Adv Comput Math (2010) 32:191–207
DOI 10.1007/s10444-008-9100-9

Construction of infinite unimodular sequences with zero autocorrelation

John J. Benedetto · Somantika Datta

Received: 13 September 2007 / Accepted: 25 March 2008 /
Published online: 18 September 2008

Abstract Unimodular waveforms x are constructed on the integers with the property that the autocorrelation of x is one at the origin and zero elsewhere. There are three different constructions: exponentials of the form $e^{2\pi i n^{\alpha}\theta}$, sequences taken from roots of unity, and sequences constructed from the elements of real Hadamard matrices. The first is expected and elementary and the second is based on the construction of Wiener. The third is the most intricate and is really one of a family of distinct but structurally similar waveforms. A natural error estimate problem is posed for the last construction. The analytic solution is not as useful as the simulations because of the inherent counting problems in the construction.

Keywords Infinite unimodular sequences · Zero autocorrelation · Hadamard matrices

Mathematics Subject Classification (2000) 42-XX (Fourier Analysis)

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,

Communicated by Yuesheng Xu.

J. J. Benedetto (✉) · S. Datta
Department of Mathematics, University of Maryland, College Park, MD 20742, USA
e-mail: jjb@math.umd.edu

whose inverse Fourier transforms are the autocorrelations of bounded functions or waveforms 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. This is the setting with which we deal. In fact we shall construct three such classes of waveforms x. The first construction uses elementary analysis, the second generalizes a construction of Wiener, and the third is based on Hadamard matrices. This last construction is the most intricate.

The aforementioned problem, 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 communications. In the former, the waveforms x can play a role in effective target recognition, see, e.g., [1, 4, 5, 8–11, 13]; and in the latter they are used to address synchronization issues in cellular (phone) access technologies, especially code division multiple access, e.g., [14, 15]. The radar and communication methods combine in recent advanced multifunction RF systems.

In radar there are two main reasons that the waveforms 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 Notation

We shall use the standard notation from harmonic analysis, e.g., [3, 12]. $C(\mathbb{T}^d)$ is the space of complex 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 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. For any positive integer N, we denote the $d-$dimensional square in $\mathbb{Z}^d$ by $S(N)$, and, so, by $S(N)$ we shall mean

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

Also, for $k \in \mathbb{Z}^d$, $k = (k_1, \cdots, k_d)$,

$$\sum_{m \in S(N)} x[k+m]\overline{x[m]} = \sum_{m_1=-N}^{N} \sum_{m_2=-N}^{N} \cdots \sum_{m_d=-N}^{N} x[k+m]\overline{x[m]}.$$

Definition 1.1 The *autocorrelation* $A_x : \mathbb{Z}^d \to \mathbb{C}$ of $x : \mathbb{Z}^d \to \mathbb{C}$ is defined as

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

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

1.3 Perspective

In the setting of $\mathbb{R}$, we have the following theorem due to Wiener and Wintner [17], which was later extended to $\mathbb{R}^d$ in [2, 6].

Theorem 1.2 *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.,*

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

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

Theorem 1.3 *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*

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

Though the Wiener–Wintner theorem gives the construction of the function x it does not ensure boundedness of x, whereas our desire is to construct codes x that have constant amplitude.

1.4 Outline

The paper is divided in the following way. In Section 2 we show that the unimodular sequence $x[n] = e^{2\pi in^\alpha\theta}$, where $\alpha \in \mathbb{N}\setminus\{1\}$ and θ is irrational, has zero autocorrelation on $\mathbb{Z}\setminus\{0\}$. In Section 3 we construct polyphase sequences from roots of unity which also have zero autocorrelation on $\mathbb{Z}\setminus\{0\}$. In Section 4 we construct zero autocorrelation sequences from real Hadamard matrices. The methods of Sections 3 and 4 are actually more general than stated. For example, we can invoke the same technique of construction, but use a different permutation of the roots of unity or a different arrangement of rows of the Hadamard matrices. In this way we still obtain unimodular waveforms with zero autocorrelation.

2 Sequences of the form $e^{2\pi i n^\alpha \theta}$, $\alpha \in \mathbb{N} \setminus \{1\}$ and θ irrational

For $t \in \mathbb{R}$, let $[t]$ denote the integral part of t, that is, $[t]$ is the largest integer less than or equal to t; and let $\{t\} = t - [t]$ be the fractional part of t. I is the unit interval $[0, 1)$. For a given sequence (t_n), $n = 1, 2, \ldots$, in $\mathbb{R}$, $A(E; N)$ denotes the number of points $\{t_n\}$, $1 \leqslant n \leqslant N$, that lie in $E \subseteq [0, 1)$.

Definition 2.1 The sequence (t_n), $n = 1, 2, \ldots$, is *uniformly distributed modulo* 1 (*u.d.mod* 1) in $\mathbb{R}$ if

$$\lim_{N\to\infty} \frac{A([a, b); N)}{N} = b - a.$$

for all intervals $[a, b) \subseteq I$.

The following is the classical Weyl criterion for uniform distribution [7].

Theorem 2.2

a. *The sequence* (t_n), $n = 1, 2, \cdots$, *is u.d. mod* 1 *if and only if*

$$\forall h \in \mathbb{Z} \setminus \{0\}, \qquad \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i h t_n} = 0. \tag{2.1}$$

b. *Let* $p(t) = \alpha_m t^m + \alpha_{m-1} t^{m-1} + \cdots + \alpha_0$, $m > 1$, *be a polynomial with real coefficients, and let at least one of the coefficients* α_j *with* $j > 0$ *be irrational. Then the sequence* $(p(n))$, $n = 1, 2, \cdots$, *is u.d. mod* 1.

Theorem 2.3 *Let* $x : \mathbb{Z} \to \mathbb{C}$ *be defined by*

$$x[n] = e^{2\pi i n^\alpha \theta}, \qquad \theta \notin \mathbb{Q},\ \alpha \in \mathbb{N} \setminus \{1\}. \tag{2.2}$$

Then

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

Proof The autocorrelation of x at k is

$$A_x[k] = \lim_{N\to\infty} \frac{e^{2\pi i k^\alpha \theta}}{2N+1} \sum_{m=-N}^{N} e^{2\pi i \theta \left(\binom{\alpha}{1} m^{\alpha-1} k + \binom{\alpha}{2} m^{\alpha-2} k^2 + \cdots + \binom{\alpha}{\alpha-1} m k^{\alpha-1}\right)}. \tag{2.3}$$

Let $p(t) = \theta\binom{\alpha}{1} k t^{\alpha-1} + \theta\binom{\alpha}{2} k^2 t^{\alpha-2} + \cdots + \theta\binom{\alpha}{\alpha-1} k^{\alpha-1} t$. Since $\theta \notin \mathbb{Q}$ we can apply Theorem 2.2b when $k \neq 0$ to say that the sequence $(p(n))$ is u.d. mod 1. Therefore, according to Theorem 2.2a, taking $h = 1$ and $t_n = p(n)$ in (2.1), the right side of (2.3) is zero if $k \neq 0$. If $k = 0$ then $A_x[0] = 1$. □

It is elementary to prove the analogue of Theorem 2.3 for the more general case of crosscorrelation.

It is often necessary to construct unimodular waveforms on $\mathbb{Z}^d$. Let $n = (n_1, n_2, \cdots n_d) \in \mathbb{Z}^d$ and $|n| = \sqrt{n_1^2 + n_2^2 + \cdots + n_d^2}$. We define

$$\forall n \in \mathbb{Z}^d, \qquad x[n] = e^{2\pi i |n|^\alpha \theta}, \qquad \theta \notin \mathbb{Q},\ \alpha \in \mathbb{N}. \tag{2.4}$$

Theorem 2.4 *If $\alpha = 2$ then, for x defined in (2.4),*

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

Proof

$$A_x[k] = \lim_{N\to\infty} \frac{1}{(2N+1)^d} \sum_{m_1=-N}^{N} \cdots \sum_{m_d=-N}^{N} e^{2\pi i |m+k|^\alpha \theta} e^{-2\pi i |m|^\alpha \theta}. \tag{2.5}$$

If $\alpha = 2$ then the right side of (2.5) is

$$\lim_{N\to\infty} \frac{e^{2\pi i |k|^2 \theta}}{(2N+1)^d} \sum_{m_1=-N}^{N} \cdots \sum_{m_d=-N}^{N} e^{4\pi i (m_1 k_1 + \cdots + m_d k_d)\theta}$$

$$= \lim_{N\to\infty} e^{2\pi i |k|^2 \theta} \left(\frac{1}{2N+1} \sum_{m_1=-N}^{N} e^{4\pi i m_1 k_1 \theta} \right) \cdots \left(\frac{1}{2N+1} \sum_{m_d=-N}^{N} e^{4\pi i m_d k_d \theta} \right)$$

$$= \begin{cases} 0 \text{ if } k \neq 0 \\ 1 \text{ if } k = 0. \end{cases}$$

□

Another way to define unimodular waveforms $x : \mathbb{Z}^d \to \mathbb{C}$ is as follows. Let $n = (n_1, n_2, \cdots, n_d) \in \mathbb{Z}^d$ and let $\theta = (\theta_1, \cdots, \theta_d)$ have the property that none of the $\theta_1, \cdots, \theta_d$ is in $\mathbb{Q}$. Define $n^\alpha = (n_1^\alpha, n_2^\alpha, \cdots, n_d^\alpha)$ and let

$$x[n] = e^{2\pi i n^\alpha \cdot \theta}. \tag{2.6}$$

By a calculation similar to the proof of Theorem 2.4, we obtain the following results.

Theorem 2.5 *If $\alpha = 2$ then, for x defined in (2.6),*

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

Theorem 2.6 *Define the waveform $x : \mathbb{Z}^d \to \mathbb{C}$ as follows: for $\alpha \in \mathbb{N} \setminus \{1\}$ and $\theta \in \mathbb{R} \setminus \mathbb{Q}$, let $y : \mathbb{Z} \to \mathbb{C}$ be defined by $y[n] = e^{2\pi i n^\alpha \theta}$, and for $n = (n_1, n_2,$*

$\ldots, n_d) \in \mathbb{Z}^d$ let $x[n] = x(n_1, \ldots, n_d) = y[n_j]$, where j is fixed. Then, for any given $k = (k_1, k_2, \ldots, k_d)$,

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

Here the autocorrelation is 1 not just at the origin but at all points on the hyperplane $k_j = 0$.

3 Construction of polyphase sequences with zero autocorrelation

In [16] Wiener showed probabilistically that there exist sequences whose autocorrelations are zero everywhere except at the origin. He also constructed an explicit example of such a sequence $x = \{x[m]\}$ of ± 1s. We go back to Wiener's construction and obtain an analogous polyphase construction for n roots of unity.

Example 3.1 Let $n = 3$. We shall define $x : \mathbb{Z} \to \mathbb{C}$ such that the range of x is $\{w_0, w_1, w_2\}$, where $w_0 = 1$, $w_1 = e^{i\frac{2\pi}{3}}$, and $w_2 = e^{i\frac{4\pi}{3}}$. x is defined on $\mathbb{N}$ in the following way.

$[w_0, w_1, w_2]$, repeated $3^0 = 1$ times, giving the first 3 terms of x on $\mathbb{N}$, i.e., $x[1] = w_0$, $x[2] = w_1$, and $x[3] = w_2$; then

$[w_0,\ w_0;\ w_0,\ w_1;\ w_0,\ w_2;\ w_1,\ w_0;\ w_1,\ w_1;\ w_1,\ w_2;\ w_2,\ w_0;\ w_2,\ w_1;\ w_2,\ w_2]$, repeated $3^1 = 3$ times, so that these $18 = 2 \cdot 3^2$ terms repeated thrice give the next 54 terms of x on $\mathbb{N}$, i.e., $x[4] = w_0, \ldots, x[57] = w_2$; then

$[w_0, w_0, w_0;\ w_0, w_0, w_1;\ w_0, w_0, w_2;\ w_0, w_1, w_0;\ w_0, w_1, w_1;\ w_0, w_1, w_2;\ w_0, w_2, w_0;\ w_0, w_2, w_1;\ w_0, w_2, w_2;\ w_1, w_0, w_0;\ w_1, w_0, w_1;\ w_1, w_0, w_2;\ \ldots;\ w_2, w_2, w_2]$ repeated $3^2 = 9$ times, so that these 81 terms repeated 9 times give the next 729 terms of x on $\mathbb{N}$, i.e., $x[58] = w_0, \ldots, x[786] = w_2$.

We continue this procedure to complete the definition of x on $\mathbb{N}$. Let $x[0] = 1$ and, for all $k \in \mathbb{N}$, let $x[-k] = x[k]$. The number of elements in each row is an integer of the form $j3^j$ and each row is repeated 3^{j-1} times.

Definition 3.2 If $n > 3$, we shall define $x : \mathbb{Z} \to \mathbb{C}$, analogous to Example 3.1. Thus, x takes the values $w_j : j = 0, \ldots, n-1$, where $w_0 = 1$, $w_1 = e^{i\frac{2\pi}{n}}, \ldots, w_{n-1} = e^{i\frac{2\pi(n-1)}{n}}$, and x is defined on $\mathbb{N}$ in the following way.

$[w_0, w_1, \ldots, w_{n-1}]$, repeated $n^0 = 1$ times; then $[w_0, w_0; w_0, w_1; \ldots; w_0, w_{n-1}; w_1, w_0; w_1, w_1; \ldots; w_1, w_{n-1}; \ldots; w_{n-1}, w_0, w_{n-1}, w_1, \ldots, w_{n-1}, w_{n-1}]$ repeated $n^1 = n$ times; then $[w_0, w_0, w_0; w_0, w_0, w_1; \ldots; w_0, w_0, w_{n-1}; \ldots; w_{n-1}, w_{n-1}, w_0; \ldots; w_{n-1}, w_{n-1}, w_{n-1}]$ repeated n^2 times.

We continue this procedure to complete the definition of x on $\mathbb{N}$. Let $x[0] = 1$ and, for all $k \in \mathbb{N}$, let $x[-k] = x[k]$. The number of elements in each of these rows is an integer of the form jn^j and each such row is repeated n^{j-1} times.

Lemma 3.3 *Let $n \geqslant 2$ and define $x : \mathbb{Z} \to \mathbb{C}$ as in Definition 3.2. Fix $p \in \mathbb{N}$. Let s_p be a fixed ordered sequence of w_js of length p. Then,*

$$\lim_{N\to\infty} \frac{\textit{Number of times } s_p \textit{ appears in the first } N \textit{ terms of } x}{N} = \frac{1}{n^p}. \tag{3.1}$$

Proof

i. In order to verify (3.1) we begin by noting that in a particular row having jn^j elements, where $p \leqslant j$, any finite sequence of length p occurs as often as any other finite sequence of the same length. We can prove this by induction on p.
Consequently, in such a row, the fraction of times a particular p-tuple s_p occurs is $\frac{1}{n^p}$.
If we wish to calculate the relative frequency of the occurrence of s_p among the first N terms we might have to stop in the middle of some row. As such, we write

$$\begin{aligned} N = 1 \cdot n^1 \cdot n^0 + 2 \cdot n^2 \cdot n^1 + \ldots + (p-1)n^{p-1}n^{p-2} + pn^p n^{p-1} \\ + \ldots + Mn^M n^{M-1} + P(M+1)n^{M+1} + Q, \end{aligned}$$

where $0 \leqslant P < n^M$ and $0 \leqslant Q < (M+1)n^{M+1}$. Here $M \to \infty$ as $N \to \infty$. Thus,

$$N = \sum_{j=1}^{p-1} jn^j n^{j-1} + \sum_{j=p}^{M} jn^j n^{j-1} + P(M+1)n^{M+1} + Q = S_1 + S_2 + Q,$$

where

$$S_2 = \sum_{j=p}^{M} jn^{2j-1} + P(M+1)n^{M+1}.$$

ii. Let us denote the number of occurrences of a particular p-tuple s_p in a row of length $1 \cdot n^1$ by n_1, the number of occurrences in a row of length $2 \cdot n^2$ by n_2, and so on. Note that these rows are repeated $n^0, n^1, \cdots$ times, respectively. Therefore,

$$\begin{aligned} &\lim_{N\to\infty} \frac{\text{Number of times } s_p \text{ appears in the first } N \text{ terms of } x}{N} \\ &= \lim_{N\to\infty} \left[\frac{n^{p-1} \cdot \frac{n_p}{S_2}}{1 + \frac{S_1+Q}{S_2}} + \cdots + \frac{n^{M-1} \cdot \frac{n_M}{S_2}}{1 + \frac{S_1+Q}{S_2}} + \frac{P\frac{n_{M+1}}{S_2}}{1 + \frac{S_1+Q}{S_2}} \right. \\ &\qquad \left. + \frac{\text{Repetitions in the last } Q}{N} \right]. \end{aligned} \tag{3.2}$$

We shall show in part *iii* that $\frac{S_1+Q}{S_2} \to 0$ as $N \to \infty$. Assuming this fact, we have $\frac{Q}{N} \to 0$ as $N \to \infty$; and, hence, the last term on the right side (3.2) is zero. Thus, the right side of (3.2) is

$$n^{p-1}\frac{n_p}{S_2} + n^p\frac{n_{p+1}}{S_2} + \cdots + n^{M-1}\frac{n_M}{S_2} + P\frac{n_{M+1}}{S_2}$$
$$= \frac{n^{p-1}\cdot n_p + n^p \cdot n_{p+1} + \cdots + n^{M-1}n_M + Pn_{M+1}}{S_2} = \frac{1}{n^p},$$

where the equality follows from our assertion in the beginning of the proof that in a particular row having jn^j elements, for some j, where $p \leqslant j$, any finite sequence of length p occurs as often as any other finite sequence of the same length. Thus, we have shown that

$$\lim_{N\to\infty} \frac{\text{Number of times } s_p \text{ appears in the first } N \text{ terms of } x}{N} = \frac{1}{n^p}. \quad (3.3)$$

iii. Finally, we prove that $\frac{S_1+Q}{S_2} \to 0$ as $N \to \infty$. Note that $S_2 = S_2(M)$ goes to infinity as N goes to infinity and, S_1 being finite, $\frac{S_1}{S_2}$ goes to 0 as S_2 goes to infinity. Thus, we only need to show that $\frac{Q}{S_2}$ goes to 0 as S_2 goes to infinity. We calculate

$$0 < \frac{Q}{S_2} < \frac{(M+1)n^{M+1}}{\sum_{j=p}^{M} jn^{2j-1} + P(M+1)n^{M+1}} < \frac{(M+1)n^{M+1}}{\frac{1}{n}\sum_{j=p}^{M} jn^{2j} + P(M+1)n^{M+1}}$$
$$< \frac{(M+1)n^{M+1}}{\frac{1}{n}\sum_{j=p}^{M} n^{2j} + P(M+1)n^{M+1}} = \frac{(M+1)n^{M+1}}{\frac{1}{n}n^{2p}\sum_{j=0}^{M-p} n^{2j} + P(M+1)n^{M+1}}$$
$$= \frac{(M+1)n^{M+1}}{n^{2p-1}\frac{n^{2(M-p+1)}-1}{n-1} + P(M+1)n^{M+1}} \to 0 \text{ as } N \to \infty,$$

since M goes to ∞ along with N. □

Theorem 3.4 *Let* $\{w_j : j = 0, \ldots, n-1\}$ *be the* n *roots of unity:* $w_0 = 1, w_1 = e^{\frac{2\pi i}{n}}, \ldots, w_{n-1} = e^{\frac{2\pi i(n-1)}{n}}$. *Then,*

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

Proof

i. If $k = 0$, then

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

ii. Note that $A_x[k] = \overline{A_x[-k]}$. Further, if $k \neq 0$ and if $\lim_{N\to\infty} \frac{1}{N} \sum_{m=1}^{N} x[m+k]\overline{x[m]} = 0$, then $A_x[k] = 0$. Thus, it is enough to show that

$$\forall k > 0, \quad \lim_{N\to\infty} \frac{1}{N} \sum_{m=1}^{N} x[m+k]\overline{x[m]} = 0.$$

For the sake of simplicity let us prove the case when $k = 1$ and when we are dealing with $n = 3$ roots of unity. One should note that if $k = p$ the value of $x[m+p]\overline{x[m]}$ is the product of the first (actually, its conjugate) and last elements of some sequence $w_{i_1} \dots w_{i_{p+1}}$, $i_n \in \{1, 2, 3\}$. There are 3^{p+1} such sequences. When $k = 1$, $x[m+1]\overline{x[m]}$ can come from any one of the following $3^2 = 9$-tuples: $\overline{w_1}w_1 = 1$, $\overline{w_1}w_2 = e^{\frac{2\pi i}{3}}$, $\overline{w_1}w_3 = e^{\frac{4\pi i}{3}}$, $\overline{w_2}w_1 = e^{\frac{4\pi i}{3}}$, $\overline{w_2}w_2 = 1$, $\overline{w_2}w_3 = e^{\frac{2\pi i}{3}}$, $\overline{w_3}w_1 = e^{\frac{2\pi i}{3}}$, $\overline{w_3}w_2 = e^{\frac{4\pi i}{3}}$, $\overline{w_3}w_3 = 1$. Therefore, from Lemma 3.3, we have

$$\begin{aligned}
\lim_{N\to\infty} \frac{1}{N} \sum_{m=1}^{N} x[m+1]\overline{x[m]} &= \lim_{N\to\infty} \frac{\text{Repetitions of } w_1w_1}{N} \cdot 1 \\
\lim_{N\to\infty} \frac{\text{Repetitions of } w_1w_2}{N} \cdot e^{\frac{2\pi i}{3}} &+ \lim_{N\to\infty} \frac{\text{Repetitions of } w_1w_3}{N} \cdot e^{\frac{4\pi i}{3}} \\
+ \lim_{N\to\infty} \frac{\text{Repetitions of } w_2w_1}{N} \cdot e^{\frac{4\pi i}{3}} &+ \lim_{N\to\infty} \frac{\text{Repetitions of } w_2w_2}{N} \cdot 1 \\
+ \lim_{N\to\infty} \frac{\text{Repetitions of } w_2w_3}{N} \cdot e^{\frac{2\pi i}{3}} &+ \lim_{N\to\infty} \frac{\text{Repetitions of } w_3w_1}{N} \cdot e^{\frac{2\pi i}{3}} \\
+ \lim_{N\to\infty} \frac{\text{Repetitions of } w_3w_2}{N} \cdot e^{\frac{4\pi i}{3}} &+ \lim_{N\to\infty} \frac{\text{Repetitions of } w_3w_3}{N} \cdot 1.
\end{aligned} \tag{3.4}$$

Using (3.1) with $p = 2$ and $n = 3$, (3.4) reduces to

$$\begin{aligned}
\lim_{N\to\infty} \frac{1}{N} \sum_{m=1}^{N} x[m+1]\overline{x[m]} &= \frac{1}{3^2} \cdot 1 + \frac{1}{3^2} \cdot e^{\frac{2\pi i}{3}} + \frac{1}{3^2} \cdot e^{\frac{4\pi i}{3}} + \frac{1}{3^2} \cdot e^{\frac{4\pi i}{3}} + \frac{1}{3^2} \cdot 1 \\
&\quad + \frac{1}{3^2} \cdot e^{\frac{2\pi i}{3}} + \frac{1}{3^2} \cdot e^{\frac{2\pi i}{3}} + \frac{1}{3^2} \cdot e^{\frac{4\pi i}{3}} + \frac{1}{3^2} \cdot 1 \\
&= \frac{1}{3^2} \cdot \left(1 + e^{\frac{2\pi i}{3}} + e^{\frac{4\pi i}{3}}\right) \cdot 3 = 0.
\end{aligned}$$

In general, for $k = p$ and $n = 3$, we have

$$\lim_{N\to\infty} \frac{1}{N} \sum_{m=1}^{N} x[m+p]\overline{x[m]} = \frac{1}{3^{p+1}} \left(1 + e^{\frac{2\pi i}{3}} + e^{\frac{4\pi i}{3}}\right) \cdot 3^p = 0.$$

iii. In a similar manner we have

$$\lim_{N\to\infty} \frac{1}{N} \sum_{m=1}^{N} x[m+p]\overline{x[m]} = \frac{1}{n^{p+1}} \left(1 + e^{\frac{2\pi i}{n}} + \cdots + e^{\frac{2\pi i(n-1)}{n}}\right) \cdot n^p = 0$$

for arbitrary n. □

4 Zero autocorrelation sequences constructed from Hadamard matrices

Definition 4.1 A real *Hadamard matrix* is a square matrix whose entries are either $+1$ or -1 and whose rows are mutually orthogonal.

The examples of Hadamard matrices below, of order $2^n, n = 1, \ldots,$ were first constructed by Sylvester in 1867. Hadamard constructed Hadamard matrices of order 12 and 20. He also proved the following. 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 Hadamard. The Hadamard conjecture (due to Paley) is that Hadamard matrices of order $4k$ exist for each k.

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.

$$H_1 = [\,1\,],$$

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

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

Thus,

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix} = \begin{bmatrix} H_{2^{k-2}} & H_{2^{k-2}} & H_{2^{k-2}} & H_{2^{k-2}} \\ H_{2^{k-2}} & -H_{2^{k-2}} & H_{2^{k-2}} & -H_{2^{k-2}} \\ H_{2^{k-2}} & H_{2^{k-2}} & -H_{2^{k-2}} & -H_{2^{k-2}} \\ H_{2^{k-2}} & H_{2^{k-2}} & -H_{2^{k-2}} & H_{2^{k-2}} \end{bmatrix}. \qquad (4.1)$$

Example 4.2 To construct a unimodular waveform 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

$$H_1, H_2, H_2, H_4, H_4, H_4, H_4, H_8, \cdots . \tag{4.2}$$

Let $x[0] = 1$ and, for any $k \in \mathbb{N}$, define $x[-k] = x[k]$. x is the exponential Hadamard waveform.

We shall show that the exponential Hadamard waveform x has autocorrelation one at zero and zero elsewhere (Theorem 4.5).

Lemma 4.3 *Given $j \in \mathbb{N}$. If $k = 2^j$, let H_k be the $k \times k$ Hadamard matrix. For every Hadamard matrix H_m where $m > k$, i.e., $m = 2^{j+1}, 2^{j+2}, \cdots$, let*

$$p = \text{Number of occurrences of } H_k H_k \text{ or } -H_k - H_k \text{ in all the rows of the matrix } H_m,$$

where H_m is written as rows of $\pm H_k$, see (4.1), and let

$$n = \text{Number of occurrences of } H_k - H_k \text{ or } -H_k H_k \text{ in all the rows of the matrix } H_m.$$

Then $p = n$.

Proof We proceed by induction on m. Let $m = 2^{j+1} = 2k$. In this case,

$$H_m = \begin{bmatrix} H_{2^j} & H_{2^j} \\ H_{2^j} & -H_{2^j} \end{bmatrix} = \begin{bmatrix} H_k & H_k \\ H_k & -H_k \end{bmatrix}.$$

$H_k H_k$ occurs once and $H_k - H_k$ occurs once. Therefore, $p = n = 1$.

Now, assume the result is true for $m = 2^{j+N}$ for some $N \in \mathbb{N}$. Let $m = 2^{j+N+1}$ and let $j + N = J$. In this case, $H_m = H_{J+1}$ is

$$\begin{bmatrix} H_J & H_J \\ H_J & -H_J \end{bmatrix}. \tag{4.3}$$

By our induction assumption, the result is true in each H_J and $-H_J$. Consider the H_ks forming the boundary between the two columns of H_Js in the matrix H_{J+1}, see (4.3), noting that each H_J (or $-H_J$) is composed of $\pm H_k$s. In the first row of (4.3), if we have a_1 occurrences of $H_k H_k$ or $-H_k - H_k$ in the boundary, then in the second row we have a_1 occurrences of $H_k - H_k$ or $-H_k H_k$. Similarly, if there are b_1 occurrences of $H_k - H_k$ or $-H_k H_k$ in the boundary of the first row, then there are b_1 occurrences of $H_k H_k$ or $-H_k - H_k$ in the boundary of the second row.

In each H_J let $p = p_J$ and $n = n_J$. Due to our assumption, $p_J = n_J$. Then, with $H_{J+1} = H_{j+N+1}$, we have $p = 4p_J + a_1 + b_1$ and $n = 4n_J + b_1 + a_1$. Thus, $p = n$. □

Lemma 4.4 *Let x be the exponential Hadamard waveform and define*

$$S_N[k] = \sum_{m=1}^{N} x[m+k]x[m], \tag{4.4}$$

where N is such that counting the first N values of x will end at the last element of some Hadamard matrix in the sequence (4.2) *defined in Example* 4.2. *Let* $k > 0$ *be given so that there exists n such that* $2^{n-1} < k \leqslant 2^n$. *The contribution to the sum in* (4.4) *from all Hadamard matrices of size* 2^{n+1} *and larger is* 0.

Proof

i. We shall consider rows of the submatrix H_{2^n} in $H_{2^{n+1}}$, $H_{2^{n+2}}$, $H_{2^{n+3}}$, ... We illustrate the procedure for $k = 3$. In this case $2^{2-1} < 3 \leqslant 2^2$, i.e., $n = 2$. Consequently, we consider the rows of H_4 in H_8, H_{16}, H_{32} .... Thus, for H_8 we have

$$H_8 = \begin{bmatrix} H_4 & H_4 \\ H_4 & -H_4 \end{bmatrix}$$

$$= \left[\begin{array}{cccc|cccc} 1 & \underbrace{1}_{x[m]} & \underbrace{1}_{x[m]} & \underbrace{1}_{x[m]} & \underbrace{1}_{x[m+3]} & \underbrace{1}_{x[m+3]} & \underbrace{1}_{x[m+3]} & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ -- & -- & -- & -- & -- & -- & -- & -- \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{array}\right]. \tag{4.5}$$

The ± 1s (not submatrices) in columns 2 to 4, necessitated by considering $k = 3$, in each occurrence of H_4 in H_8, H_{16}, $H_{32,}$ ... (except for the last H_4 in each row of H_4s) are multiplied by elements in the adjacent H_4, see the $x[m+3]$ designations in (4.5) for H_8. The elements from these columns have zero contribution to the sum in (4.4). This is true because, according to Lemma 4.3, H_4 occurs next to H_4 as often as it occurs next to $-H_4$ causing cancellations.

More generally, the elements in the k columns (columns $2^n - k + 1$ to 2^n) in each occurrence of H_{2^n} in $H_{2^{n+1}}$, $H_{2^{n+2}}$, $H_{2^{n+3}}$, ... (except for the last H_{2^n} in each row of H_{2^n}s) are multiplied by elements in the adjacent H_{2^n}. The elements from these columns have zero contribution to the sum in (4.4). This is true because, according to Lemma 4.3, H_{2^n} occurs next to H_{2^n} as often as it occurs next to $-H_{2^n}$ in each of $H_{2^{n+1}}$, $H_{2^{n+2}}$, $H_{2^{n+3}}$, ... causing cancellations.

ii. We now compute the contribution from the last H_{2^n} submatrix in each row of the matrices $H_{2^{n+1}}$, $H_{2^{n+2}}$, ..., as well as that for the elements from the k columns considered in *i.*

Due to the structure of Hadamard matrices, the last column of $\pm H_{2^n}$s in any higher order matrix such as $H_{2^{n+j}}$ has the same number of H_{2^n}s as $-H_{2^n}$s. In any Hadamard matrix of higher order, the elements of the specified k columns of these $\pm H_{2^n}$s interact with H_{2^n}s occurring in the first column of $\pm H_{2^n}$s . However, the first column of each higher order matrix consists only of $+H_{2^n}$s and no $-H_{2^n}$s. The resulting cancellations yield a contribution of zero.

iii. Now consider the contribution to the sum coming from the ± 1s (not submatrices) in columns 1 to $2^n - k$ of the H_{2^n} submatrices in each row of H_{2^n} in $H_{2^{n+1}}, H_{2^{n+2}}, \ldots$. To analyze this case we consider Hadamard matrices $H_{2^{n+1}}, H_{2^{n+2}}, \ldots$ as consisting of rows of $\pm H_{2^{n-1}}$s(H_2s when $k = 3$). Equation 4.6 illustrates the situation in H_8 when $k = 3$.

$$H_8 = \begin{bmatrix} \underbrace{1}_{x[m]} & 1 & | & 1 & \underbrace{1}_{x[m+3]} & | & 1 & 1 & 1 & 1 \\ 1 & -1 & | & 1 & -1 & | & 1 & -1 & 1 & -1 \\ -- & -- & | & -- & -- & -- & -- & -- & -- & -- \\ 1 & 1 & | & -1 & -1 & | & 1 & 1 & -1 & -1 \\ 1 & -1 & | & -1 & 1 & | & 1 & -1 & -1 & 1 \\ -- & -- & & -- & -- & -- & -- & -- & -- & -- \\ 1 & 1 & & 1 & 1 & & -1 & -1 & -1 & -1 \\ 1 & -1 & & 1 & -1 & & -1 & 1 & -1 & 1 \\ 1 & 1 & & -1 & -1 & & -1 & -1 & 1 & 1 \\ 1 & -1 & & -1 & 1 & & -1 & 1 & 1 & -1 \end{bmatrix}. \tag{4.6}$$

We can then use the argument of part i by replacing H_{2^n} by $H_{2^{n-1}}$, and conclude that the contribution to the sum in (4.4) due to these columns of ± 1s (not submatrices) is also zero. □

Theorem 4.5 *Let x be the exponential Hadamard waveform. Then,*

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

Proof

i. If $k = 0$, then

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

ii. Let $k > 0$ be given and consider n for which $2^n < k \leqslant 2^{n+1}$. It is enough to show that

$$AC_N[k] = \frac{1}{N} \sum_{m=1}^{N} x[m+k]x[m] \tag{4.7}$$

tends to zero as N goes to infinity. Note that for a given N, $x[N]$ can occur in the middle of a matrix. Each Hadamard matrix of size 2^n has 4^n elements. Recall that each such matrix will be repeated 2^n times. Thus,

$$N = \sum_{j=0}^{n+1} 2^j 4^j + \sum_{j=n+2}^{M} 2^j 4^j + P4^{M+1} + S = Q + R + \tilde{P} + S, \tag{4.8}$$

where $0 \leqslant P < 2^{M+1}$, $0 \leqslant S < 4^{M+1}$, and $M \to \infty$ as $N \to \infty$. Therefore,

$$AC_N[k] = \frac{1}{N}\left[\sum_{m=1}^{Q} x[m+k]x[m] + \sum_{m=Q+1}^{Q+R} x[m+k]x[m] \right. \\ \left. + \sum_{m=Q+R+1}^{Q+R+\tilde{P}} x[m+k]x[m] + \sum_{m=Q+R+\tilde{P}+1}^{Q+R+\tilde{P}+S} x[m+k]x[m]\right]. \tag{4.9}$$

Due to Lemma 4.4, the second and the third sums in (4.9) equal zero. Thus,

$$|AC_N[k]| \leqslant \frac{1}{N}\left(\sum_{m=1}^{Q} |x[m+k]x[m]| + \sum_{m=Q+R+\tilde{P}+1}^{Q+R+\tilde{P}+S} |x[m+k]x[m]|\right) \\ = \frac{1}{N}(Q+S). \tag{4.10}$$

Since Q, which depends on k, is finite, we have $\lim_{N\to\infty} \frac{Q}{N} = 0$. For $\frac{S}{N}$ we have the estimate:

$$\frac{S}{N} < \frac{4^{M+1}}{N} < \frac{4^{M+1}}{\frac{8^{M+1}-1}{7}} \sim 7\frac{1}{2^{M+1}}. \tag{4.11}$$

Since $M \to \infty$ as $N \to \infty$, $\lim_{N\to\infty} \frac{S}{N} = 0$. From (4.10) this means that $AC_N[k] \to 0$ as $N \to \infty$ for $k > 0$. This proves that the autocorrelation is zero for all positive integers k, which, in turn, implies that the autocorrelation is zero for all non-zero k. □

Instead of having the Hadamard matrices repeat exponentially as described in Example 4.2, we can construct unimodular waveforms, whose autocorrelations vanish everywhere expect at the origin, by letting the Hadamard matrices repeat linearly.

Example 4.6 To construct a unimodular waveform 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, H_{2^n} be repeated n times. For the positive integers, let x take values 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 $x[-k] = x[k]$. x is the linear Hadamard waveform.

Lemma 4.4 is also valid for the linear Hadamard waveform; and the proof of the following result is similar to that of Theorem 4.5.

Theorem 4.7 *Let x be the linear Hadamard waveform. Then,*

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

Example 4.8 Let x be the exponential Hadamard waveform. We would like to solve the following problem: given $\epsilon > 0$, find $N \in \mathbb{N}$ such that

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

From (4.10) in the proof of Theorem 4.5, we have

$$|AC_N[k]| \leqslant \frac{1}{N}(Q + S).$$

From (4.11) we know that $\frac{S}{N} < 7\frac{1}{2^{M+1}}$, which is independent of k. Now $Q = \sum_{j=0}^{n+1} 8^j$ and n depends on k since $2^n < k \leqslant 2^{n+1}$, in particular, $\lceil \log_2(k) \rceil = n + 1$. Therefore,

$$Q = \sum_{j=0}^{\lceil \log_2(k) \rceil} 8^j = \frac{8^{\lceil \log_2(k) \rceil + 1} - 1}{7},$$

and so

$$|AC_N[k]| \leqslant \frac{1}{N} \frac{8^{\lceil \log_2(k) \rceil + 1} - 1}{7} + 7\frac{1}{2^{M+1}}. \tag{4.12}$$

Thus, the smallest N such that

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

satisfies the inequality

$$\frac{1}{N} \frac{8^{\lceil \log_2(K) \rceil + 1} - 1}{7} + 7\frac{1}{2^{M+1}} < \epsilon \tag{4.13}$$

where M and N are related by (4.8).

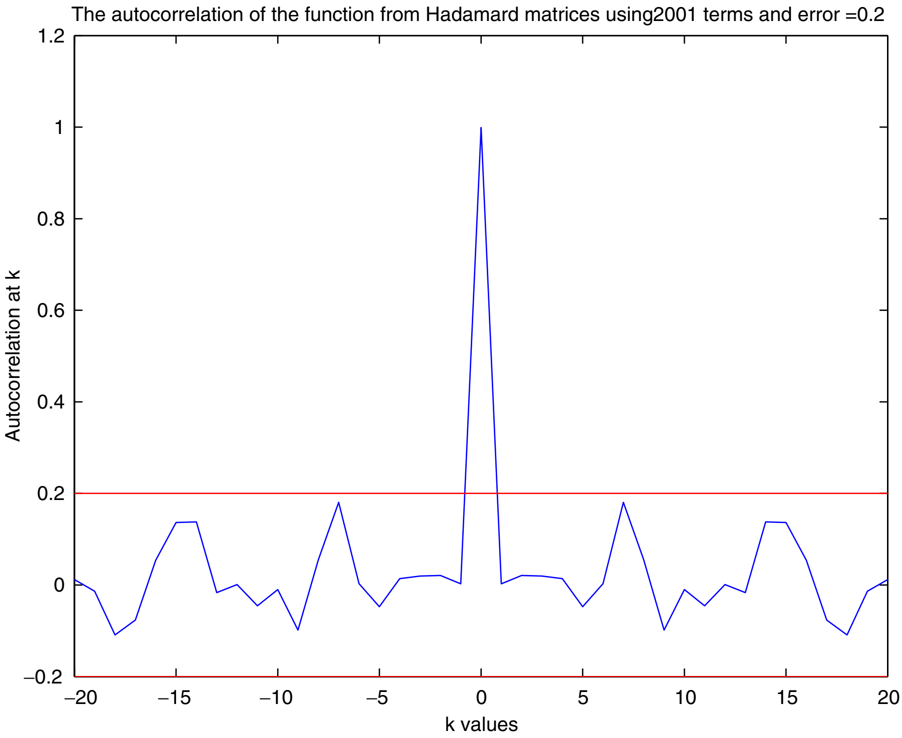

Fig. 1 Error estimates of the exponential Hadamard waveform; $\epsilon = 0.2$

Equation 4.14 gives the values of N obtained via (4.13) for $K = 16$ and several values of ϵ.

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

(4.14)

Remark The actual error estimate for the exponential Hadamard waveform is illustrated in Fig. 1. This estimate is significantly better than that obtained in (4.14). The disparity is a consequence of the difficult counting problems inherent in dealing with Hadamard matrices. However, Fig. 1 does imply a valid use of these waveforms in applications.

Acknowledgement The authors gratefully acknowledge support from ONR Grant N000 14-06-1-000 2 and AFOSR(MURI) Grant FA9550-05-1-0443.

References

1. Auslander, L., Barbano, P.E.: Communication codes and Bernoulli transformations. Appl. Comput. Harmon. Anal. **5**(2), 109–128 (1998)
2. Benedetto, J.J.: A multidimensional Wiener-Wintner theorem and spectrum estimation. Trans. Amer. Math. Soc. **327**(2), 833–852 (1991)
3. Benedetto, J.J.: Harmonic Analysis and Applications. CRC, Boca Raton (1997)
4. Benedetto, J.J., Donatelli, J.J.: Ambiguity function and frame theoretic properties of periodic zero autocorrelation waveforms. IEEE J. Special Topics Signal Process. **1**, 6–20 (2007)
5. Helleseth, T., Kumar, P.V.: Sequences with Low Correlation. Handbook of Coding Theory, vol. I, II, pp. 1765–1853. North-Holland, Amsterdam (1998)
6. Kerby, R.: The correlation function and the Wiener-Wintner theorem in higher dimension. Ph.D. thesis, University of Maryland, College Park (1990)
7. Kuipers, L., Niederreiter, H.: Uniform Distribution of Sequences. Wiley-Interscience [Wiley], New York (1974)
8. Levanon, N., Mozeson, E.: Radar Signals. Wiley Interscience, IEEE Press, New York (2004)
9. Long, M.L.: Radar Reflectivity of Land and Sea. Artech House, London (2001)
10. 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, Mainz, September 1996
11. Nathanson, F.E.: Radar Design Principles—Signal Processing and the Environment. SciTech, Mendham (1999)
12. Stein, E.M., Weiss, G.: Introduction to Fourier Analysis on Euclidean Spaces. Princeton University Press, Princeton (1971)
13. Stimson, G.W.: Introduction to Airborne Radar. SciTech, Mendham (1998)
14. 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)
15. Verdú, S.: Multiuser Detection. Cambridge University Press, Cambridge (1998)
16. Wiener, N.: Generalized harmonic analysis. Acta Math. **55**, 117–258 (1930)
17. Wiener, N., Wintner, A.: On singular distributions. J. Math. Phys. **17**, 233–246 (1939)