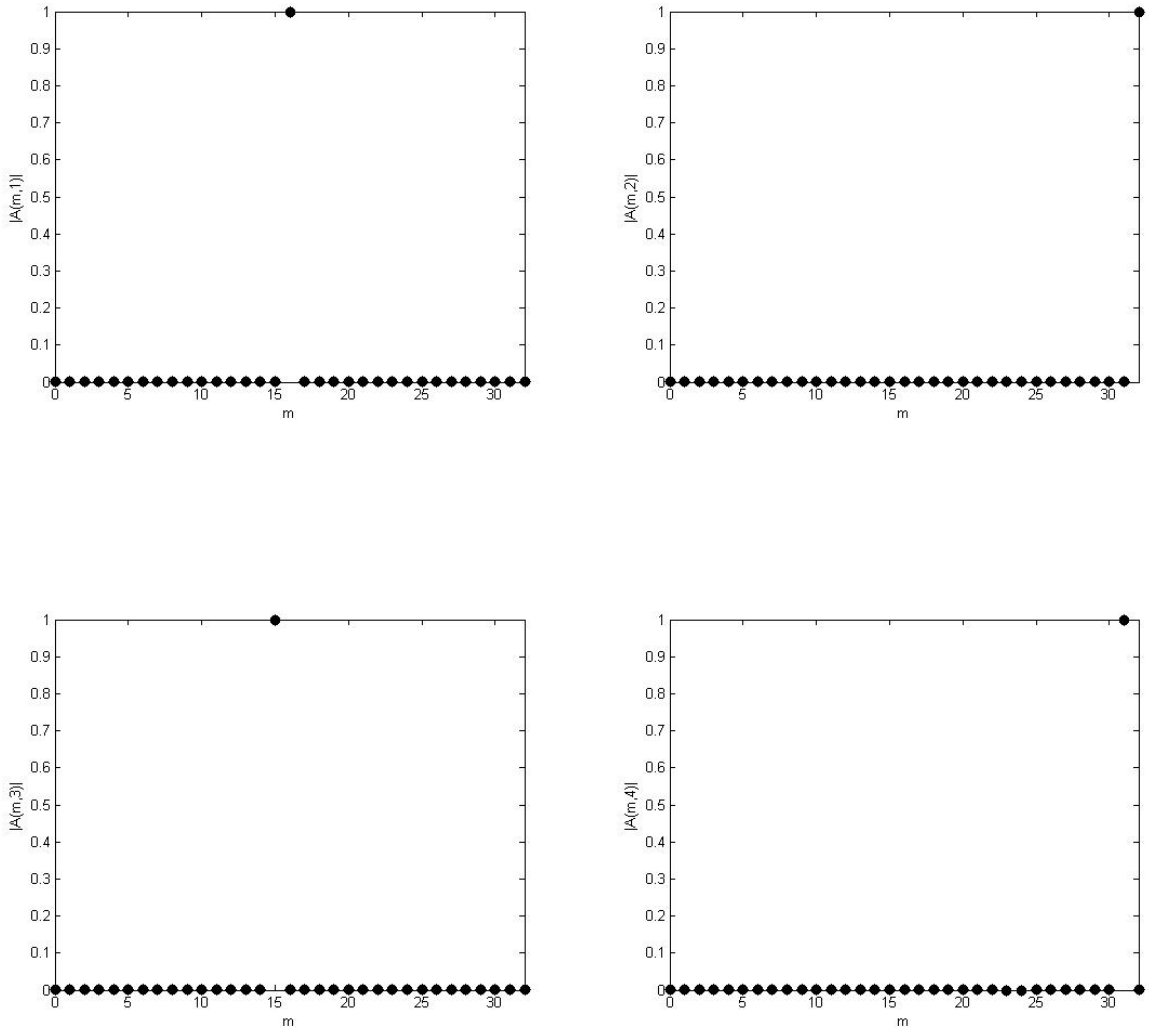

FIGURE 2. Ambiguity function modulus $|A_u(\bullet, n)|$, as a function of m, of a length 33 Wiener CAZAC waveform u evaluated at n=1,2,3,4, where $u(k) = \omega^{k^2}$ for $\omega = e^{2\pi i/33}$.

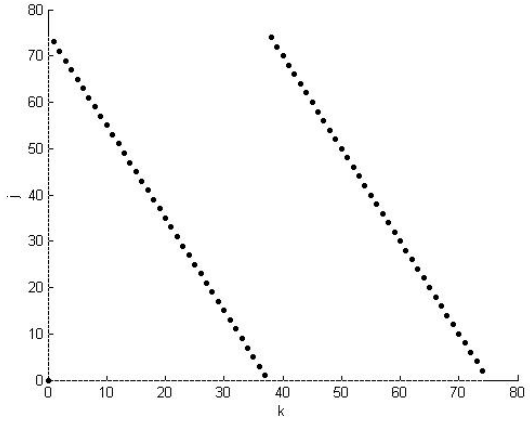

FIGURE 3. Ambiguity function domain of a length 75 Wiener CAZAC waveform u, where $|A_u(m,n)| = 1$ for a dot (m,n) and $A_u(m,n) = 0$ otherwise, and where $u(k) = \omega^{k^2}$ for $\omega = e^{2\pi i/75}$.

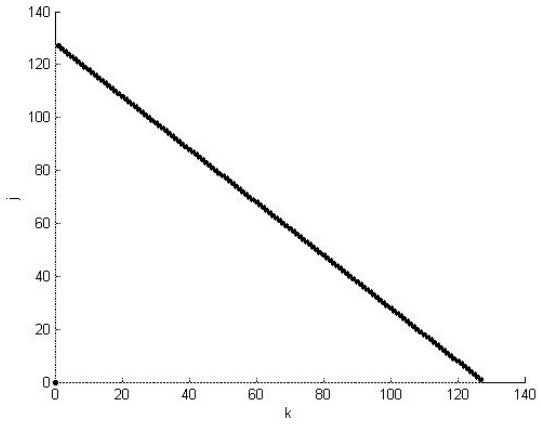

FIGURE 4. Ambiguity function domain of a length 128 Wiener CAZAC waveform u, where $|A_u(m,n)| = 1$ for a dot (m,n) and $A_u(m,n) = 0$ otherwise, and where $u(k) = \omega^{k^2}$ for $\omega = e^{2\pi i/256}$.

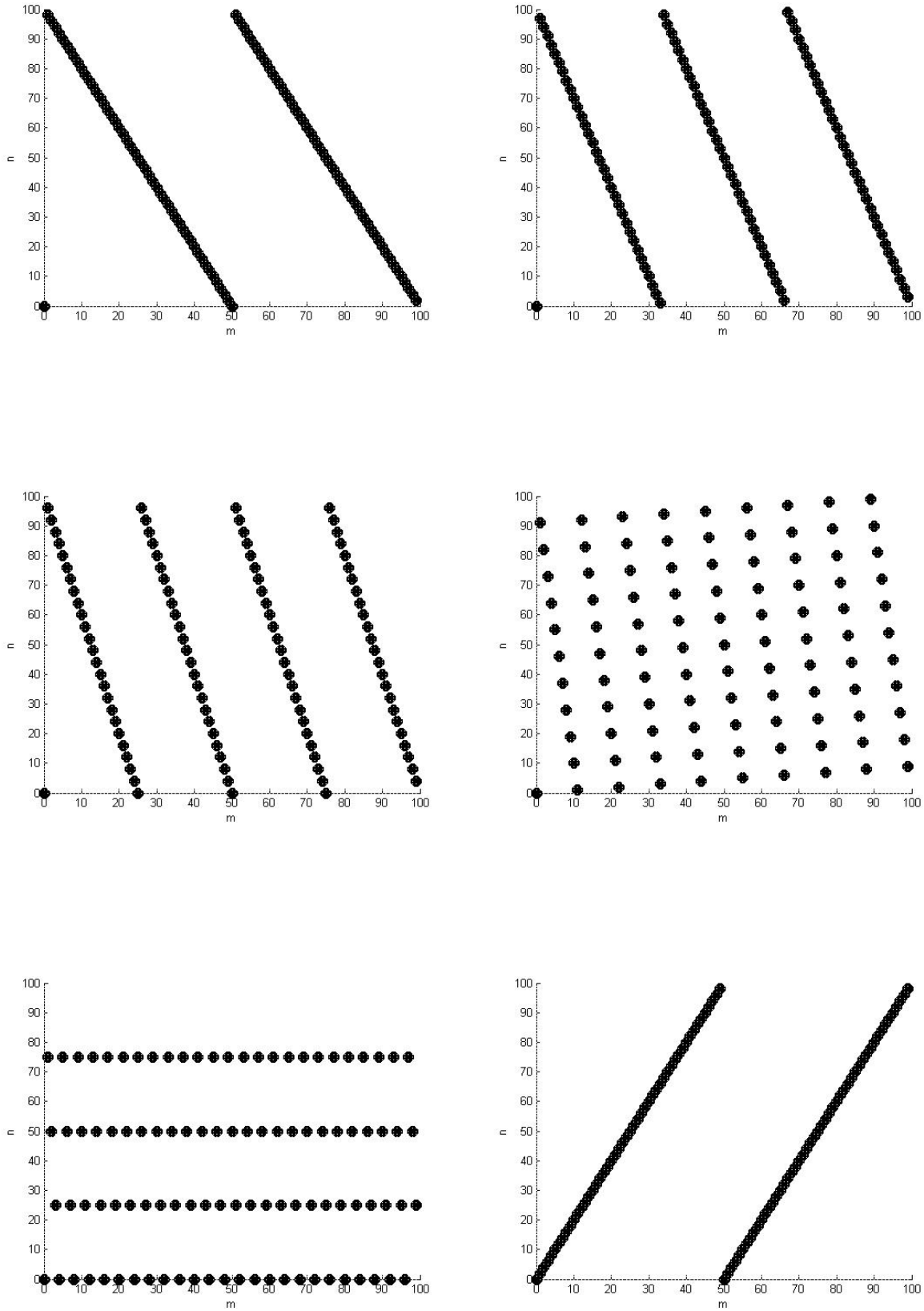

FIGURE 5. Ambiguity function domain of a length 100 Wiener CAZAC waveform u, defined in Theorem 3.3 and for j =2,3,4,9,25,98.

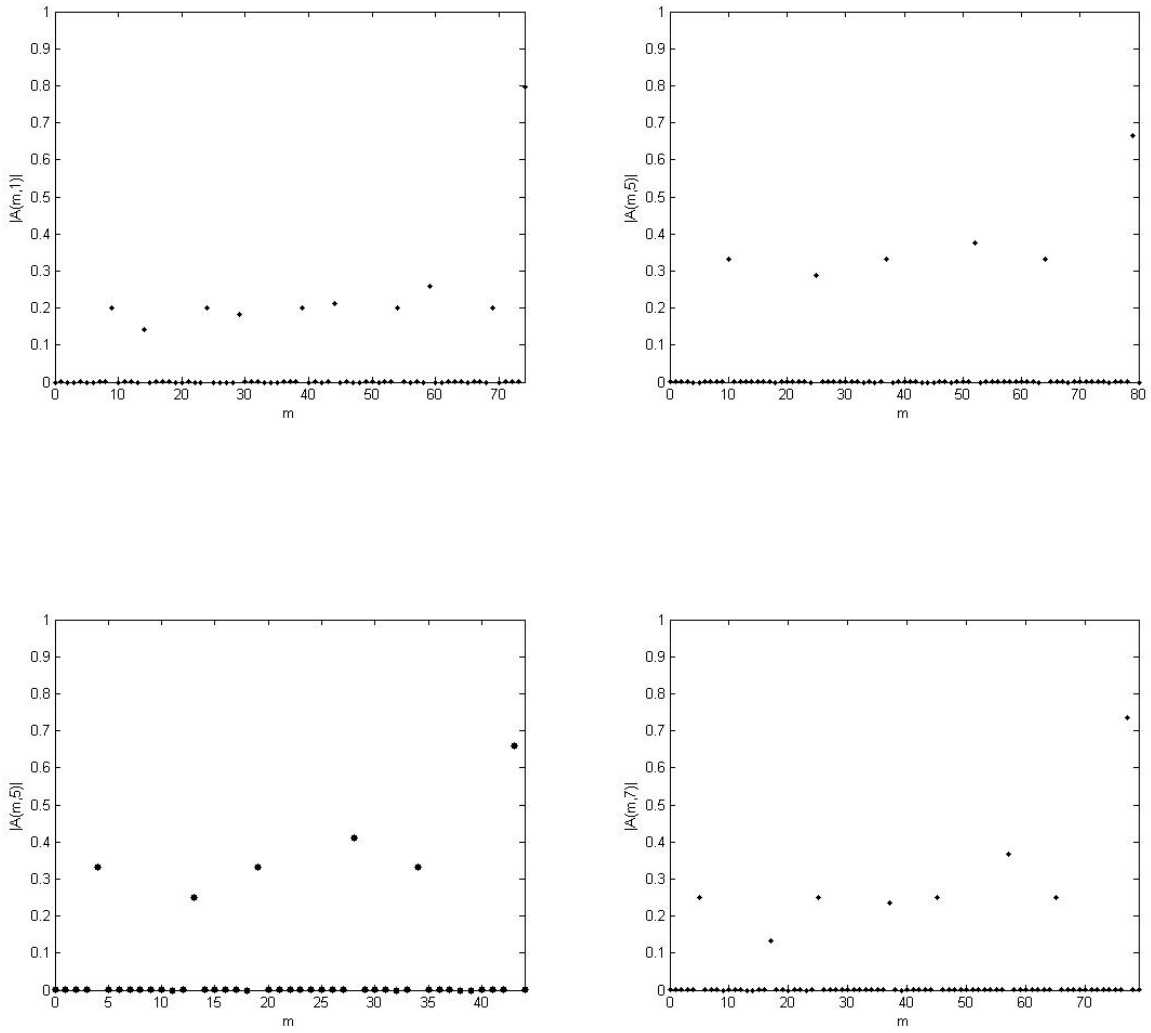

FIGURE 6. Ambiguity function modulus $|A_u(\bullet, n)|$, as a function of m, of length 3×5^2 , 9×3^2, 5×3^2, and 5×4^2 Milewski CAZAC waveforms evaluated at n =1, 5, 5, and 7, respectively.

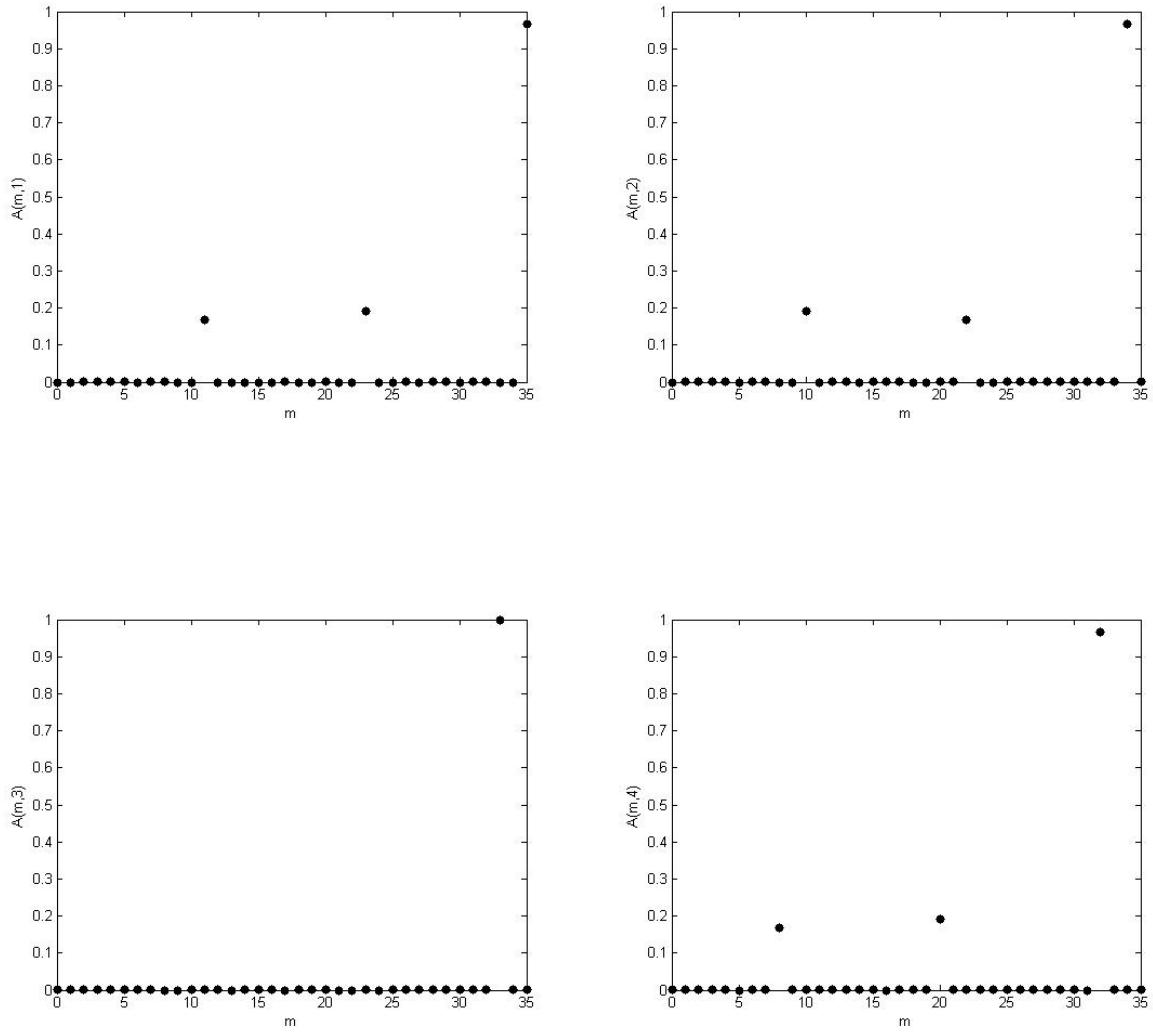

FIGURE 7. Ambiguity function modulus $|A_u(\bullet, n)|$, as a function of m, of a length 4×3^2 Milewski CAZAC waveform evaluated at $n = 1, 2, 3, 4$.

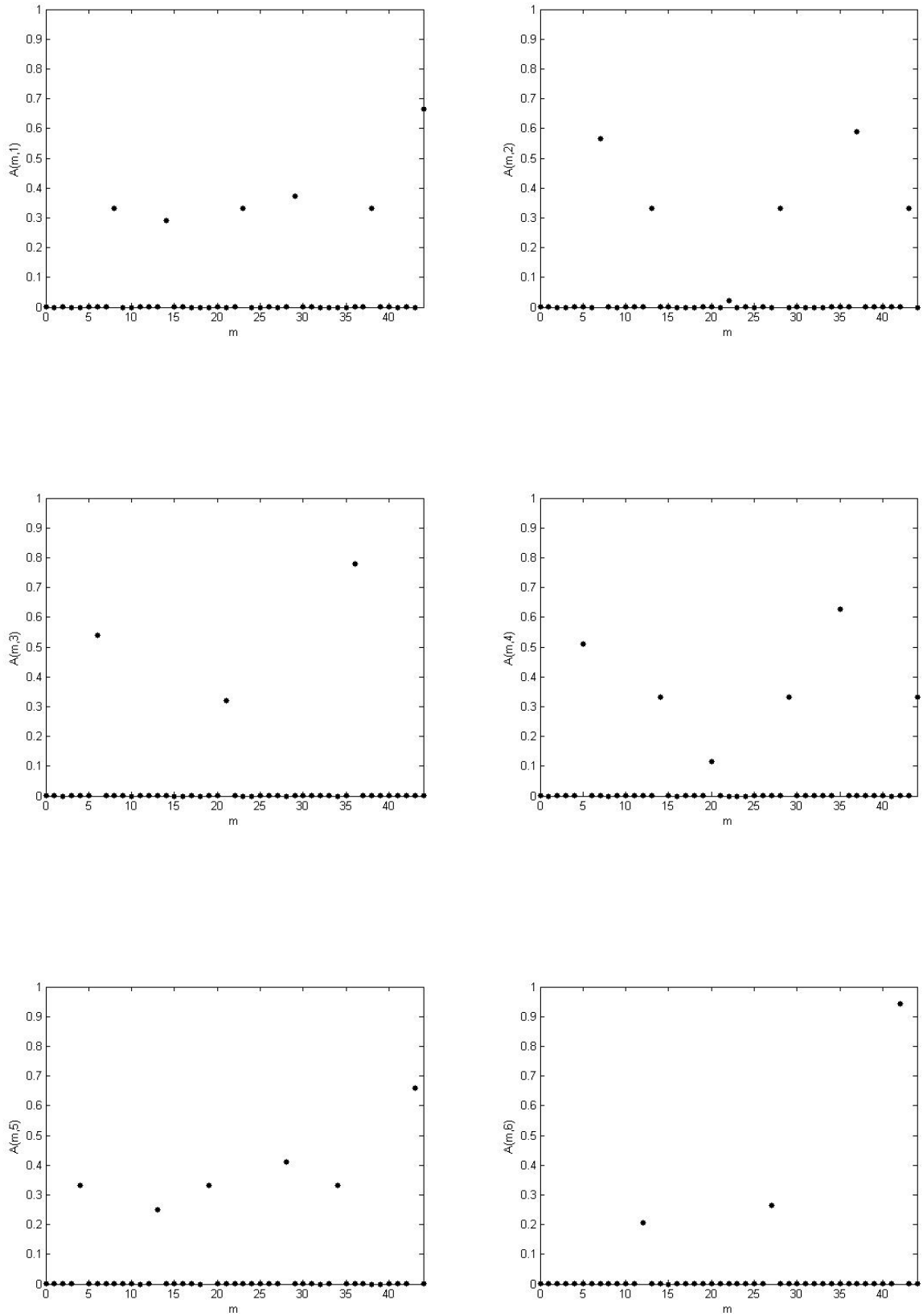

FIGURE 8. Ambiguity function modulus $|A_u(\bullet, n)|$, as a function of m, of a length $5{\times}3^2$ Milewski CAZAC waveform, generated by a length 5 Wiener CAZAC waveform and evaluated at $n = 1, 2, 3, 4, 5, 6$.