Constructions and a generalization of perfect autocorrelation sequences on $\mathbb{Z}$

John J. Benedetto and Somantika Datta
Dedicated to Gil Walter on the occasion of his 80th birthday

Abstract Low autocorrelation signals have fundamental applications in radar and communications. We construct constant amplitude zero autocorrelation (CAZAC) sequences x on the integers $\mathbb{Z}$ by means of Hadamard matrices. We then generalize this approach to construct unimodular sequences x on $\mathbb{Z}$ whose autocorrelations A_x are building blocks for all functions on $\mathbb{Z}$. As such, algebraic relations between A_x and A_y become relevant. We provide conditions for the validity of the formulas $A_{x+y} = A_x + A_y$.

1 Introduction

1.1 Background

Let $\mathbb{R}$ be the real numbers, let $\mathbb{Z}$ be the integers, and set $\mathbb{T} = \mathbb{R}/\mathbb{Z}$. A general problem is to characterize the family of positive bounded Radon measures F, whose inverse Fourier transforms are the autocorrelations of bounded sequences x. A special case is when $F \equiv 1$ on $\mathbb{T}$ and x is unimodular on $\mathbb{Z}$. The statement that $F \equiv 1$ is the same as saying that the autocorrelation of x vanishes except at 0, where it takes the value 1. We shall construct such unimodular sequences x based on the analysis of Hadamard matrices.

The problem of constructing unimodular sequences with zero autocorrelation, which our constructions address, is central in the general area of waveform design, and it is particularly relevant in several applications in the areas of radar and com-

John J. Benedetto
Norbert Wiener Center, Department of Mathematics, University of Maryland, College Park, MD 20742, e-mail: jjb@math.umd.edu

Somantika Datta
Department of Mathematics, University of Idaho, Moscow, ID 83844, e-mail: sdatta@uidaho.edu

munications, and in the general area of constructing phase coded waveforms on $\mathbb{R}$ with optimal narrow band ambiguity function behavior. In radar, the sequences x can play a role in effective target recognition, see, e.g., [1], [9], [15], [20], [21], [22], [23], [28]; and in communications they can be used to address synchronization issues in cellular (phone) access technologies, especially code division multiple access (CDMA), e.g., [30], [31], [32]. With regard to the narrow band ambiguity function we refer to [5], [6], [20], [25], which in turn refer to the vast literature in this subject.

In radar there are two main reasons that the sequences x should be unimodular, that is, have constant amplitude. 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 autocorrelation property ensures minimum interference between signals sharing the same channel.

1.2 Autocorrelation

We shall use the standard notation from harmonic analysis, e.g., [4], [27]. $\mathbb{N}$ is the set of natural numbers and $\mathbb{C}$ is the set of complex numbers. $C(\mathbb{T}^d)$ is the space of $\mathbb{C}$-valued continuous functions on $\mathbb{T}^d = \mathbb{R}^d/\mathbb{Z}^d$, and $A(\mathbb{T}^d)$ is the subspace of absolutely convergent Fourier series. $M(\mathbb{T}^d)$ is the space of bounded Radon measures on $\mathbb{T}^d$, i.e., $M(\mathbb{T}^d)$ is the dual space of the Banach space $C(\mathbb{T}^d)$ taken with the sup norm. $L^1(\mathbb{T})$ and $L^2(\mathbb{T})$ are the spaces of integrable and square integrable functions on $\mathbb{T}$, respectively. For a given $\lambda > 0$, the L^1-dilation of f, f_λ, is defined as $f_\lambda(t) = \lambda f(\lambda t)$. Let $\triangle(t) = \max(1-|t|,0)$ on $\mathbb{R}$. Let $\omega(\gamma) = \frac{1}{2\pi}\left(\frac{\sin\gamma/2}{\gamma/2}\right)^2$; ω is called the *Fejér function* [4]. The Fourier transform of $f \in L^1(\mathbb{R})$ is the function $\widehat{f}$ defined by

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

$A(\widehat{\mathbb{R}})$ denotes the space of such absolutely convergent Fourier transforms on $\widehat{\mathbb{R}}$, with an analogous definition for $A(\widehat{\mathbb{R}}^d)$. We write the pairing between the function f and $\widehat{f}$ as $f \leftrightarrow \widehat{f}$. The Fourier transform of $\triangle$ is $\omega_{2\pi}$. The complex conjugate of a function f at a point t is denoted by $\overline{f(t)}$. For a set E, the measure of E is denoted by $|E|$. Given two sets A and B, the set $A \setminus B$ consists of all elements in A that are not in B.

Definition 1. The *autocorrelation* $A_x : \mathbb{Z} \to \mathbb{C}$ of $x : \mathbb{Z} \to \mathbb{C}$ is formally defined as

$$\forall k \in \mathbb{Z}, \quad A_x[k] = \lim_{N\to\infty} \frac{1}{2N+1} \sum_{m=-N}^{N} x[k+m]\overline{x[m]}.$$

(Lower case Roman letters, such as x, are often used in some applied communities to denote functions $\mathbb{Z} \to \mathbb{C}$.) There is an analogous definition of autocorrelation for functions $f : \mathbb{R}^d \to \mathbb{C}$, e.g., see Theorem 1.

If $F \in A(\mathbb{T}^d)$ we write $\check{F} = f = \{f_k\}$, i.e., $\check{F}[k] = f_k$, where, for all $k \in \mathbb{Z}^d$, $f_k = \int_{\mathbb{T}^d} F(\gamma) e^{2\pi i k\cdot\gamma} d\gamma$. There is a similar definition for $\check{\mu}$ where $\mu \in M(\mathbb{T}^d)$, e.g., see Theorem 1.

In the setting of $\mathbb{R}$, we have the following theorem due to Wiener and Wintner [36], which was later extended to $\mathbb{R}^d$ in [3], [18].

Theorem 1. *Let μ be a bounded positive Radon measure on $\mathbb{R}$. There is a constructible function $f \in L^\infty_{loc}(\mathbb{R})$ whose autocorrelation A_f exists for all $t \in \mathbb{R}$, and $A_f = \check{\mu}$ on $\mathbb{R}$, i.e.,*

$$\forall t \in \mathbb{R}, \quad \lim_{T\to\infty} \frac{1}{2T} \int_{-T}^{T} f(t+x)\overline{f(x)} dx = \int_{\mathbb{R}} e^{2\pi i t x} d\mu(x).$$

For any positive integer N, we denote the d-dimensional square in $\mathbb{Z}^d$ by $S(N)$, i.e.,

$$S(N) = \{\mathbf{m} = (m_1, m_2, \cdots, m_d) \in \mathbb{Z}^d : -N \leqslant m_i \leqslant N, i = 1, \cdots, d\}.$$

On $\mathbb{Z}^d$ the following version of the Wiener-Wintner theorem can be obtained [12].

Theorem 2. *Let $\mu \in A(\mathbb{T}^d)$ be positive on $\mathbb{T}^d$. There is a constructible function $x : \mathbb{Z}^d \to \mathbb{C}$ such that*

$$\begin{aligned} \forall \mathbf{k} \in \mathbb{Z}^d,\ A_x[\mathbf{k}] &= \lim_{N\to\infty} \frac{1}{(2N+1)^d} \sum_{\mathbf{m}\in S(N)} x[\mathbf{k}+\mathbf{m}]\overline{x[\mathbf{m}]} \\ &= \check{\mu}[\mathbf{k}]. \end{aligned} \tag{1}$$

Although the Wiener-Wintner theorem gives the construction of the function x it does not ensure boundedness of x. In fact, x need not be an element of $\ell^\infty(\mathbb{Z})$ [19]. Our desire is to construct sequences x that have constant amplitude.

Let $\lambda \in (0,1)$ have the binary expansion $0.\alpha_1\alpha_2\alpha_3\cdots$, where each α_i is either 0 or 1. It has been shown in [34], [35] that if we consider the Lebesgue measure on $(0,1)$ and if we define the unimodular (in fact, ± 1-valued) function y by

$$y[k] = \begin{cases} 2\alpha_{2n+1} - 1 & \text{if } k = n+1,\ n \in \mathbb{N}\cup\{0\}, \\ 2\alpha_{2n} - 1 & \text{if } k = 1-n,\ n \in \mathbb{N}, \end{cases} \tag{2}$$

then, for *almost all* values of λ, the autocorrelation of y, A_y, is

$$A_y[k] = \begin{cases} 0 & \text{if } k \neq 0, \\ 1 & \text{if } k = 0. \end{cases} \tag{3}$$

Thus, A_y is the inverse Fourier transform of $F \equiv 1$ on $\mathbb{T}$. Here Lebesgue measure on (0, 1) is the probability measure ([12], page 77).

The expression (3) defines a sequence y having *perfect autocorrelation*. An explicit or deterministic construction of such a unimodular sequence on $\mathbb{Z}$ is given in [34], where the sequence consists of ± 1s. Inspired by that we propose a different class of deterministic unimodular sequences with perfect autocorrelation that are constructed from real Hadamard matrices. In fact, an extensive generalization of such constructions can be found in [8].

Definition 2. (a) Let $\mathbb{Z}/N\mathbb{Z}$ be the finite group $\{0,1,\ldots,N-1\}$ with addition modulo N. We say that $x : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ is a *constant amplitude zero autocorrelation* (CAZAC) sequence if $|x[k]| = 1$ for each $k \in \mathbb{Z}/N\mathbb{Z}$ and if

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

(b) Given $x : \mathbb{Z} \to \mathbb{C}$. The sequence x is a CAZAC sequence on $\mathbb{Z}$ if $|x[k]| = 1$ for each $k \in \mathbb{Z}$ and if $A_x[k] = 0$ for each $k \in \mathbb{Z}\backslash\{0\}$.

1.3 Outline

In Section 2.1, we review properties and problems related to Hadamard matrices. This serves as background for Section 2.2, where we establish the relation between CAZAC sequences on $\mathbb{Z}/N\mathbb{Z}$, Hadamard matrices, and the discrete Fourier transform. Then, in Section 2.3, we construct CAZAC sequences on $\mathbb{Z}$ by means of Hadamard matrices. Section 3 is devoted to extending the material of Section 2 in the following way. In Section 3.1 we construct unimodular functions on $\mathbb{Z}$ whose autocorrelations are triangles; and we view this as a generalization of the construction of CAZACs on $\mathbb{Z}$. It is natural to think of such triangles as building blocks of the functions on $\mathbb{Z}$. As such, Section 3.2 is devoted to the formula $A_{x+y} = A_x + A_y$, and we prove its validity a.e.

2 Hadamard matrices and CAZAC sequences

2.1 Hadamard matrices

Definition 3. 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 Hadamard matrix of order n. Then, the matrix

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

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

$$\begin{aligned} H_{2^k} &= \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix} \\ &= \begin{bmatrix} H_{2^{k-2}} & H_{2^{k-2}} & H_{2^{k-2}} & H_{2^{k-2}} \\ H_{2^{k-2}} & -H_{2^{k-2}} & H_{2^{k-2}} & -H_{2^{k-2}} \\ H_{2^{k-2}} & H_{2^{k-2}} & -H_{2^{k-2}} & -H_{2^{k-2}} \\ H_{2^{k-2}} & H_{2^{k-2}} & -H_{2^{k-2}} & H_{2^{k-2}} \end{bmatrix}. \end{aligned} \tag{4}$$

This method of constructing Hadamard matrices is due to Sylvester (1867) [29]. In this manner, he constructed Hadamard matrices of order 2^k for every non-negative integer k.

The most important open question in the theory of Hadamard matrices is that of existence. The *Hadamard conjecture* asserts that a Hadamard matrix of order $4N$ exists for every positive integer N [16]. Hadamard matrices of orders 12 and 20 were constructed by Hadamard in 1893 [14]. He also proved that if U is a unimodular matrix of order N, then $|\det(U)| \leq N^{N/2}$, with equality in the case U is real if and only if U is Hadamard [14]. In 1933, Paley discovered a construction that produces a Hadamard matrix of order $q+1$ when q is any prime power that is congruent to 3 modulo 4, and that produces a Hadamard matrix of order $2(q+1)$ when q is a prime power that is congruent to 1 modulo 4 [24]. His method uses finite fields. The Hadamard conjecture 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 Hadamard matrix of this order was found using a 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 announced that they constructed a Hadamard matrix of order 428. As a result, the smallest order for which no Hadamard matrix is presently known is 668.

Hadamard matrices are closely connected with Walsh functions [2], [26]. The Walsh functions, constructed by J. Walsh [33], are 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 Hadamard matrix of order 2^N as obtained by Sylvester's method.

The Walsh functions defined on $\mathbb{R}$ correspond to the wavelet packets associated with the Haar multiresolution analysis.

2.2 CAZACs and circulant Hadamard matrices

An $N \times N$ matrix A of the form

$$A = \begin{bmatrix} a_1 & a_2 & a_3 & \cdots & a_N \\ a_N & a_1 & a_2 & \cdots & a_{N-1} \\ a_{N-1} & a_N & a_1 & \cdots & a_{N-2} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ a_2 & a_3 & \cdots & a_N & a_1 \end{bmatrix}$$

is called a circulant matrix [17]. Each row is just the previous row cycled forward by one step, so that the entries in each row are just a cyclic permutation of those in the first. There is a characterization of CAZAC sequences in terms of circulant Hadamard matrices with complex entries, see Theorem 4, e.g., [10]. For any finite sequence $x = (x[0], x[1], \ldots, x[N-1])$ of N complex numbers $(N \geq 1)$, its *normalized discrete Fourier transform* $\hat{x} = (\hat{x}[0], \hat{x}[1], \ldots, \hat{x}[N-1])$ is defined by

$$\hat{x}[j] = N^{-\frac{1}{2}} \sum_{k=0}^{N-1} x[k] e^{-2\pi i k j/N} \quad (j = 0, 1, \ldots, N-1).$$

By Parseval's relation,

$$\sum_{k=0}^{N-1} |x[k]|^2 = \sum_{j=0}^{N-1} |\hat{x}[j]|^2.$$

It is easy to see that x is CAZAC if and only if x and $\hat{x}$ are unimodular (Corollary 1). This fact is a consequence of the following result.

Theorem 3. *Let $x : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ be the sequence $x = (x[0], x[1], \ldots, x[N-1])$. The condition,*

$$\forall m = 1, \ldots, N-1, \quad \frac{1}{N} \sum_{k=0}^{N-1} x[m+k]\overline{x[k]} = 0, \tag{5}$$

is valid if and only if there is a constant c such that $|\hat{x}| = c$ on $\mathbb{Z}/N\mathbb{Z}$.

Proof. (i) Suppose that $|\hat{x}| = c$ on $\mathbb{Z}/N\mathbb{Z}$. Then, for each $j \in \mathbb{Z}/N\mathbb{Z}$,

$$|\hat{x}[j]|^2 = \frac{1}{N} \sum_{k=0}^{N-1} |x[k]|^2 + \frac{1}{N} \sum_{k \neq \ell} x[k]\overline{x[\ell]} e^{-2\pi i (k-\ell) j/N},$$

and so

$$N|\hat{x}[j]|^2 = \sum_{k=0}^{N-1} |x[k]|^2 + \sum_{k \neq \ell} x[k]\overline{x[\ell]} e^{-2\pi i (k-\ell) j/N}.$$

Thus, by hypothesis, we have $N|\hat{x}[j]|^2 = \sum_{n=0}^{N-1} |\hat{x}[n]|^2$ $(= Nc^2)$, and so

$$\sum_{n=0}^{N-1} |\hat{x}[n]|^2 = \sum_{k=0}^{N-1} |x[k]|^2 + \sum_{k\neq\ell} x[k]\overline{x[\ell]}e^{-2\pi i(k-\ell)j/N}.$$

Hence, by Parseval's identity, we have

$$\forall j \in \mathbb{Z}/N\mathbb{Z}, \quad \sum_{k\neq\ell} x[k]\overline{x[\ell]}e^{-2\pi i(k-\ell)j/N} = 0. \tag{6}$$

Fix $k \in \{0,1,\ldots,N-1\}$ and let $m = k-\ell \pmod N$. Then, (6) becomes

$$\sum_{m=1}^{N-1}\sum_{\ell=0}^{N-1} x[\ell+m]\overline{x[\ell]}e^{-2\pi imj/N} = 0. \tag{7}$$

In particular, there are N^2-N terms in the sum of (6) since we exclude the diagonal of an $N\times N$ array. For compatibility, for each m there are N terms in (7), and since there are $N-1$ values of m we see that there are N^2-N terms in the sum of (7). Now let $f[m] = \sum_{\ell=0}^{N-1} x[\ell+m]\overline{x[\ell]}$. Then (7) becomes

$$\forall j \in \mathbb{Z}/N\mathbb{Z}, \quad \sum_{m=1}^{N-1} f[m]e^{-2\pi imj/N} = 0. \tag{8}$$

Multiplying both sides of (8) by $e^{2\pi ikj/N}$, for a fixed $k \in \{0,1,\ldots,N-1\}$, we have

$$\forall j \in \mathbb{Z}/N\mathbb{Z}, \quad \sum_{m=1}^{N-1} f[m]e^{-2\pi i(m-k)j/N} = 0,$$

and so

$$\sum_{m=1}^{N-1} f[m]\left(\sum_{j=0}^{N-1} e^{-2\pi i(m-k)j/N}\right) = 0 \tag{9}$$

for every fixed $k \in \{0,1,\ldots,N-1\}$. Since

$$\sum_{j=0}^{N-1} e^{-2\pi i(m-k)j/N} = \begin{cases} N, & k=m, \\ \frac{e^{-2\pi i(m-k)}-1}{e^{-2\pi i(m-k)/N}-1} = 0, & k\neq m, \end{cases}$$

and since $m \in \{1,\ldots,N-1\}$, equation (9) allows us to assert that $f[m]=0$ for each $m \in \{1,\ldots,N-1\}$. In fact, for any fixed $k \in \{1,\ldots,N-1\}$, the left side of (9) becomes $Nf[k]$, and so $f[k]=0$ by the right side of (9).
(ii) The converse is proved by retracing the steps of (i). □

Corollary 1. *Let $x : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ be the unimodular sequence $x = (x[0],x[1],\ldots,x[N-1])$. The sequence x is a CAZAC sequence if and only if $\hat{x}$ is a unimodular sequence.*

Proof. If x is a CAZAC sequence then (5) is valid and so $|\hat{x}| = c$ by Theorem 3. By Parseval's relation,

$$\sum_{j=0}^{N-1} |\hat{x}[j]|^2 = \sum_{k=0}^{N-1} |x[k]|^2$$
$$\text{or,} \quad Nc^2 = N$$

where in the last step we use the fact that x is unimodular. Thus the constant c is equal to 1 and $\hat{x}$ is a unimodular sequence. The converse follows by retracing this proof. □

Definition 4. A complex Hadamard matrix is a square matrix whose entries are unimodular and whose rows are mutually orthogonal.

We have the following characterization of CAZAC sequences in terms of circulant Hadamard matrices with complex entries.

Theorem 4. *Given a sequence $x : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$, and let H_x be 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.*

Proof.

$$H_x = \begin{bmatrix} x[0] & x[1] & \cdots & x[N-1] \\ x[N-1] & x[0] & \cdots & x[N-2] \\ \vdots & \vdots & \cdots & \vdots \\ x[1] & x[2] & \cdots & x[0] \end{bmatrix}, \quad H_x^* = \begin{bmatrix} \overline{x[0]} & \overline{x[N-1]} & \cdots & \overline{x[1]} \\ \overline{x[1]} & \overline{x[0]} & \cdots & \overline{x[2]} \\ \vdots & \vdots & \cdots & \vdots \\ \overline{x[N-1]} & \overline{x[N-2]} & \cdots & \overline{x[0]} \end{bmatrix}.$$

(i) Assume that H_x is a complex Hadamard matrix. Hence, all of the entries of H_x are unimodular and

$$H_x H_x^* = N I_N \tag{10}$$

where I_N is the $N \times N$ identity matrix. As a consequence of (10) one has for $m = 1, \ldots, N-1$,

$$\sum_{\ell=0}^{N-1} x[\ell + m]\overline{x[\ell]} = 0$$

which means that x has zero autocorrelation and is thus a CAZAC.
(ii) Conversely, suppose that x is a CAZAC. We want to show that H_x is a Hadamard matrix. We already know that all the entries of H_x are unimodular since x is unimodular and the entries of H_x are the elements of x. We want to show that $H_x H_x^* = N I_N$. Due to unimodularity

$$\sum_{\ell=0}^{N-1} |x[\ell]|^2 = N \tag{11}$$

and so the diagonal entries of $H_x H_x^*$ equal N as required. Since x is CAZAC,

$$\sum_{\ell=0}^{N-1} x[\ell+m]\overline{x[\ell]} = 0$$

for $m \neq 0$, which means that every off-diagonal entry of $H_x H_x^*$ equals zero and this together with (11) implies that $H_x H_x^*$ is a Hadamard matrix. □

Due to this characterization of CAZACs there is a basic relation between CAZACs and *finite unit normed tight frames* (FUNTFs) in $\mathbb{C}^d$. We shall say that $x : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}^d$ is a CAZAC sequence in $\mathbb{C}^d$ if each $\|x[k]\| = 1$ and

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

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

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

The norm of each $x[k]$ is then $\|x[k]\| = \langle x[k], x[k]\rangle^{1/2}$. For fundamentals on frame theory we refer to [11] or [13]. The following has been shown in [9].

Theorem 5. *Let $x = \{x[n]\}_{n=1}^N$ be a CAZAC sequence in $\mathbb{C}$. Define*

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

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

2.3 CAZACs and Hadamard sequences

In this section we construct infinite CAZAC sequences, i.e., CAZAC sequences on $\mathbb{Z}$, from real Hadamard matrices. Two different constructions are given. For the proofs of Theorem 6 and Theorem 7 we refer the readers to [8].

Example 1. To construct a unimodular sequence x, let H_1 be repeated once ($2^0 = 1$), H_2 be repeated twice (2^1), H_4 be repeated 2^2 times, H_8 be repeated 2^3 times, and, in general, let H_{2^n} be repeated 2^n times. For the positive integers, let x take values row by row from the elements of the sequence of matrices

$$H_1, H_2, H_2, H_4, H_4, H_4, H_4, H_8, \cdots. \tag{12}$$

Set $x[0] = 1$ and, for any $k \in \mathbb{N}$, define $x[-k] = x[k]$. The sequence x is called the *exponential Hadamard sequence.*

Theorem 6. *Let x be the exponential Hadamard sequence. Then,*

$$A_x[k] = \begin{cases} 1 \text{ if } k = 0, \\ 0 \text{ if } k \neq 0. \end{cases}$$

Instead of having the Hadamard matrices repeat exponentially as described in Example 1, we can construct unimodular sequences, whose autocorrelations vanish everywhere expect at the origin, by letting the Hadamard matrices repeat linearly.

Example 2. To construct the linear Hadamard sequence x, let H_1 be repeated zero times, H_2 be repeated once, H_4 be repeated twice, H_8 be repeated thrice, and, in general, let H_{2^n} be repeated n times. For the positive integers, let x take values row by row from the elements of the sequence of matrices

$$H_2, H_4, H_4, H_8, H_8, H_8, H_{16}, H_{16}, H_{16}, H_{16}, H_{32}, \cdots.$$

Set $x[0] = 1$, and, for any $k \in \mathbb{N}$, define $x[-k] = x[k]$. The sequence x is called the *linear Hadamard sequence.*

The proof of the following result is similar to that of Theorem 6.

Theorem 7. *Let x be the linear Hadamard sequence. Then,*

$$A_x[k] = \begin{cases} 1 \text{ if } k = 0, \\ 0 \text{ if } k \neq 0. \end{cases}$$

These two constructions are more general than they appear. For example, instead of $H_1 = [1]$ one could start with $H_1 = [-1]$ and obtain the following sequence of Hadamard matrices.

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

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

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

Using this sequence of Hadamard matrices in Example 1 or Example 2 would give a different sequence x but one which would still have perfect autocorrelation.

Example 3. In practice, for applications, we cannot use an infinite sequence and we would like to estimate the number of elements of the sequences in Examples 1 and 2 that can be used to make the corresponding autocorrelation reasonably small. In other words, we would like to solve the following problem: given $\varepsilon > 0$, find $N \in \mathbb{N}$ such that

$$\forall k \in \mathbb{Z}, \quad \left| \frac{1}{N} \sum_{m=1}^{N} x[m+k]x[m] \right| < \varepsilon.$$

Let x be the exponential Hadamard sequence of Example 1. Let $\varepsilon > 0$ and $K \in \mathbb{N}$. The smallest N such that

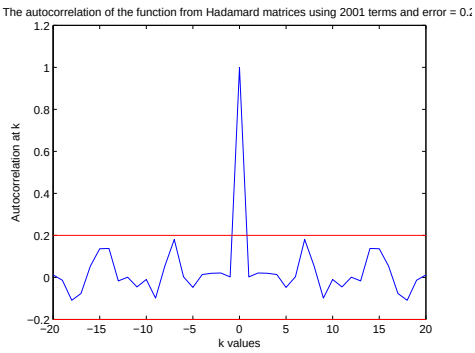

Fig. 1 Error estimates of the exponential Hadamard sequence; $\varepsilon = 0.2$.

$$\forall\, 0 < |k| \leq K, \quad \left| \frac{1}{N} \sum_{m=1}^{N} x[m+k]x[m] \right| < \varepsilon$$

satisfies the inequality

$$\frac{1}{N} \frac{8^{\lceil \log_2(K) \rceil + 1} - 1}{7} + 7 \frac{1}{2^{M+1}} < \varepsilon, \tag{13}$$

where M is a function of N. For more information about the relationship between M and N we refer to [8], [12].

(14) gives the values of N obtained via (13) for $K = 16$ and several values of ε.

ε	1	.5	.25	.1
K	16	16	16	16
M	14	15	16	17
N	$O(8^{15})$	$O(8^{16})$	$O(8^{17})$	$O(8^{18})$

(14)

The actual error estimate for the exponential Hadamard sequence is illustrated in Figure 1. This estimate is significantly better than that obtained in (13). The disparity is a consequence of the difficult counting problems inherent in dealing with Hadamard matrices. However, Figure 1 does imply a valid use of these sequences in applications.

Next let x be the linear Hadamard sequence of Example 2. Given $\varepsilon > 0$ and $K \in \mathbb{N}$. The smallest N such that

$$\forall\, 0 < |k| \leq K, \quad \left| \frac{1}{N} \sum_{m=1}^{N} x[m+k]x[m] \right| < \varepsilon$$

satisfies the inequality

$$\frac{(3\lceil \log_2(K) \rceil - 1)4^{\lceil \log_2(K) \rceil + 1} + 4 + 9 \cdot 4^{M+1}}{3M4^{M+1} - 4(4^M - 1)} < \varepsilon, \tag{15}$$

where M is a function of N.

(16) gives the values of N obtained from (15) for $K = 16$ and several values of ε. Once again, Figure 2 illustrates that the actual error estimates are much better than that obtained in (15).

ε	1	.5	.25	.1
K	16	16	16	16
M	5	7	13	31
N	35048	735464	5.16×10^9	7.97×10^{20}

(16)

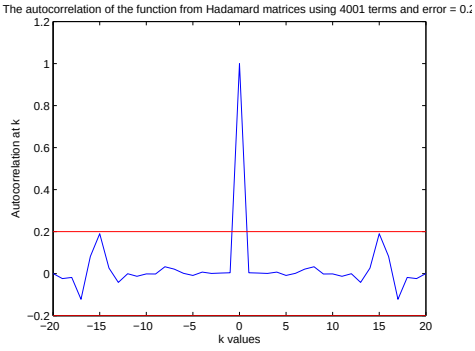

Fig. 2 Error estimates of the linear Hadamard sequence; $\varepsilon = 0.2$.

3 Autocorrelations as sums of triangles

3.1 The construction of sequences with triangular autocorrelation

In this section a generalization of (3), the autocorrelation function of the sequence given by (2), and of those constructed from Hadamard matrices in Section 2.3 and also in [8] is given.

Theorem 8. *Given $M \in \mathbb{N}$ and $K > 0$. Let $A : \mathbb{Z} \to \mathbb{R}$ be defined by*

$$A[k] = \begin{cases} K\left(1 - \frac{|k|}{M}\right) & \text{if } 0 \le |k| \le M, \\ 0 & \text{otherwise.} \end{cases} \tag{17}$$

Then there exists a constructible sequence $x : \mathbb{Z} \to \mathbb{R}$ with constant amplitude $\sqrt{K}$ whose autocorrelation, A_x, is A.

Proof. (i) As mentioned in Section 1.2 one can deterministically construct a unimodular sequence y on $\mathbb{Z}$ whose autocorrelation is

$$A_y[k] = \begin{cases} 0 & \text{if } k \neq 0, \\ 1 & \text{if } k = 0, \end{cases} \tag{18}$$

and we use (18) at the end of the proof. Wiener's construction [34] of y is as follows. On the positive integers let y take values in the following order:
$[1,-1]$ (this row has $1 \cdot 2^1$ elements and is repeated $2^0 = 1$ time);
$[1,1;1,-1;-1,1;-1,-1]$ (this row has $2 \cdot 2^2$ elements and is repeated $2^1 = 2$ times);
$[1,1,1;1,1,-1;1,-1,1;1,-1,-1;-1,1,1;-1,1,-1;$
$-1,-1,1;-1,-1,-1]$ (this row has $3 \cdot 2^3$ elements and is repeated $2^2 = 4$ times); etc. Thus, $y[1] = 1, y[2] = -1, y[3] = 1, y[4] = 1, \ldots$. In addition, let $y[0] = 1$, and, for $k \in \mathbb{N}$, let $y[-k] = y[k]$.

(ii) We define the function $x : \mathbb{Z} \to \mathbb{C}$ by $x[k] = \sqrt{K} y[\lceil \frac{k}{M} \rceil]$, where $\lceil . \rceil$ denotes the next largest integer. Note that $|x| = \sqrt{K}$.

We show that the autocorrelation A_x of x is A as defined in (17). Since x is a real sequence, the autocorrelation function is even, and so it is enough to prove the result for $k > 0$. Let $0 \le Mp \le k \le M(p+1)$ for some $p \in \mathbb{N} \cup \{0\}$. For any given integer N, let n_N be the smallest integer such that $N < M(n_N + 1)$. Then we have

$$\begin{aligned} A_x[k] &= \lim_{N\to\infty} \frac{1}{2N+1} \sum_{m=-N}^{N} x[m+k]\overline{x[m]} \\ &= \lim_{N\to\infty} \frac{1}{2N+1} \sum_{m=-Mn_N}^{Mn_N} x[k+m]x[m] + \lim_{N\to\infty} \frac{1}{2N+1} \sum_{Mn_N < |m| \le N} x[m+k]x[m] \\ &= \lim_{N\to\infty} (S_{1,N}(k) + S_{2,N}(k)) = S_1(k) + S_2(k). \end{aligned} \tag{19}$$

First, we calculate bounds on $S_{2,N}(k)$.

$$|S_{2,N}(k)| = \left| \frac{1}{2N+1} \sum_{Mn_N<|m|\leq N} x[m+k]x[m] \right|$$
$$\leq \frac{1}{2N+1} \sum_{Mn_N<|m|\leq N} |x[m+k]x[m]| = \frac{K}{2N+1} \sum_{Mn_N<|m|\leq N} 1 = \frac{2K(N-Mn_N)}{2N+1}.$$

We know from the definition of n_N that $N - Mn_N < M$. Therefore, $S_2(k) = 0$. Consequently, $A_x[k] = \lim_{N\to\infty} S_{1,N}(k) = S_1(k)$. Next, we write

$$S_1(k) = \lim_{N\to\infty} \frac{1}{2N+1} \sum_{m=-Mn_N}^{Mn_N} x[k+m]x[m]$$
$$= \lim_{N\to\infty} \frac{1}{2N+1} \sum_{n=-n_N}^{n_N-1} \sum_{m=Mn+1}^{M(n+1)} x[k+m]x[m] + \lim_{N\to\infty} \frac{1}{2N+1} x[-n_N+k]x[-n_N]. \tag{20}$$

Since x has the same value $\sqrt{K}y[n+1]$ for all the integers $m \in [Mn+1, M(n+1)]$, one can replace the $x[m]$ in the first term of the right side of (20) by $\sqrt{K}y[n+1]$. Since the second term of the right side of (20) is 0 this implies

$$S_1(k) = \lim_{N\to\infty} \frac{1}{2N+1} \sum_{n=-n_N}^{n_N-1} \sum_{m=Mn+1}^{M(n+1)} x[m+k]\sqrt{K}y[n+1]$$
$$= \lim_{N\to\infty} \frac{1}{2N+1} \left(\sum_{n=-n_N}^{n_N-1} \sum_{m=Mn+1}^{Mn+M(p+1)-k} x[m+k]\sqrt{K}y[n+1] \right.$$
$$\left. + \sum_{n=-n_N}^{n_N-1} \sum_{Mn+M(p+1)-k+1}^{M(n+1)} x[m+k]\sqrt{K}y[n+1] \right)$$
$$= \lim_{N\to\infty} \frac{K}{2N+1} \sum_{n=-n_N}^{n_N-1} \left(\sum_{m=Mn+1}^{Mn+M(p+1)-k} y[n+p+1]y[n+1] \right.$$
$$\left. + \sum_{m=Mn+M(p+1)-k+1}^{M(n+1)} y[n+p+2]y[n+1] \right)$$
$$= \lim_{N\to\infty} \frac{K}{2N+1} \sum_{n=-n_N}^{n_N-1} \big((M(p+1)-k)y[n+p+1]y[n+1]$$
$$+ (k-Mp)y[n+p+2]y[n+1] \big)$$

$$= \lim_{N\to\infty} \frac{M(p+1)-k}{2N+1} \frac{2n_N K}{2n_N} \sum_{n=-n_N}^{n_N-1} y[n+p+1]y[n+1] +$$
$$+ \lim_{N\to\infty} \frac{(k-Mp)}{2N+1} \frac{2n_N K}{2n_N} \sum_{n=-n_N}^{n_N-1} y[n+p+2]y[n+1].$$

Since $n_N \to \infty$ as $N \to \infty$, we have

$$\lim_{N\to\infty} S_{1,N}(k) = \lim_{N\to\infty} \frac{M(p+1)-k}{2N+1} 2n_N K A_y[p] + \lim_{N\to\infty} \frac{k-Mp}{2N+1} 2n_N K A_y[p+1]$$
$$= \lim_{N\to\infty} \left(p+1-\frac{k}{M}\right) \frac{2n_N M}{2N+1} K A_y[p] \tag{21}$$
$$+ \lim_{N\to\infty} \left(\frac{k}{M}-p\right) \frac{2n_N M}{2N+1} K A_y[p+1].$$

Note that

$$\lim_{N\to\infty} \frac{2n_N M}{2N+1} = 1. \tag{22}$$

In fact, from the choice of n_N, we have $Mn_N \le N < M(n_N+1)$ so that $2Mn_N+1 \le 2N+1 < 2M(n_N+1)+1$, and hence

$$\frac{2Mn_N}{2M(n_N+1)+1} < \frac{2Mn_N}{2N+1} \le \frac{2Mn_N}{2Mn_N+1}.$$

n_N goes to infinity as N goes to infinity and so taking limits throughout as N goes to infinity we obtain (22).

Substituting (22) in (21) and using the fact that $S_2(k) = 0$, we obtain from (19) that

$$A_x[k] = S_1(k) = K\left(p+1-\frac{k}{M}\right) A_y[p] + K\left(\frac{k}{M}-p\right) A_y[p+1].$$

If $0 \le k \le M$ then $p = 0$. For every other range of k, p is non-zero. Using the values of $A_y[p]$ as given by (18) and the fact that A_x is an even function one obtains (17). □

Remark 1. The function A defined in Theorem 8 is the triangle $\triangle_{K,M}(t) = K\max(1-\frac{|t|}{M}, 0)$ on $\mathbb{R}$ with height K and base length $2M$ restricted to the integers. The Fourier transform of $\triangle_{K,M}(t)$ is $KM\left(\frac{\sin \pi M\gamma}{\pi M\gamma}\right)^2$. Thus in Theorem 8 we have constructed a sequence x of constant amplitude whose autocorrelation is the inverse Fourier transform of the dilated Fejér function $K\omega_{2\pi M}$.

3.2 The additive property of triangular autocorrelation a.e.

As mentioned in Section 1.2, and repeated in the proof of Theorem 8, it has been shown in [34], [35] that if $\lambda \in (0,1)$ has binary expansion $0.\alpha_1\alpha_2\alpha_3\cdots$, if we consider the Lebesgue measure on $(0,1)$, and if we define the unimodular (in fact, ± 1-valued) function y by

$$y[k] = \begin{cases} 2\alpha_{2n+1} - 1 & \text{if } k = n+1, n \in \mathbb{N} \cup \{0\}, \\ 2\alpha_{2n} - 1 & \text{if } k = 1-n, n \in \mathbb{N}, \end{cases}$$

then, for *almost all* values of λ, the autocorrelation of y, A_y, is

$$A_y[k] = \begin{cases} 0 & \text{if } k \neq 0, \\ 1 & \text{if } k = 0. \end{cases}$$

In Theorem 8 it was shown that given $M \in \mathbb{N}$ this y can be used to construct x such that x has constant amplitude and

$$A_x[k] = \begin{cases} 1 - \frac{|k|}{M}, & \text{if } 0 \leq |k| \leq M, \\ 0, & \text{otherwise.} \end{cases}$$

In this case, x is unimodular. We shall now show that the autocorrelation of the sum of two such functions is the sum of the respective autocorrelations for almost all x.

We begin with the following calculation.

Example 4. Let X be the set of unimodular functions $x : \mathbb{Z} \to \mathbb{C}$ for which there exists a positive integer M with the property,

$$A_x[k] = \begin{cases} 1 - \frac{|k|}{M}, & \text{if } 0 \leq |k| \leq M, \\ 0, & \text{otherwise.} \end{cases}$$

For given $M \in \mathbb{N}$ let Ω be the set of all possibilities of any $2M$ consecutive values of $x \in X$. Then $\text{card}(\Omega) = 2^{2M}$. Let E be the subset of Ω such that given ε, the sum of the $2M$ consecutive values of x exceeds $M\varepsilon$ in absolute value. Among the $2M$ values suppose that there are $(M-j)$ $+1$s and $(M+j)$ -1s where $-M \leq j \leq M$. So the absolute value of the sum of $2M$ consecutive values would be $|M+j-(M-j)| = 2|j|$. The sum of these values exceeds $M\varepsilon$ in absolute value if $[M\varepsilon] \leq 2|j| \leq 2M$. The number of ways of having $(M-j)$ $+1$s and $(M+j)$ -1s is $\binom{2M}{M-j} = \binom{2M}{M+j}$. The total number of possible values for which the sum exceeds $M\varepsilon$ is

$$\text{card}(E) = \sum_{|j|=[\frac{M\varepsilon}{2}]}^{M} \binom{2M}{M-j} = \sum_{j=[\frac{M\varepsilon}{2}]}^{M} \binom{2M}{M-j} + \sum_{j=[\frac{M\varepsilon}{2}]}^{M} \binom{2M}{M+j} = 2\sum_{j=[\frac{M\varepsilon}{2}]}^{M} \binom{2M}{M-j}.$$

Consequently,

$$\frac{\text{card}(E)}{\text{card}(\Omega)} = 2^{-2M} 2 \sum_{j=[\frac{M\varepsilon}{2}]}^{M} \binom{2M}{M-j} = 2^{-2M+1} \sum_{j=[\frac{M\varepsilon}{2}]}^{M} \binom{2M}{M-j}.$$

Theorem 9. *(a) Let X be the set of unimodular functions $x : \mathbb{Z} \to \mathbb{C}$ for which there exists a positive integer M with the property,*

$$A_x[k] = \begin{cases} 1 - \frac{|k|}{M}, & \text{if } 0 \le |k| \le M, \\ 0, & \text{otherwise.} \end{cases}$$

Then there is a well defined finite Borel measure p on X induced from Lebesgue measure [1] *on $(0,1)$, in a manner described in the proof.*
(b) For almost all $x, y \in X$, with respect to p, we have

$$A_{x+y} = A_x + A_y,$$

noting that $x+y$ does not necessarily have constant amplitude and that A_{x+y} is not generally a triangle.

Proof. (a) We know from (2) and (3) that there is $S_0 \subseteq [0,1]$ defined by the properties: $|S_0| = 1$ and

$$\forall \lambda \in S_0, \quad \exists \mu_\lambda : \mathbb{Z} \to \mathbb{C} \text{ such that } |\mu_\lambda| = 1 \text{ and } A_{\mu_\lambda}[k] = \delta_{0,k} \text{ on } \mathbb{Z}.$$

From Theorem 8 we know that for each $M \in \mathbb{N}$, there is $S_M \subseteq [0,1]$ defined by the properties: $|S_M| = 1$ and

$$\forall \lambda \in S_M, \ \exists \mu_\lambda : \mathbb{Z} \to \mathbb{C} \text{ such that } |\mu_\lambda| = 1 \text{ and } A_{\mu_\lambda}[k] = \max\left(0, 1 - \frac{|k|}{M}\right) \text{ on } \mathbb{Z}.$$

In fact, by the way we defined μ_λ in Theorem 8 we could take $S_M = S_0$. However, we can equally-well choose $\{S_M : S_M \subseteq S_0, |S_M| = 1\}$ to be a disjoint collection whose union is S_0. In this case we define the functions, $f_M : S_M \to X$, $\lambda \mapsto \mu_\lambda$, where $A_{\mu_\lambda}[k] = \max\left(0, 1 - \frac{|k|}{M}\right)$ on $\mathbb{Z}$, and $f : S_0 \to X$, $\lambda \mapsto f_M(\lambda)$ when $\lambda \in S_M$. In this way we use f to define a compact topology on X induced from $S_0 \subseteq [0,1]$, and to define a bounded Borel measure p on X induced from Lebesgue measure on $[0,1]$.

We provide the technical properties of p in part (b) of the proof.
(b) We have already seen the construction of such x and y in Theorem 8. Formally,

[1] For the necessary measure theory and definitions of Borel and Lebesgue measure we refer to [7].

$$\begin{aligned}
A_{x+y}[k] &= \lim_{N\to\infty}\frac{1}{2N+1}\sum_{m=-N}^{N}(x+y)[m+k]\overline{(x+y)[m]} \\
&= \lim_{N\to\infty}\frac{1}{2N+1}\sum_{m=-N}^{N}(x[m+k]+y[m+k])(\overline{x[m]}+\overline{y[m]}) \\
&= \lim_{N\to\infty}\frac{1}{2N+1}\sum_{m=-N}^{N}x[m+k]\overline{x[m]}+\lim_{N\to\infty}\frac{1}{2N+1}\sum_{m=-N}^{N}y[m+k]\overline{y[m]}+ \\
&\quad+\lim_{N\to\infty}\frac{1}{2N+1}\sum_{m=-N}^{N}x[m+k]\overline{y[m]}+\lim_{N\to\infty}\frac{1}{2N+1}\sum_{m=-N}^{N}y[m+k]\overline{x[m]} \\
&= A_x(k)+A_y(k)+\lim_{N\to\infty}\frac{1}{2N+1}\sum_{m=-N}^{N}x[m+k]\overline{y[m]}+ \\
&\quad+\lim_{N\to\infty}\frac{1}{2N+1}\sum_{m=-N}^{N}y[m+k]\overline{x[m]}. \qquad (23)
\end{aligned}$$

Let us denote the last two terms on the right side of (23) by S_3 and S_4 respectively. We want to show that $S_3 = 0$ and $S_4 = 0$.

$$S_3 = \lim_{N\to\infty}\frac{1}{2N+1}\sum_{m=-N}^{N}x[m+k]\overline{y[m]}. \qquad (24)$$

Without loss of generality we take y to be real-valued and so (24) becomes

$$S_3 = \lim_{N\to\infty}\frac{1}{2N+1}\sum_{m=-N}^{N}x[m+k]y[m]. \qquad (25)$$

Suppose that

$$A_x[k] = \begin{cases} 1-\frac{|k|}{M_1}, & \text{if } 0 \le |k| \le M_1, \\ 0, & \text{otherwise,} \end{cases}$$

and

$$A_y[k] = \begin{cases} 1-\frac{|k|}{M_2}, & \text{if } 0 \le |k| \le M_2, \\ 0, & \text{otherwise.} \end{cases}$$

Let P_N be the largest integer so that

$$M_2P_N \le N \le M_2(P_N+1). \qquad (26)$$

Then S_3 can be written as

$$S_3 = \lim_{N\to\infty} \frac{1}{2N+1} \sum_{m=-N}^{-M_2P_N-1} x[m+k]y[m] + \lim_{N\to\infty} \frac{1}{2N+1} \sum_{m=M_2P_N+1}^{N} x[m+k]y[m] +$$
$$+ \lim_{N\to\infty} \frac{1}{2N+1} \sum_{m=-M_2P_N}^{M_2P_N} x[m+k]y[m]. \tag{27}$$

Let us denote the first two terms of (27) by s_1 and s_2, respectively. Now,

$$|s_1| \leq \sum_{m=-N}^{-M_2P_N-1} 1 = N - M_2P_N$$

and

$$|s_2| \leq \sum_{m=M_2P_N+1}^{N} 1 = N - M_2P_N.$$

From (26),

$$N - M_2P_N \leq M_2(P_N+1) - M_2P_N = M_2$$

which means $|s_1| \leq M_2$ and $|s_2| \leq M_2$. Therefore,

$$\lim_{N\to\infty} \frac{|s_1|}{2N+1} \leq \lim_{N\to\infty} \frac{M_2}{2N+1} = 0$$

and also

$$\lim_{N\to\infty} \frac{|s_2|}{2N+1} \leq \lim_{N\to\infty} \frac{M_2}{2N+1} = 0.$$

Thus,

$$S_3 = \lim_{N\to\infty} \frac{1}{2N+1} \sum_{m=-M_2P_N}^{M_2P_N} x[m+k]y[m] \tag{28}$$
$$= \lim_{N\to\infty} \frac{1}{2N+1} \sum_{n=-P_N}^{P_N-1} \sum_{m=M_2n+1}^{M_2(n+1)} x[m+k]y[m] +$$
$$+ \lim_{N\to\infty} \frac{1}{2N+1} x[-M_2P_N+k]y[-M_2P_N]$$
$$= \lim_{N\to\infty} \frac{1}{2N+1} \sum_{n=-P_N}^{P_N-1} \sum_{m=M_2n+1}^{M_2(n+1)} x[m+k]y[M_2(n+1)]. \tag{29}$$

The last step (29) follows due to the fact that by construction y is constant and equal to either $+1$ or -1 in the interval $[M_2n+1, M_2(n+1)]$. So $y[M_2(n+1)]$ is either $+1$ or -1. Between (M_2n+1) and $M_2(n+1)$ there are M_2 terms. So there are M_2 values of x. Suppose that of these M_2 values there are j that have the value $+1$ and (M_2-j) that have the value -1. Upon multiplication by $y(M_2(n+1))$ we have either j values that are -1 and (M_2-j) values that are $+1$ or vice versa. In the sum on the right side of (29) there are $2P_N$ blocks of length M_2. Let us say that the first block has j_1 terms

equal to $+1$ and $(M_2 - j_1)$ terms equal to -1, the second block has j_2 terms equal to $+1$ and $(M_2 - j_2)$ terms equal to -1 and so on. Together, there are $(j_1 + j_2 + \cdots + j_{2P_N})$ terms equal to $+1$ and $(M_2 - j_1 + M_2 - j_2 + \cdots + M_2 - j_{2P_N}) = 2P_N M_2 - (j_1 + j_2 + \cdots + j_{2P_N})$ terms equal to -1. Let $P_N M_2 = M$ and $j_1 + j_2 + \cdots + j_{2P_N} = M - j$ where $-M \leq j \leq M$. Note that this M is unrelated to the M that appears in Theorem 8 and part (a) of the statement of this theorem where it indicates the length of the base of a triangle. Then $2P_N M_2 - (j_1 + j_2 + \cdots + j_{2P_N}) = 2M - (M - j) = M + j$. Thus, out of $2M$ consecutive values of $x[m+k]y[m]$ there are $(M - j)$ values that are $+1$ and $(M + j)$ values that are -1. So the absolute value of the sum of $2P_N M_2 = 2M$ consecutive values of $x[m+k]y[m]$ would be $M + j - (M - j) = 2|j|$.

Let Ω be the set of all possibilities for the $2M$ consecutive values of $x[m+k]y[m]$. From (2), each such x and y corresponds to some $\lambda \in (0,1)$. From Example 4 and the definition of $E \subseteq \Omega$ there, it follows that given ε the measure of the set for which the sum of $2M$ consecutive values exceeds $M\varepsilon$ in absolute value is

$$\frac{\text{card}(E)}{\text{card}(\Omega)} = 2^{-2M+1} \sum_{j=[\frac{M\varepsilon}{2}]}^{M} \binom{2M}{M-j}.$$

This can be transported as an explicit, computable property of p.

It can be shown in a manner identical to that in [34] that

$$\lim_{M\to\infty} 2^{-2M+1} \sum_{j=[\frac{M\varepsilon}{2}]}^{M} \binom{2M}{M-j} = 0.$$

Thus the set of x and y for which there should fail to be an integral value of $M = P_N M_2$ such that from that value on (see (28))

$$\Big| \sum_{m=-M}^{M} x[m+k]y[m] \Big| \leq M\varepsilon + 1$$

has measure zero. Therefore,

$$\overline{\lim}_{N\to\infty} \Big| \frac{1}{2N+1} \sum_{m=-M}^{M} x[m+k]y[m] \Big| \leq \frac{M\varepsilon+1}{2N+1} = \frac{P_N M_2 \varepsilon}{2N+1} + \frac{1}{2N+1}. \tag{30}$$

From (26),

$$\frac{P_N M_2}{2N+1} \leq \frac{N}{2N+1} \to \frac{1}{2}$$

as N goes to infinity. So, the left side of (30) is less than $\frac{\varepsilon}{2}$ and for almost all x and y,

$$\lim_{N\to\infty} \frac{1}{2N+1} \sum_{m=-N}^{N} x[m+k]y[m] = 0.$$

In a similar way one can show that

$$S_4 = \lim_{N\to\infty} \frac{1}{2N+1} \sum_{m=-N}^{N} y[m+k]x[m] = 0$$

for almost every x and y. This concludes proving part (b). □

Remark 2. Due to Theorem 8, Theorem 9 can be trivially generalized to x and y that have constant amplitude K_1 and K_2 respectively and have autocorrelation functions

$$A_x[k] = \begin{cases} K_1\left(1-\frac{|k|}{M_1}\right), & \text{if } 0 \le |k| \le M_1, \\ 0, & \text{otherwise,} \end{cases}$$

and

$$A_y[k] = \begin{cases} K_2\left(1-\frac{|k|}{M_2}\right), & \text{if } 0 \le |k| \le M_2, \\ 0, & \text{otherwise.} \end{cases}$$

Remark 3. Given $K > 0$ and $M \in \mathbb{N}$, on $\mathbb{R}$, the inverse Fourier transform of $MK\left(\frac{\sin \pi M\gamma}{\pi M\gamma}\right)^2$ is $K\max\left(1-\frac{|t|}{M},0\right)$. By the additive property of Fourier transform, the inverse Fourier transform of $F(\gamma) = \sum_{n=1}^{N} nK_n\left(\frac{\sin \pi n\gamma}{\pi n\gamma}\right)^2$, restricted to $\mathbb{Z}$, is

$$\check{F}[m] = \sum_{n=1}^{N} K_n \max(1-\frac{|m|}{n},0).$$

Due to Theorem 8, one can construct functions x_n such that $A_{x_n} = K_n \max(1-\frac{|m|}{n},0)$ with $|x_n| = \sqrt{K_n}$. Theorem 9 implies that the sequence $x = x_1 + \cdots + x_N$ has autocorrelation $\check{F}$. Also, $x \in \ell^\infty(\mathbb{Z})$ since $|x|$ is bounded by $\sum_{n=1}^{N}\sqrt{K_n}$. Thus we have a function $x \in \ell^\infty(\mathbb{Z})$ whose autocorrelation is the inverse Fourier transform of dilates of Fejér functions.

Example 5. Generally, $A_{x+y}[k] \neq A_x[k] + A_y[k]$. In fact, in the case of real-valued sequences $x, y \in \ell^\infty(\mathbb{Z})$, when all limits as $N \to \infty$ exist, $A_{x+y}[k] = A_x[k] + A_y[k] + 2A_{xy}[-k]$, and there is no reason to expect $A_{xy}[-k] = 0$ for each $k \in \mathbb{Z}$. Here, A_{xy} is the cross-correlation of x and y defined by

$$\forall k \in \mathbb{Z},\ A_{xy}[k] = \lim_{N\to\infty} \frac{1}{2N+1} \sum_{m=-N}^{N} x[k+m]\overline{y[m]}.$$

As a particular example, note that the binary expansions, with a precision of 16 bit, of $\lambda_x = 0.35$ and $\lambda_y = 0.9$ are 0.0101100110011001 and 0.1110011001100110, respectively. From these one can obtain sequences x and y of ± 1s by following the definition of y in (2). The partial autocorrelations of x, y, and $x+y$ have been calculated by computing the sum in Definition 1 for $N = 1000$, i.e., $2N+1 = 2001$ terms. These partial autocorrelations at the integers between -10 and 10 are plotted in Figure 3. Clearly, the sums of the autocorrelations of x and y do not match the autocorrelation of $x+y$.

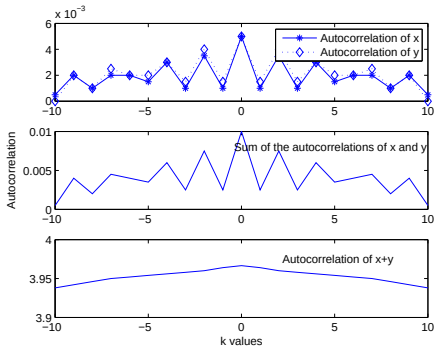

Fig. 3 Autocorrelations of two sequences x and y and their sum

4 Conclusions

In this chapter Hadamard matrices have been used to construct constant amplitude zero autocorrelation (CAZAC) sequences on $\mathbb{Z}$. Such sequences are important in the areas of radar and communication. This is generalized to the construction of unimodular sequences on $\mathbb{Z}$ whose autocorrelations are triangles. Finally, conditions under which the autocorrelation of the sum of two sequences is the same as the sum of the respective autocorrelations are studied.

Acknowledgements The first named author gratefully acknowledges the support of ONR Grant N00014-09-1-0144 and MURI-ARO Grant W911NF-09-1-0383. The second named author gratefully acknowledges the support of AFOSR Grant FA9550-10-1-0441.

References

1. Auslander, L., Barbano, P.E.: Communication codes and Bernoulli transformations. Appl. Comput. Harmon. Anal. **5**(2), 109–128 (1998)
2. Bell, D.A.: Walsh functions and Hadamard matrices. Electronics Letters **2**, 340 – 341 (1966)
3. Benedetto, J.J.: A multidimensional Wiener-Wintner theorem and spectrum estimation. Trans. Amer. Math. Soc. **327**(2), 833–852 (1991)
4. Benedetto, J.J.: Harmonic Analysis and Applications. CRC Press, Boca Raton, FL (1997)
5. Benedetto, J.J., Benedetto, R.L., Woodworth, J.T.: Björk CAZACs: theory, geometry, implementation, and waveform ambiguity behavior (2011). Preprint, to be submitted
6. Benedetto, J.J., Benedetto, R.L., Woodworth, J.T.: Optimal ambiguity functions and Weil's exponential sum bounds (2011). Preprint, to be submitted
7. Benedetto, J.J., Czaja, W.: Integration and Modern Analysis. Birkhäuser Boston Inc., Boston, MA (2009)
8. Benedetto, J.J., Datta, S.: Construction of infinite unimodular sequences with zero autocorrelation. Advances in Computational Mathematics **32**(2), 191 – 207 (2010)
9. Benedetto, J.J., Donatelli, J.J.: Ambiguity function and frame theoretic properties of periodic zero autocorrelation waveforms. IEEE J. Special Topics Signal Processing **1**, 6–20 (2007)

10. Björck, J., Saffari, B.: New classes of finite unimodular sequences with unimodular Fourier transforms. Circulant Hadamard matrices with complex entries. C. R. Acad. Sci. **320**, 319 – 324 (1995)
11. Christensen, O.: An Introduction to Frames and Riesz Bases. Birkhäuser (2003)
12. Datta, S.: Wiener's Generalized Harmonic Analysis and Waveforem Design. Ph.D. thesis, University of Maryland, College Park, Maryland (2007)
13. Daubechies, I.: Ten Lectures on Wavelets. SIAM (1992)
14. Hadamard, J.: Résolution d'une question relative aux déterminants. Bulletin des Sciences Mathématiques **17**, 240– 246 (1893)
15. Helleseth, T., Kumar, P.V.: Sequences with low correlation. In: Handbook of coding theory, Vol. I, II, pp. 1765–1853. North-Holland, Amsterdam (1998)
16. Horadam, K.J.: Hadamard Matrices and Their Applications. Princeton University Press, Princeton, NJ (2007)
17. Horn, R.A., Johnson, C.R.: Matrix analysis. Cambridge University Press, Cambridge (1990). Corrected reprint of the 1985 original
18. Kerby, R.: The Correlation Function and the Wiener-Wintner Theorem in Higher Dimension. Ph.D. thesis, University of Maryland, College Park (1990)
19. Kerby, R.: (2008). Personal communication
20. Levanon, N., Mozeson, E.: Radar Signals. Wiley Interscience, IEEE Press (2004)
21. Long, M.L.: Radar Reflectivity of Land and Sea. Artech House (2001)
22. Mow, W.H.: A new unified construction of perfect root-of-unity sequences. In: Proc. IEEE 4th International Symposium on Spread Spectrum Techniques and Applications (Germany), pp. 955–959 (1996)
23. Nathanson, F.E.: Radar Design Principles - Signal Processing and the Environment. SciTech Publishing Inc., Mendham, NJ (1999)
24. Paley, R.E.A.C.: On orthogonal matrices. Journal of Mathematics and Physics **12**, 311 –320 (1933)
25. Richards, M.A., Scheer, J.A., Holm, W.A. (eds.): Principles of Modern Radar: Basic Principles. SciTech Publishing Inc., Raleigh, NC (2010)
26. Schipp, F., Wade, W.R., Simon, P.: Walsh Series, An Introduction to Dyadic Harmonic Analysis. Taylor & Francis (1990)
27. Stein, E.M., Weiss, G.: Introduction to Fourier Analysis on Euclidean Spaces. Princeton University Press, Princeton, N.J. (1971)
28. Stimson, G.W.: Introduction to Airborne Radar. SciTech Publishing Inc., Mendham, NJ (1998)
29. Sylvester, J.J.: 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**, 461– 475 (1867)
30. Ulukus, S., Yates, R.D.: Iterative construction of optimum signature sequence sets in synchronous CDMA systems. IEEE Trans. Inform. Theory **47**(5), 1989–1998 (2001)
31. Verdú, S.: Multiuser Detection. Cambridge University Press, Cambridge, UK (1998)
32. Viterbi, A.J.: CDMA: Principles of Spread Spectrum Communication. Addison-Wesley (1995)
33. Walsh, J.L.: A closed set of normal orthogonal functions. American Journal of Mathematics **45**, 5 – 24 (1923)
34. Wiener, N.: Generalized harmonic analysis. Acta Math. (55), 117–258 (1930)
35. Wiener, N.: The Fourier Integral and Certain of its Applications. Cambridge Mathematical Library. Cambridge University Press, Cambridge (1988). Reprint of the 1933 edition. With a foreword by Jean-Pierre Kahane
36. Wiener, N., Wintner, A.: On singular distributions. J. Math. Phys. pp. 233–246 (1939)