CAZAC SEQUENCES AND HAAGERUP'S CHARACTERIZATION OF CYCLIC $N-$ROOTS

JOHN J. BENEDETTO, KATHERINE CORDWELL, AND MARK MAGSINO

Abstract. Constant amplitude zero autocorrelation (CAZAC) sequences play an important role in waveform design for radar and communication theory. They also have deep and intricate connections in several topics in mathematics, including Fourier analysis, Hadamard matrices, and cyclic N-roots. Our goals are to describe these mathematical connections, to provide a unified exposition of the theory of CAZAC sequences integrating several diverse ideas, to introduce new techniques for constructing CAZAC sequences alongside established methods, and to give an exposition of the fascinating unpublished theorem of Uffe Haagerup (1949–2015), that proves that the number of CAZAC generating cyclic N-roots is finite. The role of the uncertainty principle in the proof is essential.

1. Introduction

1.1. **Background and goal.** In this subsection, we *define* a Constant Amplitude Zero Auto-Correlation (CAZAC) sequence, *describe* some scenarios where CAZAC sequences play a role, and state the *goal* of this paper.

Definition 1.1 (CAZAC sequence)**.** Given a function, $x : \mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{C}$.

a. The *auto-correlation*, $A_x : \mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{C}$, of x is defined by

$$\forall\, m \in \mathbb{Z}/N\mathbb{Z}, \quad A_x[m] = \frac{1}{N} \sum_{k=0}^{N-1} x[m+k]\, \overline{x[k]}.$$

b. The function (sequence), $x : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$, is a *Constant Amplitude Zero Auto-Correlation* (CAZAC) sequence if

$$\forall\, m \in \mathbb{Z}/N\mathbb{Z}, \quad |x[m]| = 1, \quad \text{(CA)}$$

and

$$\forall\, m \in \mathbb{Z}/N\mathbb{Z} \setminus \{0\}, \quad \frac{1}{N} \sum_{k=0}^{N-1} x[m+k]\, \overline{x[k]} = 0. \quad \text{(ZAC)}.$$

Date: March 17, 2018.

2010 *Mathematics Subject Classification.* Primary 42Bxx; Secondary 42-06, 42-02.

Key words and phrases. Cyclic $N-$roots, CAZAC (constant amplitude zero auto-correlation) sequences, uncertainty principle for $\mathbb{Z}/p\mathbb{Z}$, complex Hadamard matrices.

The first named author gratefully acknowledges the support of DTRA Grant 1-13-1-0015 and ARO Grants W911NF 15-1-0112,16-1-0008, and 17-1-0014. The second named author gratefully acknowledges the support of the Norbert Wiener Center (NWC) as a Daniel Sweet Undergraduate Research Fellow, as well as being a Banneker-Key Scholar. The third named author gratefully acknowledges the support of the NWC and the Department of Mathematics of the University of Maryland. The authors all want to give their thanks to Professor Enrico Au-Yeung of DePaul University for sharing his notes about some of this material from 2010-2012, when he was at the NWC. The first named author also gratefully acknowledges many number theoretic insights on this material by Professor Robert L. Benedetto of Amherst College.

Equation (CA) is the condition that x has constant amplitude 1. Equation (ZAC) is the condition that u has zero auto-correlation for $m \in (\mathbb{Z}/N\mathbb{Z}) \setminus \{0\}$, i.e., off the dc-component.

The construction of CAZAC sequences, or modifications where ZAC is replaced by low auto-correlation, is a central problem in the general area of waveform design; and it is particularly relevant in several applications in the areas of radar and communications.

In radar, CAZAC sequences can play a role in effective target recognition and other fundamental applications, see, e.g., [38], [39], [26], [63], [65], [21], [55], [49], [45], [1], [30], [58] [35], [46], [43], [42], [28], [51]. There has been a striking recent application of low correlation sequences to radar in terms of compressed sensing [36].

In communications, CAZAC sequences can be used to address synchronization issues in cellular access technologies, especially code division multiple access ($CDMA$), e.g., [64], [66].

The radar and communications methods have combined in recent advanced multifunction RF systems ($AMRFS$).

In radar there are two main reasons that the sequences x should have the constant amplitude property (CA). First, a transmitter can operate at peak power if x has constant peak amplitude - the system does not have to deal with the surprise of greater than expected amplitudes. Second, amplitude variations during transmission due to additive noise can be theoretically eliminated. The zero auto-correlation property (ZAC) ensures minimum interference between signals sharing the same channel.

The applications referenced above are part of a broad range of applications of the narrow band and wide band ambiguity function. The (ZAC) or low auto-correlation property can be viewed as the boundary value of an ambiguity function, which in the narrow band case is essentially the short time Fourier transform (STFT), see [69], [68], [9], [12], [6], [29]. We shall not deal with the ambiguity function in this paper.

There are also purely mathematical roots for the construction of CAZAC sequences, e.g., [9]. One example, that inspired the role of probability theory in the subject, is due to Wiener, see [7]. Our interest in CAZAC sequences was inspired by the deep ideas and techniques of Björck and Saffari, e.g., [15], [18], and [54], *and* by the good fortune of the first named author to benefit personally by discussions with both Björck and Saffari,

Our *goal* is simply stated: for various values of N, count and construct the CAZAC sequences of length N. This entails providing a unified exposition relating cyclic N-roots, complex circulant Hadamard matrices, and CAZAC sequences. We require a profound theorem due to Haagerup [32], see Subsection 1.3. His work builds on a brilliant counterexample by Björck, see Subsections 1.2 and 4.1, as well as explicit calculations by many others, e.g., [19], [13], In pursuit of our goal, we give several new explicit calculations with the point of view of constructing new CAZAC sequences.

1.2. **Gaussian and non-Gaussian CAZAC sequences.** The beautiful story of this subsection was told expertly by Saffari in [54], pages 220-222, To begin, we define the discrete Fourier transform (DFT).

Definition 1.2. *a.* Given a finite sequence, $x = (x[0], x[1], \ldots, x[N-1]) \in \mathbb{C}^N$. The *discrete Fourier transform* (DFT), $\mathcal{F}_N(x) = \widehat{x} \in \mathbb{C}^N$, of x is defined by

$$\mathcal{F}_N(x)[n] = \widehat{x}[n] = \frac{1}{N^{1/2}} \sum_{m=0}^{N-1} x[m] e^{-2\pi i m n/N}, \quad n = 0, 1, \ldots, N-1.$$

Elementary calculations yield the *inversion formula*,

$$x[m] = \frac{1}{N^{1/2}} \sum_{n=0}^{N-1} \widehat{x}[n] e^{2\pi i m n/N}, \quad m = 0, 1, \ldots, N-1, \tag{1}$$

and *Parseval's formula*,

$$\sum_{m=0}^{N-1} |x[m]|^2 = \sum_{n=0}^{N-1} |\widehat{x}[n]|^2. \tag{2}$$

b. Notationally, for a given N, let $e_m = e^{-2\pi i m/N}$ and $W_N = e^{2\pi i/N} = e_1$. Also, for a given $x \in \mathbb{C}^N$, we denote translation by τ so that $\tau_m[k] = x[k-m]$. Clearly, W_N is an N-root of unity, and recall that it is *primitive* N-root of unity if it is not also an M-root of unity for some $M < N$. Thus, W_N^M is a primitive N-root of unity if and only if $\gcd(M, N) = 1$.

c. For a given N, the DFT matrix, $\mathcal{D}_N$, is defined as the $N \times N$ matrix,

$$\mathcal{D}_N = \left[\frac{1}{N^{1/2}} W_N^{-mn} \right]_{m,n=0}^{N-1},$$

and, for convenience, assume that W_N is a primitive N-root of unity. Using Equation (2) we see that $\mathcal{D}_N$ is a unitary matrix, i.e., $\mathcal{D}_N^* \mathcal{D}_N = I$, the $N \times N$-identity matrix, where $\mathcal{D}_N^*$ is the complex conjugate of the transpose of $\mathcal{D}_N$. The trace of $\mathcal{D}_N$ is a sum of Gaussians, as defined in Example 1.3. The remarkable properties of these *Gauss sums* are stated and proved, with perspective, in [4] Chapter 3.9.

d. We have that

$$\forall x \in \mathbb{C}^N, \quad \mathcal{F}_N(x) = \widehat{x} = \mathcal{D}_N(x) \in \mathbb{C}^N,$$

see [4], [62] for much more on the DFT.

We shall say that a sequence, $x = (x[0], x[1], \ldots, x[N-1]) \in \mathbb{C}^N$, is *unimodular* if each $|x[j]| = 1$, and it is *bi-unimodular* if each $|x[m]| = |\widehat{x}[n]| = 1$. In, [15], Björck began his analysis of bi-equimodular sequence, i.e., $|x[m]| = A$ for all $m \in \mathbb{Z}/N\mathbb{Z}$ and $|\widehat{x}[n]| = B$ for all $n \in \mathbb{Z}/N\mathbb{Z}$, also see [18]. It is an interesting fact, and elementary to verify, that *a sequence, $x = (x[0], x[1], \ldots, x[N-1]) \in \mathbb{C}^N$, is bi-unimodular if and only if it is a CAZAC sequence*, see Proposition 2.1.

Example 1.3 (Gaussian sequence)**.** Given an integer $N \geq 2$, and define the *Gaussian sequence*, $g_{N,a,b}[m]$, $m = 0, \ldots, N-1$, by the formula

$$g_{N,a,b}[m] = W_N^{am^2+bm}, \ m = 0, \ldots, N-1,$$

where $a, b \in \mathbb{Z}$ and $\gcd(a, N) = 1$, that is, a and N are relatively prime, see Definition 1.2, part *b*. We write $g_N = g_{N,1,0}$.

Björck and Saffari noted, by an elementary calculation, that if $N \geq 3$ is odd, then $\{g_N[m]\}_{m=0}^{N-1} = \{e^{2\pi i m^2/N}\}_{m=0}^{N-1}$ is a CAZAC sequence, and also noted that Gauss was aware of this fact, probably in terms of the bi-unimodular equivalence! In this regard, see Example 2.5.

At Stockholm University in 1983, Per Enflo asked the following question for a given odd prime p. Is it true that the modified Gaussian sequences, $\{g_p[m]\, W_p^{jm}\}_{m=0}^{p-1}$, $j \in \mathbb{Z}$, are the only bi-unimodular sequences of length p? Gaussian sequences are the special case when $j = 0$. The answer was known to be "yes" for $p = 3$ and $p = 5$. A positive answer generally

would have helped Enflo with estimates he was making on exponential sums. Ultimately he made these estimates independent of his question, but it led to deep mathematical questions in other directions.

The $p = 3$ case is elementary to resolve. It is much more involved for the $p = 5$ case, which was first *checked* and settled by L. Lovász in 1983 (private communication to Björck), and proved by Haagerup in 1996 [31], also see Remark 1.7 and Section 3.

Björck tried to answer Enflo's question positively by computer search for $p = 7$. However, the counterexample,

$$(1, 1, 1, e^{i\theta}, 1, e^{i\theta}, e^{i\theta}), \quad \theta = \arccos\left(-\frac{3}{4}\right), \tag{3}$$

"popped out" as Björck put it!, see [54] and Section 4.

The rest is history, or, rather, the start of an important, and still unresolved and incomplete quest.

1.3. **Haagerup's theorem.** We shall now state Haagerup's theorem mentioned in Subsection 1.1. In order to do this, we shall require several notions, that are equivalent to the CAZAC sequence property. To this end, we begin by defining a cyclic N root, see [14].

Definition 1.4. A *cyclic N-root* is a solution $z = (z_0, z_1, \cdots z_{N-1}) \in \mathbb{C}^N$ to the following set of equations

$$\begin{cases} z_0 + z_1 + \cdots + z_{N-1} = 0 \\ z_0 z_1 + z_1 z_2 + \cdots + z_{N-1} z_0 = 0 \\ \qquad\qquad \cdots \\ z_0 z_1 \cdots z_{N-2} + \cdots + z_{N-1} z_0 \cdots z_{N-3} = 0 \\ z_0 z_1 \cdots z_{N-1} = 1. \end{cases}$$

The second definition we shall need to state Haagerup's theorem, and to provide basic perspective, is that of a complex circulant Hadamard matrix.

Definition 1.5. *a.* A *complex $N \times N$ circulant matrix C_N* is a square $N \times N$ matrix, where each row vector is rotated one element to the right relative to the preceding row vector. Thus, a circulant matrix, C_N, is defined by one vector, $c \in \mathbb{C}^N$, which appears as the first row of C_N. The remaining rows of C_N are each cyclic permutations of the vector c with offset equal to the row index, see [40]

A complex $N \times N$ *permutation matrix P_N* is defined by the property that it has exactly one entry of 1 in each row and each column and 0s elsewhere.

A complex $N \times N$ *unitary matrix U_N* is defined by the property that $U_N U_N^* = Id$, where U_N^* is the conjugate transpose or adjoint of U_N and Id is the $N \times N$ identity matrix. Thus, the rows and columns of U_N form orthonormal bases for $\mathbb{C}^N$.

b. An important application of circulant matrices is that they are diagonalized by the DFT. Thus, a system of N linear equations, $C_N X = Y \in \mathbb{C}^N$, can be solved quickly using the fast Fourier transform (FFT), e.g., see [22].

c. A *complex $N \times N$ Hadamard matrix H_N* is a square $N \times N$ matrix with unimodular entries $c_{m,n} \in \mathbb{C}$ and mutually orthogonal rows, i.e., $H_N H_N^* = N\, Id$.

d. Let H_1, H_2 be two Hadamard matrices. As matrices they are equivalent if they can be transformed one into the other by elementary row and column operations. In the case of

Hadamard matrices, this is the same as saying that H_1 and H_2 are *equivalent* if there exist diagonal unitary matrices D_1, D_2 and permutation matrices P_1, P_2 such that

$$H_2 = D_1 P_1 H_1 P_2 D_2. \tag{4}$$

Motivation for the definition of equivalence is spelled out for dephased Hadamard matrices in Subsection 2.5.

e. Bruzda et al. [13], [19] maintain a website that characterizes $N \times N$ Hadamard matrices for various, small values of N. Also, see [60].

There is a characterization of CAZAC sequences in terms of complex circulant Hadamard matrices [18]. In particular, the first row of any complex circulant Hadamard matrix is a CAZAC sequence. Moreover, if $x : \mathbb{Z}^N \to \mathbb{C}$ is a given function and if H_x is a circulant matrix with first row $x = (x[0], x[1], \ldots, x[N-1])$, then x is a CAZAC sequence if and only if H_x is a Hadamard matrix, see Proposition 2.2. Finally, there is a one-to-one correspondence between cyclic N-roots and CAZAC sequences of length N. This correspondence will be stated clearly in Proposition 2.4, and we shall prove Propositions 2.1, 2.2, and 2.4 in Subsection 2.1.

In [32] (2008), Haagerup proved the following deep and fundamental theorem, Theorem 1.6, cf. his earlier related work [31].

Theorem 1.6. *For every prime number p, the set of cyclic p-roots in $\mathbb{C}^p$ is finite. Moreover the number of cyclic p-roots counted with multiplicity is equal to*

$$\binom{2p-2}{p-1} = \frac{(2p-2)!}{(p-1)!^2}.$$

In particular, the number of complex $p \times p$ circulant Hadamard matrices with diagonal entries equal to 1 is less than or equal to $(2p-2)!/(p-1)!^2$.

Remark 1.7. *a.* Before Haagerup's theorem, Theorem 1.6, it was not known whether there were finitely many or infinitely many cyclic p-roots for most primes p.

b. Although elementary for $N = 2, 3, 4$, it is generally difficult to compute the number of cyclic N-roots. In fact, prior to Theorem 1.6, computer algebra, as opposed to theoretical means, was the only available technology for such computation, and in this setting N was necessarily small, see Björck and Fröberg [16] (1991), [17] (1994) for the cases, $5 \leq N \leq 8$, as well as [2] (1991).

For a given N, let

$$r(N) = \binom{2N-2}{N-1},$$

resp., $r_u(N)$, be the number of cyclic N-roots, resp., unimodular cyclic N-roots, see Table 1 which is taken from [32]. Backelin and Fröberg [2] (1991) contains the proof that $r(7) = 924$.

With this information, Faugère conjectured that for a given prime p there are $\binom{2p-2}{p-1}$ cyclic p-roots. This is the content of Theorem 1.6 when the number of cyclic p-roots is counted with multiplicity. The multiplicity is 1 for $p = 2, 3, 5, 7$, but it is not known if this is true for all primes. In the case $p = 9$, Faugère [25] showed there are cyclic 9-roots with multiplicity 4.

c. In Section 5 we shall outline Haagerup's proof that the set of cyclic $p-$roots in $\mathbb{C}^p$ is finite. Although this part of Haagerup's proof is ingenious, the real depth is involved in his proof that the number of cyclic p-roots counted with multiplicity is equal to $\frac{(2p-2)!}{(p-1)!^2}$.

TABLE 1. $r(N)$ and $r_u(N)$ for $N = 2, \ldots, 9$

N	2	3	4	5	6	7	8	9
$r(N)$	2	6	∞	70	156	924	∞	∞
$r_u(N)$	2	6	∞	20	48	532	∞	∞

1.4. **Outline.** Besides the material in Subsections 1.1, 1.2, and 1.3, the outline of what we do is as follows.

Section 2 gives the basic theory of CAZAC sequences. In Subsection 2.1 we prove the various elementary characterizations of CAZAC sequences in terms of the DFT and bi-unimodular sequences, Hadamard matrices, and cyclic N-roots. Subsection 2.2 is devoted to analyzing equivalence classes of CAZAC sequences. Then, in Subsections 2.3 and 2.4, we study cyclic p-roots and CAZAC sequences of non-square-free length, respectively. Finally, Subsection 2.5 deals with technical but useful properties of dephased Hadamard matrices. These subsections contain new techniques for computation.

Then, in Section 3, we construct all CAZAC sequences of lengths 3 and 5 in several ways, e.g., in the case $p = 3$ we use cyclic 3-roots, Hadamard matrices, and equivalence classes. In fact, for lengths 3 and 5 all CAZAC sequences are Gaussian roots of unity, and so we do not have to generalize to other roots of unity. Although technical, these cases are straightforward and solved by elementary means. However, we provide careful detail to illustrate various computation methods, that may be generalized to CAZAC sequences of larger prime lengths where not all CAZAC sequences can be explicitly listed.

In order to deal with the length 7 case, new ideas arise and this is the content of Section 4. We construct two CAZAC sequences, that are not generated by roots of unity; and, as a result, when written in Hadamard matrix form, they are not equivalent to the Fourier matrix. One of these sequences can be generalized to other prime lengths and is known as the Björck sequence, see Subsection 4.1.

In Section 5, we present part of Haagerup's theorem on counting the number of CAZAC sequences of prime length p. We write out that part of his proof which shows that the number of CAZAC sequences of prime length must be finite. His original work goes on to count them as well, and we refer the reader to his paper [32], which is available on the internet albeit unpublished. Even with the assertion of a finite number of CAZAC sequences and Haagerup's actual count, it is still not known how to construct all CAZAC sequences. One of the fascinating aspects of Haagerup's assertion of a finite number of CAZAC sequences of prime length is the natural *requirement* of Tchebotorev's theorem, re-discovered by Tao as an uncertainty principle inequality used in compressed sensing, and also re-discovered by Haagerup for this work on CAZAC sequences.

We close with Appendix 6 dealing mostly with real Hadamard matrices, but also with natural forays into topics as diverse as bent functions in coding theory, Walsh functions and wavelet packets, and the solution of the Littlewood conjecture related to crest factors in antenna theory.

2. Characterizations and properties of CAZAC sequences

2.1. Characterizations of CAZAC sequences.

Proposition 2.1. *Given a finite sequence,* $x = (x[0], x[1], \ldots, x[N-1]) \in \mathbb{C}^N \setminus \{0\}$.

a. x is a CA sequence if and only if $\widehat{x}$ is a ZAC sequence, and x is a ZAC sequence if and only if $\widehat{x}$ is a CA sequence, although the constant amplitude is not necessarily 1.

b. $x = (x[0], x[1], \ldots, x[N-1]) \in \mathbb{C}^N$ is a bi-unimodular sequence if and only if it is a CAZAC sequence.

c. x is a CAZAC sequence if and only if $\widehat{x}$ is a CAZAC sequence.

Proof. Parts b and ıc are immediate consequences of part a.

To prove part a we proceed as follows. Suppose $x \in \mathbb{C}^N$ is CA and let $n \neq 0$. Then, using the Parseval formula for the third equality, we have

$$\begin{aligned} NA_{\widehat{x}}[n] &= \sum_{k=0}^{N-1} \widehat{x}[n+k]\overline{\widehat{x}[k]} = \langle \tau_{-n}\widehat{x}, \widehat{x}\rangle = \langle e_n x, x\rangle \\ &= \sum_{k=0}^{N-1} |x[k]|^2 e^{2\pi ikn/N} = \sum_{k=0}^{N-1} e^{2\pi ikn/N} = 0, \end{aligned}$$

and so $\widehat{x}$ is ZAC.

Next, suppose that $x \in \mathbb{C}^N \setminus \{0\}$ is ZAC and let $m \neq 0$. Then,

$$0 = NA_x[m] = \sum_{k=0}^{N-1} x[m+k]\overline{x[k]} = \langle \tau_{-m}x, x\rangle = \sum_{k=0}^{N-1} |\widehat{x}[k]|^2 \, e^{2\pi imk/N}, \tag{5}$$

where the last step follows from the Parseval formula. Let $\widehat{y} = |\widehat{x}|^2$, so that by the inversion theorem, we have

$$\forall m \in \mathbb{Z}/N\mathbb{Z}, \quad y[m] = \frac{1}{N^{1/2}} \sum_{k=0}^{N-1} \widehat{y}[k] \, e^{2\pi imk/N}.$$

Thus, because of (5), we know that $y[m] = 0$ for $m \in \mathbb{Z}/N\mathbb{Z} \setminus \{0\}$, and so

$$\forall n \in \mathbb{Z}/N\mathbb{Z}, \quad \widehat{y}[n] = \frac{1}{N^{1/2}} \, y[0]$$

by the definition of the DFT. Hence, by the definition of $\widehat{y}$, $\widehat{x}$ is constant on $\mathbb{Z}/N\mathbb{Z}$, although not necessarily taking the value 1.

The converse directions in each case are proved by replacing x with $\widehat{x}$. □

Proposition 2.2. *Given a sequence $x : \mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{C}$, and let C_N be a complex circulant matrix with first row $x = (x[0], \cdots, x[N-1])$. Then, $x = \{x[0], \ldots, x[N-1]\}$ is a CAZAC sequence, where each $x[j] = x_j$, if and only if C_N is a Hadamard matrix.*

Proof. First, we show that if $x = (x_0, \cdots, x_{N-1})$ is the first row of a complex $N \times N$ circulant Hadamard matrix H, then x is a CAZAC sequence, $\{x[0], \ldots, x[N-1]\}$, where each $x[m] = x_m$. Because H is a Hadamard matrix, each entry has norm 1, so x satisfies the CA condition defining CAZAC sequences. Next, because H is circulant, H has the form

$$\begin{bmatrix} x_0 & x_1 & \cdots & x_{N-1} \\ x_1 & x_2 & \cdots & x_0 \\ & & \ddots & \\ x_{N-1} & x_0 & \cdots & x_{N-2} \end{bmatrix}.$$

Now, as noted in Definition 1.5, the orthogonality property of Hadamard matrices implies that $HH^* = NId$. In particular, this means that the inner product of x with column i of H is zero, where $2 \leq i \leq n$. Note that column i is of the form $x_i, x_{i+1}, \cdots, x_{i+(N-1)}$ where subscripts are taken modulo N. So the ith column is a rotation of x, and, taken together, columns $2, \ldots, N$ comprise all the nonidentity rotations of x. So, the inner product of x with any nonidentity rotation of x is 0, and thus x satisfies the zero auto-correlation property of CAZAC sequences. Hence, $x = \{x[0], \ldots, x[N-1]\}$ is a CAZAC sequence.

Conversely, we show that if $x = \{x[0], \ldots, x[N-1]\}$ is a CAZAC sequence, then $x = (x[0], \cdots, x[N-1])$ is the first row of a complex circulant Hadamard matrix $H = C_N$, of the form

$$\begin{bmatrix} x_0 & x_1 & \cdots & x_{N-1} \\ x_1 & x_2 & \cdots & x_0 \\ & & \ddots & \\ x_{N-1} & x_0 & \cdots & x_{n-2} \end{bmatrix}.$$

Now, because x is a CAZAC sequence, the absolute value of each x_i is 1. Thus, H satisfies the unimodular condition of complex Hadamard matrices.

Next, choose any row $(x_i, x_{i+1}, \cdots, x_{i+(N-1)})$ of H, where we consider subscripts mod N. Then, when we take the inner product of $(x_i, x_{i+1}, \cdots, x_{i+(N-1)})$ with itself, we obtain $x_i\overline{x_i} + x_{i+1}\overline{x_{i+1}} + \cdots + x_{N-1}\overline{x_{N-1}} = 1+1+\cdots+1 = N$, since the absolute value of each x_i is 1. If we take any other row, $(x_j, x_{j+1}, \ldots, x_{j+(N-1)})$, of H, where $i \neq j$, then the inner product $\langle (x_i, x_{i+1}, \ldots, x_{i+(N-1)}), (x_j, x_{j+1}, \ldots, x_{j+(N-1)}) \rangle$ is zero because x has zero auto-correlation. This implies that

$$HH^* = \begin{bmatrix} x_0 & x_1 & \cdots & x_{N-1} \\ x_1 & x_2 & \cdots & x_0 \\ & & \ddots & \\ x_{N-1} & x_0 & \cdots & x_{N-2} \end{bmatrix} \begin{bmatrix} \overline{x_0} & \overline{x_1} & \cdots & \overline{x_{N-1}} \\ \overline{x_1} & \overline{x_2} & \cdots & \overline{x_0} \\ & & \ddots & \\ \overline{x_{N-1}} & \overline{x_0} & \cdots & \overline{x_{N-2}} \end{bmatrix} = NId,$$

where Id is the identity matrix. Thus, H satisfies the orthogonality property of complex Hadamard matrices, and hence $H = C_N$ is a complex circulant Hadamard matrix. □

First, the proofs of Propositions 2.1 and 2.2 should be compared with those in [8]. Further, due to the characterization of CAZAC sequences in Proposition 2.2, there is a basic relation between vector-valued CAZAC sequences and finite unit norm tight frames (FUNTFs) X for $\mathbb{C}^d$. In order to state this relation, we shall say that $x : \mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{C}^d$ is a CAZAC sequence in $\mathbb{C}^d$ if each $\|x[k]\| = 1$ and

$$\forall\, k = 1, \ldots, N-1, \quad \frac{1}{N} \sum_{m=0}^{N-1} \langle x[m+k]x[m] \rangle = 0.$$

Here, $x[m] = (x_1[m], \ldots, x_d[m])$, where $x_j[m] \in \mathbb{C}$, $m \in \mathbb{Z}/N\mathbb{Z}$, and $j = 1, \ldots, d$; and the inner product is

$$\langle x[k]x[m] \rangle = \sum_{j=1}^{d} x_j[k]\, \overline{x_j[m]}.$$

Also, recall that $X = \{x_n\}_{n=0}^{N-1} \subseteq \mathbb{C}^d$ is a FUNTF if $\text{span}X = \mathbb{C}^d$ and each $\|x_n\| = 1$. This definition does not reflect the complexity of frames even in the finite FUNTF case, e.g., see [20], but it is sufficient to state Proposition 2.3, see [9] for its proof.

Proposition 2.3. *Let $x = \{x[n]\}_{n=0}^{N-1}$ be a CAZAC sequence in $\mathbb{C}$. Define*

$$\forall\, k = 0, \dots, N-1, \quad v[k] = \frac{1}{\sqrt{d}}\left(x[k], x[k+1], \dots, x[k+d-1]\right).$$

Then, $v = \{v[k]\}_{k=0}^{N-1}$ is a CAZAC sequence in $\mathbb{C}^d$ and $v = \{v[k]\}_{k=0}^{N-1}$ is a FUNTF for $\mathbb{C}^d$ with frame constant N/d.

The following fundamental result was proved by Björck in 1985 [14].

Proposition 2.4. *There is a one-to-one correspondence between unimodular cyclic N-roots and CAZAC sequences of length N and with first term $x[0] = 1$. In fact, given such a CAZAC sequence, x, we can obtain the corresponding cyclic N-root with the formula*

$$(z_0, z_1, \cdots, z_{N-1}) = \left(\frac{x[1]}{x[0]}, \frac{x[2]}{x[1]}, \cdots, \frac{x[N-1]}{x[N-2]}, \frac{x[0]}{x[N-1]}\right).$$

Proof. First, we show that if $x = (x_0, \cdots, x_{N-1})$ is a CAZAC sequence with $x_0 = 1$, then $(z_0, \dots, z_{N-1}) = (x_1/x_0, x_2/x_1, \cdots, x_0/x_{N-1}) = (x_1, x_2/x_1, \cdots, x_0/x_{N-1})$ is a unimodular cyclic N-root. First note that that $|z_i| = x_1/x_0 \cdot \overline{x_1/x_0} = x_1/x_0 \cdot x_0/x_1 = 1$ for all i, so $(z_0, \dots, z_{N-1})$ is unimodular.

Next, multiplying $z_0 \cdots z_{N-1}$ gives

$$\frac{x_1}{x_0} \cdot \frac{x_2}{x_1} \cdots \frac{x_0}{x_{N-1}} = \frac{x_1 \cdot \cdots \cdot x_{N-1} \cdot x_0}{x_0 \cdot x_1 \cdots x_{N-1}} = 1,$$

because all numerators and denominators cancel out.

Because each x_i is a unimodular complex number, we can write $x_i = e^{i\theta}$ for some θ. Then, $\overline{x_i} = e^{-i\theta} = 1/x_i$. Now, adding $z_0 + \cdots + z_{N-1}$ gives

$$\frac{x_1}{x_0} + \frac{x_2}{x_1} \cdots + \frac{x_0}{x_{N-1}} = x_1\overline{x_0} + x_2\overline{x_1} + \cdots + x_0\overline{x_{N-1}} = \langle (x_1, x_2, \cdots, x_0), (x_0, x_1, \dots, x_{N-1}) \rangle = 0$$

since $(x_0, \dots, x_N)$ is a CAZAC sequence and thus satisfies the zero auto-correlation property.

Next, taking $z_0z_1 + z_1z_2 + \cdots + z_{N-1}x_0$ gives

$$\begin{aligned} &\frac{x_1}{x_0} \cdot \frac{x_2}{x_1} + \cdots + \frac{x_{N-1}}{x_{N-2}}\frac{x_0}{x_{N-1}} + \frac{x_0}{x_{N-1}}\frac{x_1}{x_0} \\ &= x_2\overline{x_0} + x_3\overline{x_1} + \cdots + x_0\overline{x_{N-2}} + x_1\overline{x_{N-1}} \\ &= \langle (x_2, x_3, \cdots, x_1), (x_0, x_1, \dots, x_{N-1}) \rangle, \end{aligned}$$

which is 0 by the zero auto-correlation of $(x_0, \dots, x_N)$.

In general, if we take $z_0z_1 \cdots z_i + z_1 \cdots z_{i+1} + \cdots + z_N \cdot z_0 \cdots z_{i-1}$, where $0 \le i \le N-1$, we get

$$\begin{aligned} &\frac{x_1}{x_0} \cdot \frac{x_2}{x_1} \cdots \frac{x_i}{x_{i-1}} + \cdots + \frac{x_{N-1}}{x_{N-2}}\frac{x_0}{x_{N-1}} \cdots \frac{x_{i-2}}{x_{i-3}} + \frac{x_0}{x_{N-1}}\frac{x_1}{x_0} \cdots \frac{x_{i-1}}{x_{i-2}} \\ &= x_i\overline{x_0} + x_{i+1}\overline{x_1} + \cdots + x_{i-2}\overline{x_{N-2}} + x_{i-1}\overline{x_{N-1}} \\ &= \langle (x_i, x_{i+1}, \cdots, x_{i-1}), (x_0, x_1, \dots, x_{N-1}) \rangle, \end{aligned}$$

which is 0 by the zero auto-correlation of $(x_0, \dots, x_N)$.

Thus, we see that $(z_0, \dots, z_{N-1})$ is a cyclic unimodular N-root, as desired.

Now, we show that if $(z_0, \dots, z_{N-1})$ is a cyclic N-root where $x_0 = 1$, then if we recursively define $x_0 = 1$, $x_k = x_{k-1}z_{k-1}$, then we get a CAZAC sequence. (Note that this forces $z_{k-1} = x_k/x_{k-1}$, as before.)

Certainly $|x_0| = 1$. Assume inductively that $|x_{k-1}| = 1$. Then $|x_k| = |x_{k-1}||z_{k-1}| = |z_{k-1}| = 1$ because $(z_0, \ldots, z_{N-1})$ is unimodular.

Also, we can compute

$$\langle (x_0, \ldots, x_{N-1}), (x_i, \ldots, x_{i+(N-1)}) \rangle = x_0\overline{x_i} + \cdots + x_{N-1}\overline{x_{i+(N-1)}} = \frac{x_0}{x_i} + \cdots + \frac{x_{N-1}}{x_{i+(N-1)}},$$

and we have already seen that this is $z_0 z_1 \cdots z_i + z_1 \cdots z_{i+1} + \cdots + z_N \cdot z_0 \cdots z_{i-1}$, which we know to be 0 because $(z_0, \ldots, z_{N-1})$ is a cyclic N-root. □

Example 2.5. We state the following modest extensions of the Gaussian CAZAC sequence example of Example 1.3.

a. Given an integer $N \geq 2$.

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

and let W_M be a primitive M-root of unity. Then, $\{W_M^{m^2}\}_{m=0}^{N-1}$ is a CAZAC sequence of length N. We refer to $\{W_M^{m^2}\}_{m=0}^{N-1}$ as the *Wiener sequence*, see [9] and Subsection 3.4.

b. Given an odd integer $N \geq 3$. Then, $\{g_{N,a,b}[m]\}_{m=0}^{N-1}$ is a CAZAC sequence.

c. Generally, for any CAZAC sequence of length N, we can construct a sequence of length N^2 in a systematic way. The construction is due to Milewski, see [9].

2.2. **Equivalence classes of CAZAC sequences.** There are several meaningful ways of defining equivalence classes on CAZAC sequences. We shall employ the following elementary definition. Two CAZAC sequences, x and y, on $\mathbb{Z}/N\mathbb{Z}$, are *equivalent* if $x = cy$ for some $|c| = 1$, e.g., see Haagerup [32]. Do there exist only finitely many non-equivalent CAZAC sequences in $\mathbb{Z}/N\mathbb{Z}$? The answer to this question is "yes" for N prime and "no" for $N = MK^2$, see, e.g., [9], [54]. For the case of non-prime square-free N, special cases are known, and there are published arguments asserting general results.

Another definition of equivalence, that was developed in [9], is the following. Two CAZAC sequences, x and y, on $\mathbb{Z}/N\mathbb{Z}$, are defined to be *5-operation equivalent* if they can be obtained from one another by means of compositions of the five operations: rotation, translation, decimation, linear frequency modulation, and conjugation. These *5-equivalence operations* for CAZAC sequences are defined as follows for all $k \in \mathbb{Z}/N\mathbb{Z}$:

(1) (Rotation) $y[k] = cx[k]$, for some $|c| = 1$.
(2) (Translation) $y[k] = x[k - m]$, for some $m \in \mathbb{Z}/N\mathbb{Z}$.
(3) (Decimation) $y[k] = x[mk]$, for some $m \in \mathbb{Z}/N\mathbb{Z}$ for which $\gcd(m, N) = 1$.
(4) (Linear Frequency Modulation) $y[k] = W_N^k x[k]$.
(5) (Conjugation) $y[k] = \overline{x[k]}$.

Example 2.6 (Equivalence relations between CAZAC sequences and cyclic roots)**.** Suppose two CAZAC sequences, x and y, defined on $\mathbb{Z}/N\mathbb{Z}$ have associated cyclic N-roots $\{z_k\}$ and $\{w_k\}$. It is straightforward to verify the following relations (stated for all $k \in \mathbb{Z}/N\mathbb{Z}$) between the 5-equivalence operations for CAZAC sequences, and how they become relations between cyclic N-roots.

(1) $y[k] = cx[k] \Longrightarrow w_k = z_k$.
(2) $y[k] = x[k - m] \Longrightarrow w_k = z_{k-m}$.
(3) $y[k] = x[mk] \Longrightarrow w_k = \prod_{j=mk+1}^{mk+m} z_j$.

(4) $y[k] = W_N^k x[k] \Longrightarrow w_k = W_N z_k$.
(5) $y[k] = \overline{x[k]} \Longrightarrow w_k = \overline{z_k}$.

In particular, the 5-equivalence operations for CAZAC sequences give rise to operations under which cyclic N-roots are closed.

Thus, CAZAC sequences that are equivalent are also 5-operation equivalent. However, generally, CAZAC sequences that are 5-operation equivalent are not equivalent. This is significant because the numbers in Table 1 refer to the number of equivalent CAZAC sequences.

In practice, two CAZAC sequences, x and y, are not equivalent if $x[0] = y[0] = 1$, but $x[k] \neq y[k]$ for some $k > 0$. It is clearly more difficult to check if two CAZAC sequences are 5-operation equivalent than if they are equivalent.

Additionally, there are questions about how these two notions of equivalence among CAZAC sequences relate to equivalence classes of the corresponding Hadamard matrices. It is not true that CAZAC sequences from two equivalent Hadamard matrices will be equivalent in the sense of the 5-equivalence operations.

2.3. **Cyclic p-roots.** In order to address the problem of finding all cyclic p-roots computationally, where p is prime, we developed a Python script which checks every permutation of the p-roots of unity by brute force, and tried to see if and when they are cyclic p-roots. Based on this script, we were led to formulate the following result. The result itself, along with a combinatorial argument, leads to all 20 cyclic 5-roots with modulus 1, see Subsection 3.5.

Proposition 2.7. *Let p be an odd prime, and recall that $W_p = e^{2\pi i/p}$. If $s \in \{1, \cdots, p-1\}$ and $r \in \{1, \cdots, p\}$, then $(W_p^r, W_p^{r+s}, W_p^{r+2s}, \cdots, W_p^{r+(p-1)s})$ is a cyclic p-root.*

Proof. Given any cyclic p-root we can obtain another cyclic p-root by multiplying by W_p^r. In particular, we can assume without loss of generality that $r = 0$. Fix $s \in \{0, \cdots, p-1\}$. The t-th equation ($0 \leq t < p$) in the cyclic p-root system can be written as

$$\sum_{k=0}^{p-1} \prod_{\ell=0}^{t-1} x_{k+\ell} = 0$$

so we would like to verify that

$$\sum_{k=0}^{p-1} \prod_{\ell=0}^{t-1} W_p^{s(k+\ell)} = 0. \tag{6}$$

To this end, we compute directly and obtain

$$\sum_{k=0}^{p-1} \prod_{\ell=0}^{t-1} W_p^{s(k+\ell)} = \sum_{k=0}^{p-1} W_p^{skt} \prod_{\ell=0}^{t-1} W_p^{s\ell} = \sum_{k=1}^{p-1} W_p^{skt} W_p^{s\sum_{\ell=0}^{t-1}\ell} = \sum_{k=1}^{p-1} W_p^{skt} W_p^{st(t-1)/2}$$

$$= W_p^{st(t-1)/2} \sum_{k=1}^{p-1} W_p^{skt} = 0,$$

since W_p^{st} is a primitive p-root of unity. For the last (p-th) equation we want to show

$$\prod_{k=0}^{p-1} W_p^{sk} = 1. \tag{7}$$

To verify this, we once again compute directly, and obtain

$$\prod_{k=0}^{p-1} W_p^{sk} = W_p^{s\sum_{k=0}^{p-1} k} = W_p^{sp(p-1)/2} = e^{s(p-1)\pi i} = 1,$$

since p is odd. Combining Equations (6) and (7) gives us that $(1, W_p^s, \cdots, W_p^{(p-1)s})$ is a cyclic p-root. □

Corollary 2.8. *The number of cyclic p-roots that are comprised of p-roots of unity is bounded below by $p(p-1)$.*

Proof. Each cylcic p-root in Proposition 2.7 is comprised of roots of unity. There are two parameters: s and r. Note that s can take up to $p-1$ different values, and r can take up to p different values. Thus, the number of possible cyclic p-roots that can be formed by Proposition 2.7 is $p(p-1)$. This gives us the desired lower bound. □

In particular, as a consequence of Corollary 2.8, all 20 cyclic 5-roots with modulus 1 are generated by Proposition 2.7. It is natural to speculate that all cyclic p-roots are given by Proposition 2.7, and that the lower bound $p(p-1)$ of Corollary 2.8 is the exact number of cyclic p-roots that are comprised of p-roots of unity.

2.4. **CAZAC sequences of non-square-free length.** Much of the following material is found in [18], but has been recorded here for completeness.

Theorem 2.9. *Let $c \in \mathbb{C}^N$ be any constant amplitude sequence of length $N \geq 2$, and let σ be any permutation of the set $\{0, 1, \cdots, N-1\}$. Define a new sequence, $x \in \mathbb{C}^{N^2}$, by the formula,*

$$\forall a, b \in \{0, 1, \cdots, N-1\}, \quad x[aN+b] = c[b]e^{2\pi i a\sigma(b)/N}.$$

Then, x is a CAZAC sequence of length N^2.

Proof. Without loss of generality, assume $|c[i]| = 1$ for all $i = 0, 1, \ldots, N-1$. The sequence, x, is CA by its definition. We shall prove that x is also ZAC by verifying that $\widehat{x}$ is CA. Let $W_{N^2} = e^{2\pi i/N^2}$. Then,

$$|\widehat{x}[j]| = \left|\sum_{k=0}^{N^2-1} x[k]W_{N^2}^{-kj}\right| = \left|\sum_{a=0}^{N-1}\sum_{b=0}^{N-1} x[aN+b]W_{N^2}^{-(aN+b)j}\right|$$

$$= \left|\sum_{a=0}^{N-1}\sum_{b=0}^{N-1} c[b]W_{N^2}^{Na\sigma(b)}W_{N^2}^{-aNj}W_{N^2}^{-bj}\right| = \left|\sum_{b=0}^{N-1} c[b]W_{N^2}^{-bj}\sum_{a=0}^{N-1} W_{N^2}^{Na\sigma(b)}W_{N^2}^{-aNj}\right|$$

$$= \left|\sum_{b=0}^{N-1} c[b]W_{N^2}^{-bj}\sum_{a=0}^{N-1} W_{N^2}^{N(\sigma(b)-j)a}\right|. \tag{8}$$

Note that the inner sum of (8) is 0 unless $\sigma(b) \equiv j \bmod N$, in which case the inner sum is N. Thus, we can rewrite (8), taking j modulo N if necessary, as

$$|\widehat{x}[j]| = \left|\sum_{b=0}^{N-1} c[b]W_{N^2}^{-bj}\sum_{a=0}^{N-1} W_{N^2}^{N(\sigma(b)-j)a}\right| = |Nc[\sigma^{-1}(j)W_{N^2}^{-\sigma^{-1}(j)j}| = N.$$

□

Corollary 2.10. *Given an integer $N \geq 2$. There are infinitely many non-equivalent CAZAC sequences of length N^2 whose first term is 1.*

We now wish to extend Theorem 2.9 to arbitrary sequences whose length is not square free.

Theorem 2.11. *Let $Q \geq 2$ be an integer, let N^2 be the largest square dividing Q, let σ be any permutation of $\{0, 1, \cdots, N-1\}$, and consider the primitive M-root W_M, where $M = Q/N$. If $c \in \mathbb{C}^N$ is a constant amplitude sequence of length N, then define a new sequence, $x \in \mathbb{C}^Q$, by the formula,*

$$\forall a \in \{0, \cdots, M-1\} \text{ and } \forall b \in \{0, \cdots, N-1\}, \quad x[aN+b] = c[b]W_M^{a\sigma(b)+Na(a-1)/2}.$$

If at least one of N and $M-1$ is even, then x is a CAZAC sequence of length Q.

Proof. Without loss of generality, assume $|c[i]| = 1$ for every $i \in \{0, \cdots, N-1\}$. First, we note that x can be extended to an Q-periodic function on all of $\mathbb{Z}$. Indeed, if we let $k \in \mathbb{C}^Q$ be written as $k = aN + b$, then

$$\frac{x[Q+k]}{x[k]} = \frac{x[(M+a)N+b]}{x[aN+b]} = \frac{c[b]W_M^{(M+a)\sigma(b)+N(M+a)(M+a-1)/2}}{c[b]W_M^{a\sigma(b)+Na(a-1)/2}}$$

$$= \frac{W_M^{M\sigma(b)}W_M^{a\sigma(b)}W_M^{N(M^2+2Ma-M)}W_M^{Na(a-1)/2}}{W_M^{a\sigma(b)}W_M^{Na(a-1)/2}}$$

$$= W_M^{M\sigma(b)}W_M^{NM(2a+(M-1))/2} = 1,$$

since both terms are an M-th root of unity raised to a power which is an integer multiple of M.

Using this, we can directly compute the auto-correlation of x at $u = rN + s$, where $r \in \{0, \cdots, M-1\}$ and $s \in \{0, \cdots, N-1\}$ and at least one of r and s is nonzero, i.e., $u \neq 0$. Let $k = aN + b$ and $\theta = \lfloor \frac{b+s}{N} \rfloor$. Then,

$$A_x[u] = \sum_{k=0}^{Q-1} x[k+u]\overline{x[k]} = \sum_{a=0}^{M-1}\sum_{b=0}^{N-1} x[(a+r+\theta)N + (b+s)]\overline{x[aN+b]}$$

$$= \sum_{a=0}^{M-1}\sum_{b=0}^{N-1} c[b+s]W_M^{(a+r+\theta)\sigma(b+s)+N(a+r+\theta)(a+r+\theta-1)/2}\overline{c[b]}W_M^{-a\sigma(b)-Na(a-1)/2}$$

$$= C_r\sum_{b=0}^{N-1} c[b+s]\overline{c[b]}W_M^{\frac{N\theta(2r+\theta-1)}{2}+(r+\theta)\sigma(b+s)}\sum_{a=0}^{M-1} W_M^{a(\sigma(b+s)-\sigma(b)+N(r+\theta))}, \tag{9}$$

where $C_r = W_M^{N(r^2-r)/2}$. If $s = 0$, then $\theta = 0$ for every $b \in \{0, \cdots, N-1\}$, and we can write (9) as

$$C_r\sum_{b=0}^{N-1} |c[b]|^2 W_M^{r\sigma(b)}\sum_{a=0}^{M-1} W_M^{aNr} = C_r\sum_{a=0}^{M-1}\sum_{b=0}^{N-1} W_M^{r(\sigma(b)+aN)}. \tag{10}$$

Since σ is a permutation of $\{0, \cdots, N-1\}$, we can make a substitution $q = \sigma(b)$ and reorder as necessary to rewrite (10) as

$$C_r \sum_{a=0}^{M-1} \sum_{q=0}^{N-1} W_M^{r(aN+q)} = C_r \sum_{k=0}^{Q-1} W_M^{rk} = 0,$$

since $r \neq 0 \bmod N$. If $s \neq 0$, then in the inner sum of (9) we observe that $0 < |\sigma(b+s) - \sigma(b)| < N$, and thus N does not divide $(\sigma(b+s) - \sigma(b) + N(r+\theta))$ for any fixed b. It then follows that M does not divide $(\sigma(b+s) - \sigma(b) + N(r+\theta))$ for any fixed b and the inner sum is 0 for every b. Thus, if $s \neq 0$ then (9) is 0 as well. □

Corollary 2.12. *Given an integer $Q \geq 2$, that is not square-free. There are infinitely many non-equivalent CAZAC sequences of length Q whose first term is 1.*

Proof. Take $c[0] = 1$. Let N^2 be the largest square dividing Q and $M = Q/N$. If either N is even or M is odd, then Theorem 2.11 applies immediately and the sequence given in Theorem 2.11 gives us infinitely many CAZAC sequences. If N is odd and M is even, then Q has exactly one factor of 2. Thus, we can write $M = 2M'$ with M' odd. In Theorem 2.11, replace Q by $Q/2$ and M with M', and let y be the resulting CAZAC sequence of length $Q/2$. We can then construct a CAZAC sequence of length Q by taking the Kronecker product $z \otimes y$ of $z = (1, i) \in \mathbb{C}^2$ by $y \in \mathbb{C}^{Q/2}$, so that

$$z \otimes y = \left(y[0], y[1], \ldots, y\left[\frac{Q}{2} - 1\right], i\, y[0], i\, y[1], \ldots, i\, y\left[\frac{Q}{2} - 1\right] \right).$$

□

2.5. **Dephased Hadamard matrices.** One property that follows from the definition of equivalence classes of complex Hadamard matrices is that every complex Hadamard matrix is equivalent to a unique *dephased* Hadamard matrix, i.e., a Hadamard matrix with a first row and first column of 1s.

The website [19] maintained by Bruzda et al. states the following construction of this dephased form.

Proposition 2.13. [19] *Given an $N \times N$ complex Hadamard matrix,*

$$H = \begin{bmatrix} h_{0,0} & h_{0,1} & \cdots & h_{0,N-1} \\ h_{1,0} & h_{1,1} & \cdots & h_{1,N-1} \\ \vdots & \vdots & \ddots & \vdots \\ h_{N-1,0} & h_{N-1,1} & \cdots & h_{N-1,N-1} \end{bmatrix}.$$

The equivalent dephased form is

(11)

$$D_1 H D_2 = \begin{bmatrix} \overline{h}_{0,0} & 0 & \cdots & 0 \\ 0 & \overline{h}_{1,0} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \overline{h}_{N-1,0} \end{bmatrix} \begin{bmatrix} h_{0,0} & h_{0,1} & \cdots & h_{0,N-1} \\ h_{1,0} & h_{1,1} & \cdots & h_{1,N-1} \\ \vdots & \vdots & \ddots & \vdots \\ h_{N-1,0} & h_{N-1,1} & \cdots & h_{N-1,N-1} \end{bmatrix} \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & h_{0,0}\overline{h}_{0,1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h_{0,0}\overline{h}_{0,N-1} \end{bmatrix}.$$

Moreover, the equivalent dephased form is unique.

Proof. We compute the matrix product in Equation (11). In the first step, we have

$$D_1HD_2 = \begin{bmatrix} \overline{h}_{0,0}h_{0,0} & \overline{h}_{0,0}h_{0,1} & \cdots & \overline{h}_{0,0}h_{0,N-1} \\ \overline{h}_{1,0}h_{1,0} & \overline{h}_{1,0}h_{1,1} & \cdots & \overline{h}_{1,0}h_{1,N-1} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{h}_{N-1,0}h_{N-1,0} & \overline{h}_{N-1,0}h_{N-1,1} & \cdots & \overline{h}_{N-1,0}h_{N-1,N-1} \end{bmatrix} \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & h_{0,0}\overline{h}_{0,1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h_{0,0}\overline{h}_{0,N-1} \end{bmatrix},$$

from which we obtain

$$D_1HD_2 = \begin{bmatrix} \overline{h}_{0,0}h_{0,0} & \overline{h}_{0,0}h_{0,0}h_{0,1}\overline{h}_{0,1} & \cdots & h_{0,0}\overline{h}_{0,0}h_{0,N-1}\overline{h}_{0,N-1} \\ \overline{h}_{1,0}h_{1,0} & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ \overline{h}_{N-1,0}h_{N-1,0} & * & \cdots & * \end{bmatrix}.$$

We now verify that D_1HD_2 is a Hadamard matrix. First, because each h_{ij} has norm 1, and by norm multiplicativity, we see that each entry of D_1HD_2 has norm 1. Next, note that $(D_1HD_2)(D_1HD_2)^* = D_1HD_2D_2^*H^*D_1^*$. Because D_1 and D_2 are unitary matrices, we have $D_2D_2^* = I$ and $D_1D_1^* = I$; and because H is a Hadamard matrix, $HH^* = N\,Id$. Thus, we obtain $D_1HD_2D_2^*H^*D_1^* = ND_1ID_1^* = N\,Id$.

This matrix is dephased because the i^{th} entry of the first column is of the form $\overline{h}_{i,0}h_{i,0} = 1$ for $0 \leq i \leq N-1$ and the i^{th} entry of the first row, for $1 \leq i \leq N-1$, is of the form $h_{0,0}\overline{h}_{0,0}h_{0,i}\overline{h}_{0,i} = 1$.

Next, assume that there are $a_0, \ldots, a_{N-1}$, $b_0, \ldots, b_{N-1}$ such that $|a_i| = |b_i| = 1$ for $0 \leq i \leq N-1$ and

$$\begin{bmatrix} a_0 & 0 & \cdots & 0 \\ 0 & a_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{N-1} \end{bmatrix} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 1 & * & \cdots & * \end{bmatrix} \begin{bmatrix} b_0 & 0 & \cdots & 0 \\ 0 & b_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_{N-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 1 & * & \cdots & * \end{bmatrix}. \tag{12}$$

Calculating the left side of (12), we have

$$\begin{bmatrix} a_0 & a_0 & \cdots & a_0 \\ a_1 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ a_{N-1} & * & \cdots & * \end{bmatrix} \begin{bmatrix} b_0 & 0 & \cdots & 0 \\ 0 & b_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_{N-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 1 & * & \cdots & * \end{bmatrix},$$

and so we obtain

$$\begin{bmatrix} a_0b_0 & a_0b_1 & \cdots & a_0b_{N-1} \\ a_1b_0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ a_{N-1}b_0 & * & \cdots & * \end{bmatrix} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 1 & * & \cdots & * \end{bmatrix}.$$

From this, we find $a_0 = \cdots = a_{N-1} = b_0^{-1}$ and $b_0 = \cdots = b_{N-1} = a_0^{-1}$. Say $a_0 = x$ and $b_0 = x^{-1}$. Then, Equation (12) becomes

$$\begin{bmatrix} x & 0 & \cdots & 0 \\ 0 & x & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & x \end{bmatrix} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 1 & * & \cdots & * \end{bmatrix} \begin{bmatrix} x^{-1} & 0 & \cdots & 0 \\ 0 & x^{-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & x^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 1 & * & \cdots & * \end{bmatrix},$$

or

$$xx^{-1} \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 1 & * & \cdots & * \end{bmatrix} \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 1 & * & \cdots & * \end{bmatrix},$$

and, thus, we have

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 1 & * & \cdots & * \end{bmatrix} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 1 & * & \cdots & * \end{bmatrix}.$$

Therefore, the equivalent dephased form is unique. □

3. Roots of unity CAZAC sequences of prime length

3.1. **Introduction.** All CAZAC sequences of lengths 3 and 5 are roots of unity, and they are known. We shall give the calculations, not only for exposition, but because they provide us with the ability to explore various methods for explicitly computing CAZAC sequences in different ways. For the case of $p = 3$, we shall give 3 different techniques. The first uses the correspondence between cyclic N-roots and CAZAC sequences, the second uses the correspondence between CAZAC sequences and Hadamard matrices, and the last capitalizes on the various notions of equivalence of CAZAC sequences. Then we proceed similarly for the case $p = 5$. There are 6 unimodular cyclic 3-roots and 20 unimodular cyclic 5-roots, see Table 1. We shall see that some of our calculations apply for arbitrary prime lengths; and shall close the section by putting the material in the context of the 5-operation equivalence relations defined in Subsection 2.2.

3.2. **Constructing CAZAC sequences of length 3 using cyclic 3-roots.** We first would like to look at the specific case of cyclic 3-roots, which correspond to CAZAC sequences of length 3. In this case we are looking for solutions $(x, y, z) \in \mathbb{C}^3$ to the system of equations,

$$\begin{cases} x + y + z = 0 \\ xy + yz + zx = 0 \\ xyz = 1. \end{cases} \tag{13}$$

This system is easily solvable in the following way. First, multiply the second equation in (13) by z. This yields

$$xyz + yz^2 + xz^2 = 0.$$

By factoring z in the last two terms on the left hand side and using the third equation in (13) we have

$$1 + z^2(x + y) = 0.$$

Rearranging the first equation in (13) gives us that $x + y = -z$. Substituting this into the above, we obtain

$$1 - z^3 = 0,$$

or, in other words, z must be a 3rd root of unity. Note that the same computations can also be applied to x and y, and thus x and y must also be 3rd roots of unity.

This leads to the conjecture that the 6 permutations of the 3rd roots of unity $(1, e^{2\pi i/3}, e^{4\pi i/3})$ indeed generate all 6 CAZAC sequences of length 3. To this end, first let us write all 6 permutations of the 3rd roots of unity and the corresponding candidate CAZAC sequences. Then, we verify that the sequences really are CAZAC sequences by observing that they are known CAZAC sequences or 5-operation equivalent.

The 6 permutations of the 3rd roots of unity are

(1) $(1, e^{2\pi i/3}, e^{4\pi i/3})$
(2) $(1, e^{4\pi i/3}, e^{2\pi i/3})$
(3) $(e^{2\pi i/3}, 1, e^{4\pi i/3})$
(4) $(e^{2\pi i/3}, e^{4\pi i/3}, 1)$
(5) $(e^{4\pi i/3}, 1, e^{2\pi i/3})$
(6) $(e^{4\pi i/3}, e^{2\pi i/3}, 1)$.

Let (z_0, z_1, z_2) be a permutation of the 3rd roots of unity. To convert (z_0, z_1, z_2) to the corresponding CAZAC sequence, we begin by letting $x[0] = 1$. Then, we define $x[1]$ and $x[2]$ as

$$x[1] = z_0$$
$$x[2] = z_0 z_1.$$

Using this, we can construct Table 2.

TABLE 2. Cyclic 3-roots and CAZAC sequences of length 3

Cyclic 3-root	CAZAC sequence
$(1, e^{2\pi i/3}, e^{4\pi i/3})$	$(1, 1, e^{2\pi i/3})$
$(1, e^{4\pi i/3}, e^{2\pi i/3})$	$(1, 1, e^{4\pi i/3})$
$(e^{2\pi i/3}, 1, e^{4\pi i/3})$	$(1, e^{2\pi i/3}, e^{2\pi i/3})$
$(e^{2\pi i/3}, e^{4\pi i/3}, 1)$	$(1, e^{2\pi i/3}, 1)$
$(e^{4\pi i/3}, 1, e^{2\pi i/3})$	$(1, e^{4\pi i/3}, e^{4\pi i/3})$
$(e^{4\pi i/3}, e^{2\pi i/3}, 1)$	$(1, e^{4\pi i/3}, 1)$

In particular, each of the 6 sequences generated by the 6 permutations of the roots of unity generates either a known CAZAC sequence or an aforementioned transformation of a known CAZAC sequences. Thus, Table 2 lists all 6 CAZAC sequences of length 3.

3.3. **Constructing CAZAC sequences of length 3 using Hadamard matrices.** In [13], [19], it is stated that all 3×3 Hadamard matrices are equivalent to the Fourier matrix. In fact, we shall obtain this result from computations in this subsection. The website [19] further characterizes the set of 3×3 Hadamard matrices into two types:

$$\left\{ \begin{bmatrix} e^{ia} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{ic} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & W_3 & W_3^2 \\ 1 & W_3^2 & W_3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{ix} & 0 \\ 0 & 0 & e^{iy} \end{bmatrix} \right\} \bigcup$$

$$\left\{ \begin{bmatrix} e^{ia} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{ic} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & W_3^2 & W_3 \\ 1 & W_3 & W_3^2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{ix} & 0 \\ 0 & 0 & e^{iy} \end{bmatrix} \right\},$$

where $a, b, c, x, y \in [0, 2\pi)$. We shall use these two forms to find all 3×3 circulant Hadamard matrices.

First, we consider the first form and compute the matrix product:

$$\begin{bmatrix} e^{ia} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{ic} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & W_3 & W_3^2 \\ 1 & W_3^2 & W_3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{ix} & 0 \\ 0 & 0 & e^{iy} \end{bmatrix} = \begin{bmatrix} e^{ia} & e^{i(a+x)} & e^{i(a+y)} \\ e^{ib} & e^{i(b+x+\frac{2}{3}\pi)} & e^{i(b+y-\frac{2}{3}\pi)} \\ e^{ic} & e^{i(c+x-\frac{2}{3}\pi)} & e^{i(c+y+\frac{2}{3}\pi)} \end{bmatrix}. \tag{14}$$

In order for this matrix to be circulant, the following system of equations must hold mod 2π:

$$\begin{cases} a = b + x + \frac{2\pi}{3} = c + y + \frac{2\pi}{3} \\ c = a + x = b + y + \frac{4\pi}{3} \\ a + y = b = c + x + \frac{4\pi}{3}. \end{cases} \tag{15}$$

From the first equation in (15) we have

$$a = b + x + \frac{2}{3}\pi. \tag{16}$$

Using (16) in the second equation of (15), we calculate that

$$c = a + x = \left(b + x + \frac{2}{3}\pi \right) + x = b + 2x + \frac{2}{3}\pi. \tag{17}$$

From (16), (17), and the third equation of (15) we obtain,

$$y = c + x + \frac{4}{3}\pi - a = \left(b + 2x + \frac{2}{3}\pi \right) + x + \frac{4}{3}\pi - \left(b + x + \frac{2}{3}\pi \right) = 2x + \frac{4}{3}\pi. \tag{18}$$

Finally, returning to the first equation of (15) and using (17) and (18), we have

$$b = c + y - x = \left(b + 2x + \frac{2}{3}\pi \right) + \left(2x + \frac{4}{3}\pi \right) - x = b + 3x + 2\pi. \tag{19}$$

In particular, (19) implies that $3x \equiv 0 \bmod 2\pi$, i.e., x is $\frac{2}{3}\pi, 0$, or $-\frac{2}{3}\pi$. Letting $x = \frac{2}{3}\pi$, we obtain as one solution: $x = \frac{2}{3}\pi$, $a = \frac{4}{3}\pi + b$, $c = b$, and $y = \frac{2}{3}\pi$, where b is left indeterminate.

As such, we return to (14) and use this solution to compute

$$\begin{bmatrix} e^{i(\frac{4}{3}\pi+b)} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{ib} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & W_3 & W_3^2 \\ 1 & W_3^2 & W_3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{\frac{2}{3}\pi i} & 0 \\ 0 & 0 & e^{\frac{2}{3}\pi i} \end{bmatrix} = e^{ib} \begin{bmatrix} e^{-\frac{2}{3}\pi i} & 1 & 1 \\ 1 & e^{-\frac{2}{3}\pi i} & 1 \\ 1 & 1 & e^{-\frac{2}{3}\pi i} \end{bmatrix}.$$

The first row of the resulting circulant Hadamard matrix is $e^{ib}(e^{\frac{-2}{3}\pi i}, 1, 1)$. We let $b = \frac{2}{3}\pi$ and choose $(1, e^{\frac{2}{3}\pi i}, e^{\frac{2}{3}\pi i})$ as the representative for this class of CAZAC sequences and find our first CAZAC sequence.

As a second solution, we choose $x = 0$, which gives $a = \frac{2}{3}\pi + b$, $c = \frac{2}{3}\pi + b$, and $y = \frac{4}{3}\pi$, where b is again indeterminate. We return to (14) and compute,

$$\begin{bmatrix} e^{i(\frac{2}{3}\pi+b)} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{i(\frac{2}{3}\pi+b)} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & W_3 & W_3^2 \\ 1 & W_3^2 & W_3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & e^{\frac{4}{3}\pi i} \end{bmatrix} = e^{ib} \begin{bmatrix} e^{\frac{2}{3}\pi i} & e^{\frac{2}{3}\pi i} & 1 \\ 1 & e^{\frac{2}{3}\pi i} & e^{\frac{2}{3}\pi i} \\ e^{\frac{2}{3}\pi i} & 1 & e^{\frac{2}{3}\pi i} \end{bmatrix}.$$

The first row of this circulant Hadamard matrix is $e^{ib}(e^{\frac{2}{3}\pi i}, e^{\frac{2}{3}\pi i}, 1)$. Letting $b = -\frac{2}{3}\pi$, we have $(1, 1, e^{\frac{4}{3}\pi i})$ as our second CAZAC sequence.

The final solution is $x = -\frac{2}{3}\pi$, $a = b$, $c = b - \frac{2}{3}\pi$, and $y = 0$, where b is indeterminate. Returning to (14), we take

$$\begin{bmatrix} e^{ib} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{i(b-\frac{2}{3}\pi)} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & W_3 & W_3^2 \\ 1 & W_3^2 & W_3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{-\frac{2}{3}\pi i} & 0 \\ 0 & 0 & 1 \end{bmatrix} = e^{ib} \begin{bmatrix} 1 & e^{-\frac{2}{3}\pi i} & 1 \\ 1 & 1 & e^{-\frac{2}{3}\pi i} \\ e^{-\frac{2}{3}\pi i} & 1 & 1 \end{bmatrix}.$$

The first row of this circulant Hadamard matrix is $e^{ib}(1, e^{-\frac{2}{3}\pi i}, 1)$, and so letting $b = 0$, we have $(1, e^{\frac{4}{3}\pi i}, 1)$ as our third CAZAC sequence.

Now, we consider the second form of 3×3 Hadamard matrices in the union written at the beginning of this subsection, and take the product,

$$\begin{bmatrix} e^{ia} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{ic} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & W_3^2 & W_3 \\ 1 & W_3 & W_3^2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{ix} & 0 \\ 0 & 0 & e^{iy} \end{bmatrix} = \begin{bmatrix} e^{ia} & e^{i(a+x)} & e^{i(a+y)} \\ e^{ib} & e^{i(b+x-\frac{2}{3}\pi)} & e^{i(b+y+\frac{2}{3}\pi)} \\ e^{ic} & e^{i(c+x+\frac{2}{3}\pi)} & e^{i(c+y-\frac{2}{3}\pi)} \end{bmatrix}. \tag{20}$$

In order for the right hand side matrix to be circulant, the following equations must hold mod 2π:

$$\begin{cases} a = b + x + \frac{4\pi}{3} = c + y + \frac{4\pi}{3} \\ c = a + x = b + y + \frac{2\pi}{3} \\ a + y = b = c + x + \frac{2\pi}{3}. \end{cases} \tag{21}$$

Using the first equation in (21) we have

$$a = b + x + \frac{4}{3}\pi. \tag{22}$$

Next, using the second equation in (21) and as well as (22), we calculate that

$$c = a + x = \left(b + x + \frac{4}{3}\pi\right) + x = b + 2x + \frac{4}{3}\pi. \tag{23}$$

We now use the third equation in (21) along with (22) and (23), and obtain

$$y = c + x + \frac{2}{3}\pi - a = \left(b + 2x + \frac{4}{3}\pi\right) + x + \frac{2}{3}\pi - \left(b + x + \frac{4}{3}\pi\right) = 2x + \frac{2}{3}\pi \tag{24}$$

Finally, we return to the first equation of (21) and use (23) and (24) to compute

$$b = c + y - x = \left(b + 2x + \frac{4}{3}\pi\right) + \left(2x + \frac{2}{3}\pi\right) - x = b + 3x + 2\pi. \tag{25}$$

Similar to the previous calculations, (25) gives $3x \equiv 0 \bmod 2\pi$, or $x = \frac{2}{3}\pi$, $x = 0$, i.e., x is 0, $\frac{2}{3}\pi$ or $-\frac{2}{3}\pi$.

Our first solution is $x = \frac{2}{3}\pi$, $a = b$, $c = b + \frac{2}{3}\pi$, and $y = 0$, where b is arbitrary. As such, we return to (20) and compute

$$\begin{bmatrix} e^{ib} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{i(b+\frac{2}{3}\pi)} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & W_3 & W_3^2 \\ 1 & W_3^2 & W_3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{\frac{2}{3}\pi} & 0 \\ 0 & 0 & 1 \end{bmatrix} = e^{ib} \begin{bmatrix} 1 & e^{\frac{2}{3}\pi i} & 1 \\ 1 & 1 & e^{\frac{2}{3}\pi i} \\ e^{\frac{2}{3}\pi i} & 1 & 1 \end{bmatrix}.$$

The first row of the resulting circulant Hadamard matrix is $e^{ib}(1, e^{\frac{2}{3}\pi i}, 1)$, and so letting $b = 0$ we obtain $(1, e^{\frac{2}{3}\pi i}, 1)$ as the fourth CAZAC sequence.

Our second solution is $x = 0$, $y = \frac{2}{3}\pi$, $a = b + \frac{4}{3}\pi$, and $c = b + \frac{4}{3}\pi$ where b is arbitrary. In this case, we take

$$\begin{bmatrix} e^{i(b+\frac{4}{3}\pi)} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{i(b+\frac{4}{3}\pi)} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & W_3 & W_3^2 \\ 1 & W_3^2 & W_3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & e^{\frac{2}{3}\pi} \end{bmatrix} = e^{ib} \begin{bmatrix} e^{-\frac{2}{3}\pi i} & e^{-\frac{2}{3}\pi i} & 1 \\ 1 & e^{-\frac{2}{3}\pi i} & e^{-\frac{2}{3}\pi i} \\ e^{-\frac{2}{3}\pi i} & 1 & e^{-\frac{2}{3}\pi i} \end{bmatrix}.$$

The first row of this circulant Hadamard matrix is $e^{ib}(e^{-\frac{2}{3}\pi i}, e^{-\frac{2}{3}\pi i}, 1)$, and so letting $b = \frac{2}{3}\pi$ we obtain $(1, 1, e^{\frac{2}{3}\pi i})$ as the fifth CAZAC sequence.

A third solution is $x = -\frac{2}{3}\pi$, $y = -\frac{2}{3}\pi$, $a = b + \frac{2}{3}\pi$, and $c = b$. We take

$$\begin{bmatrix} e^{i(b+\frac{2}{3}\pi)} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{ib} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & W_3 & W_3^2 \\ 1 & W_3^2 & W_3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{-\frac{2}{3}\pi} & 0 \\ 0 & 0 & e^{-\frac{2}{3}\pi} \end{bmatrix} = e^{ib} \begin{bmatrix} e^{\frac{2}{3}\pi i} & 1 & 1 \\ 1 & e^{\frac{2}{3}\pi i} & 1 \\ 1 & 1 & e^{\frac{2}{3}\pi i} \end{bmatrix}.$$

The first row of this Hadamard matrix is $e^{ib}(e^{\frac{2}{3}\pi i}, 1, 1)$, and so letting $b = -\frac{2}{3}\pi$ we obtain $(1, e^{\frac{4}{3}\pi i}, e^{\frac{4}{3}\pi i})$ as the sixth and final CAZAC sequence.

To summarize, the six CAZAC sequences that we have obtained are:

$$(1, e^{2\pi i/3}, e^{2\pi i/3})$$

$$(1, 1, e^{4\pi i/3})$$

$$(1, e^{4\pi i/3}, 1)$$

$$(1, e^{2\pi i/3}, 1)$$

$$(1, 1, e^{2\pi i/3})$$

$$(1, e^{4\pi i/3}, e^{4\pi i/3});$$

and they are associated with the following circulant Hadamard matrices:

$$\begin{bmatrix} 1 & e^{2\pi i/3} & e^{2\pi i/3} \\ e^{2\pi i/3} & 1 & e^{2\pi i/3} \\ e^{2\pi i/3} & e^{2\pi i/3} & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & e^{4\pi i/3} \\ e^{4\pi i/3} & 1 & 1 \\ 1 & e^{4\pi i/3} & 1 \end{bmatrix}, \begin{bmatrix} 1 & e^{4\pi i/3} & 1 \\ 1 & 1 & e^{4\pi i/3} \\ e^{4\pi i/3} & 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & e^{2\pi i/3} & 1 \\ 1 & 1 & e^{2\pi i/3} \\ e^{2\pi i/3} & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & e^{2\pi i/3} \\ e^{2\pi i/3} & 1 & 1 \\ 1 & e^{2\pi i/3} & 1 \end{bmatrix}, \begin{bmatrix} 1 & e^{4\pi i/3} & e^{4\pi i/3} \\ e^{4\pi i/3} & 1 & e^{4\pi i/3} \\ e^{4\pi i/3} & e^{4\pi i/3} & 1 \end{bmatrix}.$$

Note that these CAZAC sequences match the CAZAC sequences found in Subsection 3.2.

3.4. **5-operation equivalence relations.** Let p be prime. In this subsection we show that the 5-operation equivalence relation is an equivalence relation which is generated by a group G acting on $U_p^p \subseteq \mathbb{C}^p$, where U_p^p is the group of ordered p-tuples of p roots of unity. We apply this to the specific cases of $p = 3$ and $p = 5$ in Section 3.5 to illustrate yet another way to generate all CAZAC sequences of length 3 and also to generate all sequences of length 5 in the process. We define the five operations again in the following way:

(1) $c_0x[n] = x[n]$ and $c_1x[n] = \overline{x[n]}$;
(2) $\tau_b x[n] = x[n-b]$, $b \in \mathbb{Z}/p\mathbb{Z}$;
(3) $\pi_c x[n] = x[cn]$, $c \in \mathbb{Z}/p\mathbb{Z}$, $c \neq 0$;
(4) $e_d x[n] = e^{2\pi idn/p}x[n]$, $d \in \mathbb{Z}/p\mathbb{Z}$;
(5) $\omega_f x[n] = e^{2\pi if/p}x[n]$, $f \in \mathbb{Z}/p\mathbb{Z}$.

With this, we can define the set G as

$$G = \{(a, b, c, d, f) : a \in \{0, 1\},\ b, c, d, f \in \mathbb{Z}/p\mathbb{Z},\ c \neq 0\},$$

which has size $|G| = 2p^3(p-1)$. To each element $(a, b, c, d, f) \in G$ we associate the operator $\omega_f e_d \pi_c \tau_b c_a$. To motivate the group operation we take $(a, b, c, d, f), (h, j, k, \ell, m) \in G$. One can show that the composition of the associated operators is

$$(\omega_m e_\ell \pi_k \tau_j c_h) \circ (\omega_f e_d \pi_c \tau_b c_a) = \omega_{m+(-1)^h(f-jc)} e_{\ell+(-1)^h kd} \pi_{ck} \tau_{cj+b} c_{a+h}.$$

As such we define the operation $\cdot : G \times G \to G$ by

$$(a, b, c, d, f) \cdot (h, j, k, \ell, m) = (a + h, cj + b, ck, \ell + (-1)^h kd, m + (-1)^h(f - jc)).$$

Theorem 3.1. *The operation $\cdot$ defines a group operation for G. In particular, $(G, \cdot)$ is a group.*

Proof. We need to show that the operation is associative, has an identity element, and that each element has an inverse. It is easily verified that the identity element is $(0, 0, 1, 0, 0)$. Given an element $(a, b, c, d, f) \in G$, it is elementary to verify that

$$(a, b, c, d, f)^{-1} = (-a, -bc^{-1}, c^{-1}, (-1)^{-a+1}c^{-1}d, (-1)^{-a+1}(f + bc^{-1}d)).$$

Finally, for associativity we first compute

$$\begin{aligned}
&(v, w, x, y, z) \cdot ((a, b, c, d, f) \cdot (h, j, k, \ell, m)) \\
&= (v, w, x, y, z) \cdot (a + h, cj + b, ck, \ell + (-1)^h kd, m + (-1)^h(f - jc)) \\
&= (a + h + v, cjx + bx + w, ckx, \ell + (-1)^h kd + (-1)^{a+h} cky, \\
&\quad m + (-1)^h(f - jc) + (-1)^{a+h}(z - cjx - bx)).
\end{aligned}$$

Then, we compute

$$\begin{aligned}
&((v, w, x, y, z) \cdot (a, b, c, d, f)) \cdot (h, j, k, \ell, m) \\
&= (a + v, bx + w, cx, d + (-1)^a cy, f + (-1)^a(z - bx)) \cdot (h, j, k, \ell, m) \\
&= (a + h + v, cxj + bx + w, ckx, \ell + (-1)^h kd + (-1)^{a+h} kcy, \\
&\quad m + (-1)^h(f - jc) + (-1)^{a+h}(z - cjx - bx)).
\end{aligned}$$

Consequently, $\cdot$ is an associative operation. □

Since $(G, \cdot)$ is a group, it defines a proper group action on U_p^p. There are $p(p-1)$ many CAZAC sequences which start with 1 in U_p^p. If we construct all CAZAC sequences in U_p^p, including those whose first term is not 1, we see that there are $p^2(p-1)$ CAZAC sequences in U_p^p.

Theorem 3.2. *Let p be an odd prime and let $x \in U_p^p$ be the Wiener sequence $x[n] = e^{2\pi i s n^2/p}$, where $s \in \mathbb{Z}/p\mathbb{Z}$, see Example 2.5. Denote the stabilizer of x under the group $(G, \cdot)$ as G_x. If $p \equiv 1 \mod 4$, then $|G_x| = 4p$. If $p \equiv 3 \mod 4$, then $|G_x| = 2p$. In particular, the orbit of x has size $p^2(p-1)/2$ if $p \equiv 1 \mod 4$ and has size $p^2(p-1)$ if $p \equiv 3 \mod 4$.*

Proof. First, let $(a, b, c, d, f) \in G$, and note that

$$(\omega_f e_d \pi_c \tau_b c_a)(x)[n] = W_p^{f+dn} c_a x[cn - b] = W_p^{f+dn+(-1)^a s(cn-b)^2}.$$

Setting $n = 0$ gives the condition that for $(a, b, c, d, f) \in G$,

$$f + (-1)^a s b^2 \equiv 0 \mod p, \tag{26}$$

from which we conclude that

$$f \equiv -(-1)^a s b^2 \mod p. \tag{27}$$

Setting $n = 1$ and substituting for f as in (27) gives us another condition, viz.,

$$(-1)^a s(c-b)^2 + d - (-1)^a s b^2 \equiv s \mod p. \tag{28}$$

From (28) we can solve for d to obtain

$$d \equiv s + (-1)^a s(2bc - c^2) \mod p. \tag{29}$$

Now, note that for any other $n > 1$, we can use (27) and (29) to obtain the equation

$$(-1)^a s(nc-b)^2 + n + (-1)^a s(2bc - c^2)n - (-1)^a s b^2 \equiv s n^2 \mod p. \tag{30}$$

After expanding and cancelling terms, we reduce (30) to

$$c^2 \equiv (-1)^a \mod p. \tag{31}$$

If $a = 0$, then (31) has two solutions, which we shall denote by c_0^+ and c_0^-. If $a = 1$, then by the law of quadratic reciprocity, (31) has two solutions, c_1^+ and c_1^- if $p \equiv 1 \mod 4$, but no solutions if $p \equiv 3 \mod 4$. Thus, if $p \equiv 3 \mod 4$, we obtain the following as stabilizers of x:

(1) $(0, b, c_0^+, 1 + 2bc_0^+ - (c_0^+)^2, -b^2)$
(2) $(0, b, c_0^-, 1 + 2bc_0^- - (c_0^-)^2, -b^2)$

which holds for any $b \in \mathbb{Z}/p\mathbb{Z}$. If $p \equiv 1 \mod 4$, then the following two sets of stabilizers also hold:

(1) $(0, b, c_1^+, 1 + 2bc_1^+ - (c_1^+)^2, -b^2)$
(2) $(0, b, c_1^-, 1 + 2bc_1^- - (c_1^-)^2, -b^2)$

for any $b \in \mathbb{Z}/p\mathbb{Z}$. Thus, if $p \equiv 1 \mod p$ there are $4p$ stabilizers for x, and if $p \equiv 1 \mod p$ there are $2p$ stabilizers for x. □

Corollary 3.3. *If $p \equiv 3 \mod 4$, there is only one equivalence class of CAZAC sequences in U_p^p.*

Theorem 3.4. *Let $p \equiv 1 \mod 4$, and $x, y \in \mathbb{C}^N$. Let $x = e^{2\pi i n^2/p}$ and $y = e^{2\pi i s n^2/p}$, where s is not a quadratic residue modulo p. Then, x and y belong to different 5-operation equivalence classes.*

Proof. Let $s = 1$ in the proof of Theorem 3.2, and for $(a, b, c, d, f) \in G$, we have

$$(\omega_f e_d \pi_c \tau_b c_a)(\varphi)[n] = W_p^{f+dn} c_a \varphi[cn - b] = W_p^{f+dn+(-1)^a(cn-b)^2}.$$

Emulating the proof of Theorem 3.2, we let $n = 0$ and obtain the condition,

$$f \equiv -(-1)^a b^2 \mod p.$$

Now letting $n = 1$ we have the condition,

$$d \equiv s + (-1)^a(2bc - c^2) \mod p.$$

For arbitrary $n > 1$, we obtain

$$(-1)^a(nc - b)^2 + sn + (-1)^a(2bc - c^2)n - (-1)^a b^2 \equiv sn^2 \mod p. \tag{32}$$

After expanding and cancelling terms, we calculate that

$$c^2 \equiv (-1)^a s \mod p.$$

Since $p \equiv 1 \mod 4$ and s is not a residue modulo p, (32) cannot be solved for either value of a. Thus, x and y must belong to different equivalence classes. □

Corollary 3.5. *If $p \equiv 1 \mod 4$, then there are exactly two equivalence classes of CAZAC sequences in U_p^p both of which have size $p^2(p-1)/2$.*

3.5. **5-operation equivalence for lengths 3 and 5.** We now apply the results from Subsection 3.4 to show there is only one 5-operation equivalence class for length 3 CAZAC sequences. Indeed, suppose that $x = (1, 1, e^{2\pi i/3})$. Then, the other five CAZAC sequences can be obtained from 5-operation equivalency as follows:

(1) $c_1 x = (1, 1, e^{4\pi i/3})$
(2) $e_1 c_1 x = (1, e^{2\pi i/3}, e^{2\pi i/3})$
(3) $e_1 x = (1, e^{2\pi i/3}, 1)$
(4) $e_2 x = (1, e^{4\pi i/3}, e^{4\pi i/3})$
(5) $e_2 c_1 x = (1, e^{4\pi i/3}, 1)$

Corollary 3.5 tells us that there are two 5-operation equivalence classes in the case $p = 5$. To write them explicitly, we start with the Wiener sequence,

$$x = (1, e^{2\pi i/5}, e^{8\pi i/5}, e^{8\pi i/5}, e^{2\pi i/5}).$$

We show that we can obtain 10 CAZAC sequences by applying 5-operation equivalencies to x:

(1) $x = (1, e^{2\pi i/5}, e^{8\pi i/5}, e^{8\pi i/5}, e^{2\pi i/5})$
(2) $c_1 x = (1, e^{8\pi i/5}, e^{2\pi i/5}, e^{2\pi i/5}, e^{8\pi i/5})$
(3) $\omega_1 \tau_1 c_1 x = (1, e^{2\pi i/5}, 1, e^{4\pi i/5}, e^{4\pi i/5})$
(4) $\omega_4 \tau_1 x = (1, e^{8\pi i/5}, 1, e^{6\pi i/5}, e^{6\pi i/5})$
(5) $\omega_4 \tau_2 c_1 x = (1, e^{6\pi i/5}, e^{8\pi i/5}, e^{6\pi i/5}, 1)$
(6) $\omega_1 \tau_2 x = (1, e^{4\pi i/5}, e^{2\pi i/5}, e^{4\pi i/5}, 1)$
(7) $\omega_4 \tau_3 c_1 x = (1, 1, e^{6\pi i/5}, e^{8\pi i/5}, e^{6\pi i/5})$
(8) $\omega_1 \tau_3 x = (1, 1, e^{4\pi i/5}, e^{2\pi i/5}, e^{4\pi i/5})$
(9) $\omega_1 \tau_4 c_1 x = (1, e^{4\pi i/5}, e^{4\pi i/5}, 1, e^{2\pi i/5})$
(10) $\omega_4 \tau_4 x = (1, e^{6\pi i/5}, e^{6\pi i/5}, 1, e^{8\pi i/5})$.

To find the other orbit, we use the fact that 3 is not a quadratic residue modulo 5 and apply Theorem 3.4. We then let x be the Wiener sequence,

$$x = (1, e^{6\pi i/5}, e^{4\pi i/5}, e^{4\pi i/5}, e^{6\pi i/5}),$$

and we compute

(1) $x = (1, e^{6\pi i/5}, e^{4\pi i/5}, e^{4\pi i/5}, e^{6\pi i/5})$
(2) $c_1 x = (1, e^{4\pi i/5}, e^{6\pi i/5}, e^{6\pi i/5}, e^{4\pi i/5})$
(3) $\omega_3 \tau_1 c_1 x = (1, e^{6\pi i/5}, 1, e^{2\pi i/5}, e^{2\pi i/5})$
(4) $\omega_2 \tau_1 x = (1, e^{4\pi i/5}, 1, e^{8\pi i/5}, e^{8\pi i/5})$
(5) $\omega_2 \tau_2 c_1 x = (1, e^{8\pi i/5}, e^{4\pi i/5}, e^{8\pi i/5}, 1)$
(6) $\omega_3 \tau_2 x = (1, e^{2\pi i/5}, e^{6\pi i/5}, e^{2\pi i/5}, 1)$
(7) $\omega_2 \tau_3 c_1 x = (1, 1, e^{8\pi i/5}, e^{4\pi i/5}, e^{8\pi i/5})$
(8) $\omega_3 \tau_3 x = (1, 1, e^{2\pi i/5}, e^{6\pi i/5}, e^{2\pi i/5})$
(9) $\omega_3 \tau_4 x = (1, e^{2\pi i/5}, e^{2\pi i/5}, 1, e^{6\pi i/5})$
(10) $\omega_2 \tau_4 x = (1, e^{8\pi i/5}, e^{8\pi i/5}, 1, e^{4\pi i/5})$.

In conclusion, we have explicitly shown that the $p = 3$ case has exactly one orbit, and have shown which 5-operation transformations generate them starting with

$$x = (1, 1, e^{2\pi i/3}).$$

In the $p = 5$ case we have explicitly shown that there are two orbits under 5-operation equivalence. We generated both orbits using two different Wiener sequences, and have written the 5-operation transformations that generate them.

4. Non-roots of unity CAZAC sequences of prime length

4.1. **Björck sequences of prime length.** In Subsection 1.2, we stated Björck's 1984 counterexample, Equation (3), showing that not all CAZAC sequences of length 7 are Gaussian sequences or even roots of unity.

Let p be a prime number, and let $(\frac{k}{p})$ denote the *Legendre symbol* modulo p, defined as

$$\left(\frac{k}{p}\right) = \begin{cases} 0, & \text{if } k \equiv 0 \,(\mathrm{mod}\, p), \\ 1, & \text{if } k \equiv n^2 \,(\mathrm{mod}\, p) \ \text{ for some } n \in \mathbb{Z}, \\ -1, & \text{if } k \not\equiv n^2 \,(\mathrm{mod}\, p) \ \text{ for all } n \in \mathbb{Z}. \end{cases}$$

Thus, we can define the function $\Lambda : \mathbb{Z}/p\mathbb{Z} \longrightarrow \{+1, 0, -1\}$ as

$$\Lambda[k] = \left(\frac{k}{p}\right).$$

The pre-image of $+1$ under the function Λ is the set $\mathcal{Q}$ of non-zero *quadratic residues* modulo p; and the pre-image of -1 under the function Λ is the set $\mathcal{Q}^C$ of *quadratic non-residues* modulo p. Λ is a *character* of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. This means that Λ, when restricted to $(\mathbb{Z}/p\mathbb{Z})^\times$, is a group homomorphism into the multiplicative group $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$. See [34], Chapters V and VI, for a classical treatment, and [6] for a critical application estimating values of the ambiguity function by means of estimates in terms of Weil's proof of the Riemann hypothesis for finite fields.

Definition 4.1. Let p be a prime number, and so $\mathbb{Z}/p\mathbb{Z}$ is a field.

If $p \equiv 1 \pmod 4$, the *Björck sequence*, $b_p : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$, of length p, is defined as

$$\forall k = 0, 1, ..., p-1, \quad b_p[k] = e^{i\theta_p(k)},$$

where

$$\theta_p(k) = \left(\frac{k}{p}\right) \arccos\left(\frac{1}{1+\sqrt{p}}\right).$$

If $p \equiv 3 \pmod 4$, or, equivalently, for $p \equiv -1 \pmod 4$, the *Björck sequence*, $b_p : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$, of length p, is defined as

$$\forall k = 0, 1, ..., p-1, \quad b_p[k] = \begin{cases} e^{i\theta_p(k)}, & \text{if } k \in \mathcal{Q}^C \subseteq (\mathbb{Z}/p\mathbb{Z})^\times, \\ 1, & \text{otherwise,} \end{cases}$$

where

$$\theta_p(k) = \arccos\left(\frac{1-p}{1+p}\right).$$

In [14] Björck proved that Björck sequences are CAZAC sequences, and elaborated on it in [15] by analyzing the structure of bi-equimodular functions. The structure is related to the subgroup of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$, e..g., the group of quadratic residues. It was in this context that he used Proposition 2.4 in [15], and which he had originally proved in [14]. The following is Björck's main theorem on the topic. Because of the role of the Legendre symbol in the definition of Björck sequences, it is natural to expect a more computational proof of Theorem 4.2 in terms of the Legendre symbol. This was done by J. J. Benedetto, R. L. Benedetto, and J. T. Woodworth [5] (2012).

Theorem 4.2. *Let p be prime.*

a. If $p \equiv 1 \pmod 4$, then $b_p : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ is a 3-valued CAZAC sequence of length p.

b. If $p \equiv 3 \pmod 4$, then $b_p : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ is a 2-valued CAZAC sequence of length p.

Remark 4.3. *a.* Let $p \equiv 1 \pmod 4$. Note that the Legendre symbol sequence of length p has the form $\{0, 1, \ldots, -1, \ldots, 1\}$, i.e., $(\frac{p-1}{p}) = 1$, see Example 4.4. In this case of $p \equiv 1 \pmod 4$, Definition 4.1 is equivalent to the following sequence constructed by replacing elements of the Legendre sequence. We replace 0 by 1, every term 1 by

$$\eta = \exp\left(i \arccos\frac{\sqrt{p}-1}{p-1}\right) = \frac{1}{\sqrt{p}+1} + i\frac{\sqrt{p+2\sqrt{p}}}{\sqrt{p}+1},$$

and every term -1 by the complex conjugate $\overline{\eta}$ of η. Then, $1, \eta, \overline{\eta}$ are the 3 values of this Björck CAZAC sequence. See Saffari [54] for a generalization.

b. Let $p \equiv 3 \pmod 4$. Note that the Legendre symbol sequence of length p has the form $\{0, 1, \ldots, -1, \ldots, -1\}$, i.e., $(\frac{p-1}{p}) = -1$, see Example 4.4. In this case of $p \equiv 3 \pmod 4$, Definition 4.1 is equivalent to the following sequence constructed by replacing elements of the Legendre sequence. We replace 0 by 1, every term -1 by

$$\xi = \exp\left(i \arccos\frac{1-p}{1+p}\right) = \frac{1-p}{1+p} + i\frac{2\sqrt{p}}{1+p},$$

and leave the original $1s$ as they are. Then, $1, \xi$ are the 2 values of this Björck CAZAC sequence.

Example 4.4. *a.* As an example of the assertion in Remark 4.3 that if $p \equiv 1 \pmod 4$, then the Legendre symbol sequence of length p has the form $\{0, 1, \ldots, -1, \ldots, 1\}$, i.e., $(\frac{p-1}{p}) = 1$, let $p = 13$. Consequently, $12 \equiv 5^2 \pmod{13}$.

b. As an example of the assertion in Remark 4.3 that if $p \equiv 3 \pmod 4$, then the Legendre symbol sequence of length p has the form $\{0, 1, \dots, -1, \dots, -1\}$, i.e., $(\frac{p-1}{p}) = -1$, let $p = 19$. In this case, it is generally difficult to prove assertions of the form,

$$k \not\equiv n^2 \,(\mathrm{mod}\, p) \;\text{ for all } n \in \mathbb{Z}.$$

Fortunately, we have Legendre's theorem, which asserts for $k \neq 0$ that

$$\left(\frac{k}{p}\right) \equiv k^{(p-1)/2} \,(\mathrm{mod}\, p),$$

and so

$$\left(\frac{p-1}{p}\right) = \left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4, \\ -1, & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

[34].

c. By straightforward calculations, we see that Björck sequences are Gaussian for $p = 3, 5$.

d. The theory of frames and CAZAC sequences are natural allies, especially in the case of non-Gaussian CAZAC sequences such as the Björck sequences, e.g., see [10], [44]. In fact, finite Gabor frames for $\mathbb{C}^d$ with CAZAC sequences as generating functions are a natural source of examples and direction for finding further examples, in order to deal with open questions in topics such as compressed sensing and Zauner's conjecture in quantum mechanics.

4.2. **Circulant Hadamard matrices not equivalent to $\mathcal{D}_7$.** If we consider $p \times p$ Hadamard matrices, where p is prime, we want to know if the Hadamard matrices generated by CAZAC sequences are always equivalent to $\mathcal{D}_p$, the $p \times p$ DFT matrix. If $p = 2, 3, 5$, then we have already noted that all Hadamard matrices are equivalent to $\mathcal{D}_p$, regardless of whether or not they are generated by a CAZAC sequence [19].

If $p = 7$, then Björck's example shows that there are Hadamard matrices not equivalent to $\mathcal{D}_7$ [19]. One such Hadamard matrix H_1 is defined as follows. Let $\theta = \arccos(-3/4)$ and let $d = \exp(i\theta)$, and set

$$H_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & d^{-1} & 1 & d & d^{-1} & d & 1 \\ 1 & d^{-1} & d^{-1} & d & 1 & 1 & d \\ 1 & d^{-2} & d^{-2} & d^{-1} & d^{-1} & 1 & d^{-1} \\ 1 & 1 & d^{-1} & 1 & d^{-1} & d & d \\ 1 & d^{-2} & d^{-1} & d^{-1} & d^{-2} & d^{-1} & 1 \\ 1 & d^{-1} & d^{-2} & 1 & d^{-2} & d^{-1} & d^{-1} \end{bmatrix},$$

[19], [31]. To continue the process, let $P_1 = P_2 = Id_7$ and D_1, D_2 be the following matrices:

$$D_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & d & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & d & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & d \end{bmatrix}, \qquad D_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & d & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & d & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & d & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Then, we can define an equivalent circulant Hadamard matrix H_2 by

$$H_2 = D_1 H_1 D_2 = \begin{bmatrix} 1 & d & d & 1 & d & 1 & 1 \\ 1 & 1 & d & d & 1 & d & 1 \\ 1 & 1 & 1 & d & d & 1 & d \\ d & 1 & 1 & 1 & d & d & 1 \\ 1 & d & 1 & 1 & 1 & d & d \\ d & 1 & d & 1 & 1 & 1 & d \\ d & d & 1 & d & 1 & 1 & 1 \end{bmatrix}.$$

In particular, the first column of H_2 is the length 7 Björck sequence and so H_2 is the Hadamard matrix associated with the length 7 Björck sequence.

Another matrix, that is equivalent to neither $\mathcal{D}_7$ nor H_1, is

$$J_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a^{-2} & a^{-1}b^{-1} & a^{-1}c^{-1} & a^{-1} & a^{-1}c & a^{-1}b \\ 1 & a^{-1}b^{-1} & a^{-2}b^{-2} & a^{-1}b^{-2}c^{-1} & a^{-1}b^{-1}c^{-1} & a^{-1}b^{-1}c & a^{-1}c \\ 1 & a^{-1}c^{-1} & a^{-1}b^{-2}c^{-1} & a^{-2}b^{-2}c^{-2} & a^{-1}b^{-2}c^{-2} & a^{-1}b^{-1}c^{-1} & a^{-1} \\ 1 & a^{-1} & a^{-1}b^{-1}c^{-1} & a^{-1}b^{-2}c^{-2} & a^{-2}b^{-2}c^{-2} & a^{-1}b^{-2}c^{-1} & a^{-1}c^{-1} \\ 1 & a^{-1}c & a^{-1}b^{-1}c & a^{-1}b^{-1}c^{-1} & a^{-1}b^{-2}c^{-1} & a^{-2}b^{-2} & a^{-1}b^{-1} \\ 1 & a^{-1}b & a^{-1}c & a^{-1} & a^{-1}c^{-1} & a^{-1}b^{-1} & a^{-2} \end{bmatrix},$$

where $a \approx \exp(4.312839i), b \approx \exp(1.356228i), c \approx \exp(1.900668i)$, see [16], [19]. The numbers, a, b, and c, are algebraic numbers whose explicit values can be found in [16]. We can put these two matrices in circulant form by multiplying J_1 on the left and right by the matrix,

$$D = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & ab & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & abc & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & abc & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & ab & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & a \end{bmatrix}.$$

Carrying out the multiplication, the circulant form of J_1, denoted as J_2, can be written as

$$J_2 = DJ_1D = \begin{bmatrix} 1 & a & ab & abc & abc & ab & a \\ a & 1 & a & ab & abc & abc & ab \\ ab & a & 1 & a & ab & abc & abc \\ abc & ab & a & 1 & a & ab & abc \\ abc & abc & ab & a & 1 & a & ab \\ ab & abc & abc & ab & a & 1 & a \\ a & ab & abc & abc & ab & a & 1 \end{bmatrix}.$$

5. Haagerup's theorem

5.1. **Introduction.** We shall now outline that part of Haagerup's proof of his Theorem 1.6 [32] in which he proves that there are only finitely many cyclic p-roots. The complete proof in which the precise number of cyclic p-roots is computed requires sophisticated complex analysis that is beyond the scope of our theme.

At the risk of oversimplifying, the proof that there are only finitely many cyclic p-roots is divided in two parts: an ingenious algebraic manipulation using the DFT, coupled with an application of the uncertainty principle for $\mathbb{Z}/p\mathbb{Z}$.

5.2. **Algebraic manipulation.** Recall that cyclic N-roots are solutions $z = (z_0, \dots, z_{N-1}) \in \mathbb{C}^N$ of the system of equations:

$$\begin{cases} z_0 + z_1 + \cdots + z_{N-1} = 0 \\ z_0 z_1 + z_1 z_2 + \cdots + z_{N-1} z_0 = 0 \\ \qquad\qquad \cdots \\ z_0 z_1 \cdots z_{N-2} + \cdots + z_{N-1} z_0 \cdots z_{N-3} = 0 \\ z_0 z_1 \cdots z_{N-1} = 1, \end{cases} \tag{33}$$

see Definition 1.4. In particular, because of the last equation of (33), $z_j \in \mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ for any cyclic N-root $z \in \mathbb{C}^N$. Haagerup makes several substitutions to transform (33).

First, assume $z \in \mathbb{C}^N$ is a cyclic N-root. Let $x_0 = 1$ and $x_j = z_0 z_1 \cdots z_{j-1}$ for all $j = 1, \dots, N-1$. Thus, $x_{j+1}/x_j = z_j$ for $j = 0, \dots, N-2$, where the last equation of (33) guarantees that x_{j+1}/x_j is well-defined. Further, for $j = N-1$, we have

$$\frac{x_0}{x_{N-1}} = \frac{1}{z_0 z_1 \cdots z_{N-2}} = z_{N-1},$$

because $z_0 z_1 \cdots z_{N-1} = 1$ by the last equation of (33). Substituting these equations, that relate the x_j and z_i, into (33) we see that $x = (x_0, \dots, x_{N-1})$ is a solution to the system,

$$\begin{cases} x_0 = 1 \\ \frac{x_1}{x_0} + \frac{x_2}{x_1} + \ldots + \frac{x_0}{x_{N-1}} = 0 \\ \frac{x_2}{x_0} + \frac{x_3}{x_1} + \ldots + \frac{x_1}{x_{N-1}} = 0 \\ \qquad\qquad \cdots \\ \frac{x_{N-1}}{x_0} + \frac{x_0}{x_1} + \ldots + \frac{x_{N-2}}{x_{N-1}} = 0. \end{cases} \tag{34}$$

Conversely, if $x = (x_0, \dots, x_{N-1}) \in (\mathbb{C}^\times)^N$ is a solution to the system (34), then it is easy to check that

$$z = (z_0, \dots, z_{N-1}) = \left(\frac{x_1}{x_0}, \frac{x_2}{x_1}, \dots, \frac{x_0}{x_{N-1}} \right) \in (\mathbb{C}^\times)^N$$

is a solution to (33). Haagerup says that solutions x to (34) are *cyclic N-roots on the x-level*.

Second, assume $x = (x_0, \dots, x_{N-1}) \in (\mathbb{C}^\times)^N$ is a cyclic N-root on the x-level. Let $y_j = 1/x_j$, for $j = 0, \dots, N-1$. Then,

$$(x, y) = (x_0, \dots, x_{N-1}, y_0, \dots, y_{N-1}) \in (\mathbb{C}^\times)^N \times (\mathbb{C}^\times)^N$$

is a solution to the system,

$$\begin{cases} x_0 = y_0 = 1, \\ x_k y_k = 1, 1 \le k \le N-1, \\ \sum_{m=0}^{N-1} x_{k+m} y_m = 0, 1 \le k \le N-1. \end{cases} \tag{35}$$

Conversely, if $(x, y) \in \mathbb{C}^N \times \mathbb{C}^N$ is solution to (35), then, noting the condition $x_k y_k = 1$ of (35), it is easy to check that $x \in (\mathbb{C}^\times)^N$ and that x is a solution to (34). Haagerup says solutions $(x, y) \in \mathbb{C}^N \times \mathbb{C}^N$ to (35) are *cyclic N-roots on the (x, y)-level*.

Third, Haagerup introduces the DFT into the mix, and proves that the system of equations (35) for the cyclic N-roots on the (x, y)-level are equivalent to the following system of equations for $(x, y) \in \mathbb{C}^N \times \mathbb{C}^N$:

$$\begin{cases} x_0 = y_0 = 1 \\ x_m y_m = 1, 1 \leq m \leq N-1 \\ \widehat{x}_n \widehat{y}_{-n} = 1, 1 \leq n \leq N-1. \end{cases} \tag{36}$$

Without providing the details, we can see how the third equation of (36) is deduced from (35) by writing out the product $\widehat{x}_n \widehat{y}_{-n}$.

Since we began recording these equivalences with cyclic N-roots $z = (z_0, \ldots, z_N)$ as defined in Subsection 1.3, we wrote $x_m, \widehat{x}_n$ in (36), but this is really $x[m], \widehat{x}[n]$ in the notation from Subsection 1.2.

None of the details in this subsection is difficult to prove, *but* Haagerup's strategy is dazzling! The transformations from the cyclic N-roots problem (33) to that of (36) preserve the number of distinct solutions, and so solving (36) is equivalent to solving (33), viz., if there are $0 \leq M \leq \infty$ solutions to one, then there are $0 \leq M \leq \infty$ solutions to the other. As such, Haagerup's proof that the set of cyclic p-roots is finite will be to solve (36).

5.3. **The uncertainty principle for $\mathbb{Z}/p\mathbb{Z}$.** In order to prove that the set of cyclic p-roots is finite (Theorem 5.6), Haagerup's strategy required Theorem 5.3 and Theorem 5.5. Theorem 5.3 is an uncertainty principle for the finite Abelian group $\mathbb{Z}/p\mathbb{Z}$, where p is prime. Its proof uses Chebotarëv's theorem, a fact known to Haagerup in 1996. We should point out that Gabidulin also understood the role of Chebotarëv's theorem if one wanted to prove Theorem 5.6.

Theorem 5.1. *(Chebotarëv 1926) Let p be prime and let $\mathcal{D}_p$ be the unitary Fourier matrix on $\mathbb{C}^p$, defined as*

$$\mathcal{D}_N = \left[\frac{1}{N^{1/2}} W_N^{-mn} \right]_{m,n=0}^{N-1},$$

see Definition 1.2. Then, all square submatrices of $\mathcal{D}_p$ have non-zero determinant.

Remark 5.2. There have been many different proofs of this theorem since Chebotarëv's original proof in 1926. A sampling of authors of published proofs is Danilevskii (1937), Reshetnyak (1955), Dieudonné (1970), M. Newman (1975), Evans and I. Stark (1977), Stevenhagen and Lenstra (1996), Goldstein, Guralnick, and Isaacs (c. 2004), and Tao (2005). There is also the proof by Frenkel (2004), that he first wrote down as a solution to a problem in the 1998 Schweitzer Competition! In fact, Chebotarëv's original proof provides much more information than Theorem 5.1 asserts, see [57], which is also a spectacular exposition of Chebotarëv's life and mathematical contributions, including his celebrated density theorem.

Independently, Tao [61] used Theorem 5.1 in order to prove Theorem 5.3. Further, he noted that the two results are equivalent, a fact discovered independently by András Biró. Theorem 5.3 itself is a refinement for the setting of $\mathbb{Z}/p\mathbb{Z}$ of the uncertainty principle inequality,

$$|\mathrm{supp}(u)|\,|\mathrm{supp}(\widehat{u})| \geq |G|, \tag{37}$$

where G is a finite Abelian group, $u : G \longrightarrow \mathbb{C}$ is a function, $\widehat{u}$ is the discrete Fourier transform of u, $|X|$ is the cardinality of X, and $\mathrm{supp}(u) = \{x \in G : u(x) \neq 0\}$ is the *support*

of u, see [62] for a systematic treatment of the discrete Fourier transform. The inequality, (37), is due to Donoho and Stark [24], cf., [56].

Theorem 5.3. *If $u \neq 0 \in \mathbb{C}^p$ and $\widehat{u} = \mathcal{F}_p u$ is the discrete Fourier transform of u, then $|\text{supp}(u)| + |\text{supp}(\widehat{u})| \geq p + 1$, where $|\text{supp}(u)|$, the support of u, denotes the number of non-zero coordinates of u.*

Algebraic varieties are a central object of study in algebraic geometry. Classically, and for us, an *algebraic variety* is defined as the set of solutions of a system of polynomial equations over the real or complex numbers. The following is a basic theorem.

Theorem 5.4. *A compact algebraic variety in $\mathbb{C}^N$ is a finite set, e.g., see* [52]*, Theorem 13.3.*

Theorem 5.5. *If the number of solutions $(x, y) \in \mathbb{C}^N \times \mathbb{C}^N$ to (36) is infinite, then there are $u, v \in \mathbb{C}^N \setminus \{0\}$ such that $u_k v_k = 0$ and $\widehat{u}_k \widehat{v}_{-k} = 0$ for each $0 \leq k \leq N-1$.*

Proof. Let $W \subseteq \mathbb{C}^N \times \mathbb{C}^N$ denote the set of solutions to (36), and assume W is an infinite set. Since W is an algebraic variety, then, by Theorem 5.4 and the Heine-Borel theorem, W must be unbounded. Choose a sequence $\{(x^{(m)}, y^{(m)})\} \subseteq W$ for which

$$\lim_{m\to\infty} (||x^{(m)}||_2^2 + ||y^{(m)}||_2^2)^{1/2} = \infty.$$

Let $u^{(m)}$ and $v^{(m)}$ be the normalizations of $x^{(m)}$ and $y^{(m)}$, respectively, i.e., $u^{(m)} = x^{(m)}/||x^m||_2$. Therefore, the sequence, $\{(u^{(m)}, v^{(m)})\}$, is contained in a compact set. Suppose that this sequence converges to (u, v), passing to a subsequence if necessary. Because each $(x^{(m)}, y^{(m)})$ is a solution to (36), $x_0^{(m)} = y_0^{(m)} = 1$ for all $m \in \mathbb{N}$. Thus, $||x^{(m)}||_2^2 = 1 + c_m$ and $||y^{(m)}||_2^2 = 1 + d_m$, where $c_m, d_m > 0$. It follows that

$$||x^{(m)}||_2^2 ||y^{(m)}||_2^2 = (1 + c_m)(1 + d_m) \geq 1 + c_m + d_m = ||x^{(m)}||_2^2 + ||y^{(m)}||_2^2 - 1.$$

Hence, by our choice of $\{(x^{(m)}, y^{(m)})\}$, we have

$$\lim_{m\to\infty} ||x^{(m)}||_2^2 ||y^{(m)}||_2^2 = \infty.$$

Now, from (36), we know that $x_k^{(m)} y_k^{(m)} = \widehat{x^{(m)}}_k \widehat{y^{(m)}}_{-k} = 1$ for each $m \geq 1$ and each $1 \leq k \leq N-1$; and so

$$u_k v_k = \widehat{u}_k \widehat{v}_{-k} = \lim_{m\to\infty} (||x^{(m)}||_2 ||y^{(m)}||_2)^{-1}$$

for $1 \leq k \leq N-1$. In addition, this equality is also true for $k = 0$, because $x_0^{(m)} = y_0^{(m)} = 1$. Therefore, since

$$\lim_{m\to\infty} ||x^{(m)}||_2 ||y^{(m)}||_2 = \infty,$$

we have that $u_k v_k = \widehat{u}_k \widehat{v}_{-k} = 0$.

□

Theorem 5.6. *(Haagerup) The set of cyclic p-roots is finite.*

Proof. Let $N = p$ in (36). Assume for the sake of obtaining a contradiction that the set of solutions to (36) is infinite. Then, by Theorem 5.5, there are $u, v \in \mathbb{C}^p \setminus \{0\}$ with $u_k v_k = 0$ and $\widehat{u}_k \widehat{v}_{-k} = 0$, $k = 0, 1, \ldots, p-1$.

This means that $\mathrm{supp}(u) \cap \mathrm{supp}(v) = \emptyset$ and $\mathrm{supp}(\widehat{u}) \cap (-\mathrm{supp}(\widehat{v})) = \emptyset$. In particular, we obtain $|\mathrm{supp}(u)| + |\mathrm{supp}(v)| \leq p$ and $|\mathrm{supp}(\widehat{u})| + |\mathrm{supp}(\hat{v})| \leq p$; and so,

$$|\mathrm{supp}(u)| + |\mathrm{supp}(v)| + |\mathrm{supp}(\widehat{u})| + |\mathrm{supp}(\widehat{v})| \leq 2p.$$

However, by Theorem 5.3, we have

$$|\mathrm{supp}(u)| + |\mathrm{supp}(v)| + |\mathrm{supp}(\widehat{u})| + |\mathrm{supp}(\widehat{v})| \geq 2(p+1),$$

and this gives the desired contradiction. □

6. Appendix – Real Hadamard matrices

Definition 6.1. A *real Hadamard matrix* is a square matrix whose entries are either $+1$ or -1 and whose rows are mutually orthogonal.

Let H be a real Hadamard matrix of order n. Then, the matrix

$$\begin{bmatrix} H & H \\ H & -H \end{bmatrix}$$

is a real Hadamard matrix of order $2n$. This observation can be applied repeatedly, as Kronecker products, to obtain the following sequence of real Hadamard matrices.

$$H_1 = \begin{bmatrix} 1 \end{bmatrix},$$

$$H_2 = \begin{bmatrix} H_1 & H_1 \\ H_1 & -H_1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

$$H_4 = \begin{bmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \cdots.$$

Thus,

$$\begin{aligned} H_{2^k} &= \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix} \\ &= \begin{bmatrix} H_{2^{k-2}} & H_{2^{k-2}} & H_{2^{k-2}} & H_{2^{k-2}} \\ H_{2^{k-2}} & -H_{2^{k-2}} & H_{2^{k-2}} & -H_{2^{k-2}} \\ H_{2^{k-2}} & H_{2^{k-2}} & -H_{2^{k-2}} & -H_{2^{k-2}} \\ H_{2^{k-2}} & H_{2^{k-2}} & -H_{2^{k-2}} & H_{2^{k-2}} \end{bmatrix}. \end{aligned} \tag{38}$$

This method of constructing real Hadamard matrices is due to Sylvester (1867) [59]. In this manner, he constructed real Hadamard matrices of order 2^k for every non-negative integer k.

Hadamard conjecture 1. The *Hadamard conjecture 1* is that a real Hadamard matrix of order $4k$ exists for every positive integer k [37]. Real Hadamard matrices of orders 12 and 20 were constructed by Hadamard in 1893 [33]. He also proved that if U is a unimodular matrix of order n, then $|\det(U)| \leqslant n^{n/2}$, with equality in the case U is real if and only if U is a real Hadamard matrix [33]. In 1933, Paley discovered a construction that produces a real Hadamard matrix of order $q+1$ when q is a prime power that is congruent to 3 modulo 4, and that produces a real Hadamard matrix of order $2(q+1)$ when q is a prime power that is congruent to 1 modulo 4 [47]. In fact, the Hadamard conjecture 1 should probably

be attributed to Paley. The smallest order that cannot be constructed by a combination of Sylvester's and Paley's methods is 92. A real Hadamard matrix of this order was found by computer by Baumert, Golomb, and Hall in 1962. They used a construction, due to Williamson, that has yielded many additional orders. In 2004, Hadi Kharaghani and Behruz Tayfeh-Rezaie constructed a real Hadamard matrix of order 428. As a result, the smallest order for which no real Hadamard matrix is presently known is 668.

Hadamard conjecture 2. If $x : \mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{R}$ is CAZAC sequence for $N \geq 2$, then the *Hadamard conjecture 2* asserts that $N = 4$ and x is a translate of the 4-tuple $\pm[1, 1, 1, -1]$. The conjecture goes back to Ryser [53]. From definitions it is straightforward to show that $N = 4M^2$. The major progress has been made by Turyn (1965), B. Schmidt (1999 and 2000), Leung, Ma, and B. Schmidt (2004), see [41]. They proved that the Hadamard conjecture 2 is true if M is a power of a prime greater than 3 as well as it being true for all $N \leq 10^{11}$.

Remark 6.2 (Finite abelian groups)**.** It is natural to pose the problems that we have considered about CAZAC sequences on $\mathbb{Z}/N\mathbb{Z}$ for the general case of finite Abelian groups, G. In fact, Gauss' theorem asserts that every such G can be written as

$$G = \mathbb{Z}/N_1\mathbb{Z} \times \cdots \mathbb{Z}/N_n\mathbb{Z},$$

where the N_j can be chosen as powers of primes. Beyond its purely mathematical interest, see [62], [27], this extension is important in coding theory, e.g., the analysis of bent functions and difference sets for the group $\mathbb{Z}/2\mathbb{Z}^n$ by Dillon (1975) and Rothaus (1976), independently, see, e.g., [23], [48], [54].

Remark 6.3 (Walsh functions and wavelet packets)**.** Hadamard matrices are closely connected with Walsh functions [3]. The normalized Walsh functions [67] form an orthonormal basis for $L^2(\mathbb{T})$. Every Walsh function is constant over each of a finite number of subintervals of $(0, 1)$. A set of Walsh functions written down in appropriate order as rows of a matrix will give a real Hadamard matrix of order 2^n as obtained by Sylvester's method. When Walsh functions are transported to the real line in the correct way, they not only provide an orthonormal basis for $L^2(\mathbb{R})$, but are the primordial example of wavelet packets using multiresolution analysis in wavelet theory, e.g., see [11].

Remark 6.4 (The Littlewood flatness problem and antenna theory)**.** Let $\mathcal{U}_N$ denote the class of unimodular trigonometric polynomials $U(\gamma) = \sum_{n=0}^{N} u_n\, e^{2\pi i n\gamma}$, i.e., $|u_n| = 1$ for $n = 0, \ldots, N$. The *Littlewood flatness problem* is to determine whether or not there are $U_N \in \mathcal{U}_N$ for which

$$\lim_{N\to\infty} \frac{\|U_N\|_\infty}{\|U_N\|_2} = 1. \tag{39}$$

It turns out that Gauss sums and their variants play a natural role in dealing with (39). There have been herculean efforts to prove (39), sometimes in concert with subtle failures only discovered by relatively herculean efforts. Finally, Kahane (1980) proved that such polynomials exist, but it still remains to construct them, see [50]. The ratio in (39) is the crest factor of U_N, and $\mathcal{U}_N$ combined with (39) play a role in antenna array signal processing where crest factors are analyzed, see [4] for details and references.

References

1. Louis Auslander and Paulo E. Barbano, *Communication codes and Bernoulli transformations*, Appl. Comput. Harmon. Anal. **5** (1998), no. 2, 109–128.

2. J. Backelin and Ralf Fröberg, *How we proved that there are exactly 924 cyclic 7–roots*, Proc. ISSAC1991, ACM Press (1991).
3. D. A. Bell, *Walsh functions and Hadamard matrices*, Electronics Letters **2** (1966), 340 – 341.
4. John J. Benedetto, *Harmonic Analysis and Applications*, Studies in Advanced Mathematics, CRC Press, Boca Raton, FL, 1997. MR MR1400886 (97m:42001)
5. John J. Benedetto, Robert L. Benedetto, and Joseph T. Woodworth, *Björck CAZACs and the discrete ambiguity function*, (2012), 62 pages, Technical Report.
6. John J. Benedetto, Robert L. Benedetto, and Joseph T. Woodworth, *Optimal ambiguity functions and Weil's exponential sum bound*, Journal of Fourier Analysis and Applications **18** (2012), no. 3, 471–487.
7. John J. Benedetto and Somantika Datta, *Construction of infinite unimodular sequences with zero autocorrelation*, Advances in Computational Mathematics **32** (2010), 191–207.
8. ———, *Constructions and a generalization of perfect autocorrelation sequences on Z*, Invited Chapter 8 in volume dedicated to Gil Walter. Editors X. Shen and A. Zayed (2012).
9. John J. Benedetto and Jeffrey J. Donatelli, *Ambiguity function and frame theoretic properties of periodic zero autocorrelation waveforms*, IEEE J. Special Topics Signal Processing **1** (2007), 6–20.
10. John J. Benedetto and Jeffrey J. Donatelli, *Frames and a vector-valued ambiguity function*, Asilomar Conference on Signals, Systems, and Computers, invited, October 2008.
11. John J. Benedetto and Michael Frazier (eds.), *Wavelets: Mathematics and applications*, Studies in Advanced Mathematics, CRC Press, Boca Ratan, FL, 1994.
12. John J. Benedetto, Ioannis Konstantinidis, and Muralidhar Rangaswamy, *Phase-coded waveforms and their design*, IEEE Signal Processing Magazine, invited **26** (2009), no. 1, 22–31.
13. Ingemar Bengtsson, Wojciech Bruzda, Asa Ericsson, Jan-Ak Larsson, Wojciech Tadej, and Karol Zyczkowski, *Mutually unbiased bases and Hadamard matrices of order six*, arXiv: quan-ph/0610161v3 (2007), 1–34.
14. Göran Björck, *Functions of modulus one on $\mathbf{Z}_p$ whose Fourier transforms have constant modulus*, A. Haar memorial conference, Vol. I, II (Budapest, 1985), Colloq. Math. Soc. János Bolyai, vol. 49, North-Holland, Amsterdam, 1987, pp. 193–197.
15. ———, *Functions of modulus one on $\mathbb{Z}_n$ whose Fourier transforms have constant modulus, and cyclic n-roots*, Proc. of 1989 NATO Adv. Study Inst. on Recent Advances in Fourier Analysis and its Applications, 1990, pp. 131–140.
16. Göran Björck and Ralf Fröberg, *A faster way to count the solutions of inhomogeneous systems of algebraic equations, with applications to cyclic n-roots*, Journal of Symbolic Computation **12** (1991), no. 3, 329–336.
17. Göran Björck and Ralf Fröberg, *Methods to "divide out" certain solutions from systems of algebraic equations, applied to find all cyclic 8 roots (Lulea 1992)*, Lecture Notes in Pure and Applied Math., Dekker, New York **156** (1994), 57–70.
18. Göran Björck and Bahman Saffari, *New classes of finite unimodular sequences with unimodular Fourier transforms. Circulant Hadamard matrices with complex entries*, C. R. Acad. Sci., Paris **320** (1995), 319 – 324.
19. Wojciech Bruzda, Wojciech Tadej, and Karol Zyczkowski, *Complex Hadamard matrices – a catalogue (since 2006)*, http://chaos.if.uj.edu.pl/ karol/hadamard/index.php h=0301.
20. Ole Christensen, *An Introduction to Frames and Riesz Bases, 2nd edition*, Springer-Birkhäuser, New York, 2016 (2003).
21. D. C. Chu, *Polyphase codes with good periodic correlation properties*, IEEE Transactions on Information Theory **18** (1972), 531–532.
22. Philip J. Davis, *Circulant Matrices*, Wiley, New York, 1970.
23. J. F. Dillon, *Elementary Hadamard difference sets*, Proc. 6th Southeast Conf. Comb., Graph Theory, and Comput., Boca Ratan, FL (1975), 237–249.
24. David L. Donoho and Philip B. Stark, *Uncertainty principles and signal recovery*, SIAM Journal on Applied Mathematics **49** (1989), no. 3, 906–931.
25. J. C. Faugère, *Finding all the solutions of cycli-9 using Gröbner basis techniques*, Computer Mathematics (Matsuyama 2001) Lecture Notes Ser. Comput. World Science Publ. **9** (2001), 1–12.
26. R. L. Frank and S. A. Zadoff, *Phase shift pulse codes with good periodic correlation properties*, IRE Trans. Inf. Theory, **8** (1962), 381–382.

27. John Gilbert and Ziemowit Rzeszotnik, *The norm of the Fourier transform on finite abelian groups*, Ann. Inst. Fourier, Grenoble **60** (2010), no. 4, 1317–1346.
28. Solomon W. Golomb and Guang Gong, *Signal Design for Good Correlation*, Cambridge University Press, 2005.
29. Karlheinz H. Gröchenig, *Foundations of Time-Frequency Analysis*.
30. Jiann-Ching Guey and Mark R. Bell, *Diversity waveform sets for delay-doppler imaging*, IEEE Transactions on Information Theory **44** (1998), no. 4, 1504–1522.
31. Uffe Haagerup, *Orthogonal maximal abelian $*$-subalgebras of the $n \times n$ matrices and cyclic n-roots*, Operator algebras and quantum field theory (Rome, 1996), Int. Press, Cambridge, MA, 1997, pp. 296–322.
32. ———, *Cyclic p-roots of prime length p and related complex Hadamard matrices*, arXiv: 0803.2629v1 (2008), 1–29.
33. Jacques Hadamard, *Résolution d'une question relative aux déterminants*, Bulletin des Sciences Mathématiques **17** (1893), 240– 246.
34. Godfrey H. Hardy and Edward M. Wright, *An Introduction to the Theory of Numbers*, fourth ed., Oxford University, Oxford, 1965.
35. Tor Helleseth and P. Vijay Kumar, *Sequences with low correlation*, Handbook of Coding Theory, Vol. I, II (Vera S. Pless and W. Cary Huffman, eds.), North-Holland, Amsterdam, 1998, pp. 1765–1853.
36. Matthew A. Herman and Thomas Strohmer, *High-resolution radar via compressed sensing*, IEEE Transactions on Signal Processing.
37. K. J. Horadam, *Hadamard Matrices and Their Applications*, Princeton University Press, Princeton, NJ, 2007.
38. John R. Klauder, *The design of radar signals having both high range resolution and high velocity resolution*, Bell System Technical Journal **39** (1960), 809–820.
39. John R. Klauder, A. C. Price, Sidney Darlington, and Walter J. Albersheim, *The theory and design of chirp radars*, Bell System Technical Journal **39** (1960), 745–808.
40. Irwin Kra and Santiago R. Simanca, *On circulant matrices*, Notices Amer. Math. Soc. **59** (2012), no. 3, 368–377.
41. K. H. Leung, S. L Ma, and B. Schmidt, *Non-existence of abelian difference sets: Lander's conjecture for prime power orders*, Trans. Amer. Math. Soc. **356** (2004), no. 11, 4343–4358.
42. Nadav Levanon and Eli Mozeson, *Radar Signals*, Wiley Interscience, IEEE Press, 2004.
43. M. L. Long, *Radar Reflectivity of Land and Sea*, Artech House, 2001.
44. Mark Magsino, *Constructing tight Gabor frames using CAZAC sequences*, Sampling Theory in Signal and Image Processing **16** (2017), 73–99.
45. Wai Ho 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.
46. F. E. Nathanson, *Radar Design Principles - Signal Processing and the Environment*, SciTech Publishing Inc., Mendham, NJ, 1999.
47. R. E. A. C. Paley, *On orthogonal matrices*, Journal of Mathematics and Physics **12** (1933), 311 –320.
48. V. S. Pless, W. C. Huffman, and R. A. Brualdi (eds.), *Handbook of coding theory. Vol. I, II*, North-Holland, Amsterdam, 1998.
49. Branislav M. Popovic, *Generalized chirp-like polyphase sequences with optimum correlation properties*, IEEE Transactions on Information Theory **38** (1992), no. 4, 1406–1409.
50. Hervé Queffelec and Bahman Saffari, *On bernstein's inequality and Kahane's ultraflat polynomials*, J. Fourier Analysis and Applications **2** (1996), 519–582.
51. Mark A. Richards, James A. Scheer, and William A. Holm (eds.), *Principles of Modern Radar*, SciTech Publishing, Inc., Raleigh, NC, 2010.
52. Walter Rudin, *Function Theory in the Unit Ball*, Springer Verlag, Gründlehren Series, Volume 241, New York, 1980.
53. H. J. Ryser, *Combinatorial Mathematics*, John Wiley and Sons, New York, 1963.
54. Bahman Saffari, *Some polynomial extremal problems which emerged in the twentieth century*, Twentieth century harmonic analysis—a celebration (Il Ciocco, 2000), NATO Sci. Ser. II Math. Phys. Chem., vol. 33, Kluwer Acad. Publ., Dordrecht, 2001, pp. 201–233.
55. Merrill I. Skolnik, *Introduction to Radar Systems*, McGraw-Hill Book Company, New York, 1980.

56. Kennan T. Smith, *The uncertainty principle on groups*, SIAM j. Applied. Math. **50** (1990), 876–882.
57. P. Stevenhagen and H. W. Lenstra, *Chebotarëv and his density theorem*, The Mathematical Intelligencer **18** (1996), no. 2, 26–37.
58. George W. Stimson, *Airborne Radar*, SciTech Publishing, Inc., Mendham, New Jersey, 1998.
59. J. J. Sylvester, *Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to newton's rule, ornamental tile-work, and the theory of numbers*, Philosophical Magazine **34** (1867), 461–475.
60. Wojcieh Tadej and Karol Zyczkowski, *A concise guide to complex Hadamard matrices*, Open Systems and Information Dynamics **13** (2006), 133–177.
61. Terence Tao, *An uncertainty principle for cyclic groups of prime order*, Mathematics Research Letters **12** (2005), 121–127.
62. Audrey Terras, *Fourier Analysis on Finite Groups and Applications*, no. 43, Cambridge University Press, 1999.
63. Richard J. Turyn, *Sequences with small correlation*, Error Correcting Codes (Proc. Sympos. Math. Res. Center, Madison, Wis., 1968), John Wiley, New York, 1968, pp. 195–228.
64. S. Ulukus and R. D. Yates, *Iterative construction of optimum signature sequence sets in synchronous CDMA systems*, IEEE Trans. Inform. Theory **47** (2001), no. 5, 1989–1998.
65. David E. Vakman, *Sophisticated Signals and the Uncertainty Principle in Radar*, Springer-Verlag, New York, 1969.
66. S. Verdú, *Multiuser Detection*, Cambridge University Press, Cambridge, UK, 1998.
67. Joseph L. Walsh, *A closed set of normal orthogonal functions*, American Journal of Mathematics **45** (1923), 5–24.
68. Philip M. Woodward, *Probability and Iinformation Theory, with Aapplications to Radar*, Pergamon Press, Oxford.
69. _____, *Theory of radar information*, IEEE Transactions on Information Theory **1** (1953), no. 1, 108–113.

Norbert Wiener Center, Department of Mathematics, University of Maryland, College Park, MD 20742, USA
E-mail address: jjb@math.umd.edu
URL: http://www.math.umd.edu/~jjb

Norbert Wiener Center, Department of Mathematics, University of Maryland, College Park, MD 20742, USA

Norbert Wiener Center, Department of Mathematics, University of Maryland, College Park, MD 20742, USA