Constructive Approximation in Waveform Design

John J. Benedetto

Abstract. Effective waveform design, for topics such as code division multiple access (CDMA), is essential to transmit many messages clearly and simultaneously on the same frequency band so that one user's message does not become another user's noise. Unimodular sequences are an essential characteristic for the applicability in communications and radar of waveforms whose autocorrelations have prescribed zero sets. Constructive approximations of unimodular sequences whose autocorrelations vanish on prescribed sets are made. The analysis depends significantly on Wiener's Generalized Harmonic Analysis and on some number theoretic properties from the theory of uniform distribution of sequences. Periodic CAZAC (constant amplitude zero autocorrelation) codes are also designed.

§1. Introduction

1.1 Basic problem

Let $\mathbb{Z}$ be the integers and let $p = \{p_k : k \in \mathbb{Z}\}$ be a positive definite sequence with a prescribed zero-set on $\mathbb{Z}$. We shall address the *basic problem* of constructing unimodular digital codes u defined on $\mathbb{Z}$ and with the property that the autocorrelation A_u of u is p. Let $\mathbb{C}$ be the complex numbers and recall that $p = \{p_k\}$ is *positive definite*, denoted by $p >> 0$, if

$$\forall N \geq 1 \text{ and } \forall c_1, \ldots, c_N \in \mathbb{C}, \sum_{1 \leq k,m \leq N} c_k \bar{c}_m p_{k-m} \geq 0.$$

The *autocorrelation* $A_u : \mathbb{Z} \to \mathbb{C}$ of $u : \mathbb{Z} \to \mathbb{C}$ is defined as

$$\forall k \in \mathbb{Z}, \quad A_u[k] = \lim_{N \to \infty} \frac{1}{2N+1} \sum_{|m| \leq N} u[k+m]\overline{u[m]},$$

Advances in Constructive Approximation
XXX (eds.), pp. 1–3.

ISBN 0-9728482-x-x

when the limit exists; and u is *unimodular* if $|u[n]| = 1$ for all $n \in \mathbb{Z}$.

We shall distinguish between algebraic and analytic approaches to the basic problem.

There are established algebraic approaches for constructing unimodular codes for solving the basic problem, *e.g.*, [16]. Our algebraic construction is in terms of periodic codes, and it is introduced in Section 7, see Section 1.3.

The main part of this paper deals with the analytic approach for solving the basic problem, and it is inspired by work of L. Auslander and Barbano [2]. Our analytic contribution is in terms of codes on $\mathbb{Z}$. The contribution itself is a technique involving Wiener's Generalized Harmonic Analysis (GHA) and methods from uniform distribution of sequences. The technique is introduced for a special example in Section 5, with supporting material in Sections 3, 4, and 6, see Section 1.4. The purpose of analytic constructions to solve the basic problem, whether it be our technique or that in [2] or others, is to provide flexibility and adaptivity in designing *robust* codes which are stable under modest perturbations.

1.2 Reason for the basic problem

The basic problem arises in several applications in the areas of radar and communications. In the former such codes play a role in effective target recognition, *e.g.*, [2], [19], [22], [25]; and in the latter they are used to address synchronization issues in cellular (phone) access technologies, especially code division multiple access (CDMA), *e.g.*, [27], [28]. The radar and communications methods combine in recent advanced multifunction RF systems (AMRFS).

Because of these applications, the codes to be constructed should exhibit a quantifiable stability under doppler shifts and/or with various additive noises. Our software package, referenced in Section 7, is a tool to evaluate such stability for the periodic algebraic codes constructed in Section 7.

There are two significant reasons that the codes u for solving the basic problem should have constant amplitude. First, a transmitter can operate at peak power if u 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 at the receiver without distorting the message.

1.3 Algebraic periodic version of the basic problem

A strong version of the basic problem is to construct unimodular K-periodic sequences u with the property that A_u vanishes outside of the periodic *dc*-domain points nK, $n \in \mathbb{Z}$. As posed, this is a solvable *algebraic problem*, *e.g.*, [1], [12], [14], [15], [20], [23], [26]; and such sequences are called CAZAC codes, where the palindromic acronym (another scientific one along with "radar") stands for constant amplitude zero autocorrelation. Using the ingenious method due to Milewski, we shall compute several such codes in Section 7. In both radar and CDMA there must also be optimal crosscorrelation behavior among sets of such codes, and our present algebraic CAZAC crosscorrelation results and software are documented in [8].

1.4 Analytic methods to address the basic problem

In the non-periodic version of the basic problem, a natural initial approach for the solution is to invoke *analytic methods* from GHA [29], cf., [6] for a recent extension of Wiener's methods as related to the construction of codes u whose autocorrelations are given positive definite functions. Adapting Wiener's techniques allows one to construct in Section 3 a code $x : \mathbb{Z} \to \mathbb{C}$ for which $A_x = p$ for a given $p >> 0$; however, x is not unimodular.

In order to address the unimodularity constraint, we invoke classical results from the theory of uniform distribution in Section 4, see [18]. As such we deal with certain Gauss-like sums, and this is probably related to code-design in terms of the Heisenberg group by Strohmer.

Using uniform distribution we deal with the basic problem for the case $p = \{p_k\}$, where $p_0 = 1$ and $p_k = 0$ for all $k \neq 0$. Because of the severe restriction of the zero-set of p we can not solve the basic problem completely in this case. However, the simplicity of p allows us to demonstrate in a relatively straightforward way how the results from Section 4 are implemented to ensure the unimodularity constraint. This is the content of Section 5.

A more powerful uniform distribution tool than those listed in Section 4 is the van der Corput difference theorem. In Section 6 we prove a generalization due to Cigler [13]. We fomulate this generalization with the primary goal of solving the basic problem for a given p, and, in the process, of specifying the required constraints on the zero set of p in order to ensure a unimodular code u for which $A_u = p$. Our secondary goal, since the proof uses methods from abstract harmonic analysis (although this may not be obvious), is to prove a version of the difference theorem for pseudo-measures with an eye to spectral synthesis, *e.g.*, [5].

Section 2 assembles some facts needed in the remaining sections.

1.5 Notation

We use the standard notation from harmonic analysis, *e.g.*, [24], [7]. For the real numbers $\mathbb{R}$, we write $\mathbb{T} = \mathbb{R}/\mathbb{Z}$. $C(\mathbb{T})$ is the space of 1-periodic complex valued continuous functions on $\mathbb{R}$, and $A(\mathbb{T})$ is the subspace of absolutely convergent Fourier series. If $F \in A(\mathbb{T})$ we write $F^\vee = f = \{f_k\}$, *i.e.*, $F^\vee[k] = f_k$; and $F(\gamma) = \sum_{k\in\mathbb{Z}} f_k e^{-2\pi i k\gamma}$. There is an analogous definition for $\mu^\vee$ in the case that $\mu \in M(\mathbb{T})$. $M(\mathbb{T})$ is the space of Radon measures on $\mathbb{T}$, i.e., $M(\mathbb{T})$ is the dual space of the Banach space $C(\mathbb{T})$ taken with the sup norm. $M_c(\mathbb{T}) \subseteq M(\mathbb{T})$ designates the space of continuous Radon measures μ, so that $\mu(\{\gamma\}) = 0$ for each $\gamma \in \mathbb{T}$.

§2. Mathematical Preliminaries

Because of the basic problem in Section 1.1 the following elementary fact is necessary.

Lemma 2.1. *Let $S_K = \{k \in \mathbb{Z} : 1 \leq |k| \leq K\}$. There is positive $P \in A(\mathbb{T}) \setminus \{1\}$ for which $p_0 = 1$ and $p_k = 0$ for each $k \in S_K$, where $P(\gamma) = \sum_{k\in\mathbb{Z}} p_k e^{2\pi i k\gamma}$.*

Proof: Recall that if $p = \{p_k\} >> 0$ then $p_{-n} = \overline{p_n}$ and $|p_n| \leq p_0$ for each $n \in \mathbb{Z}$. Choose $\{p_n\} \subseteq \mathbb{R}$; and suppose $p_n = p_{-n}$ for each n, $p_0 = 1$, and $p_n = 0$ for all $n \in S_K$. Set

$$P(\gamma) = 1 + 2 \sum_{k=K+1}^{\infty} p_k \cos 2\pi k\gamma.$$

Clearly, $|P(\gamma) - 1| \leq 2\sum_{k=K+1}^{\infty} |p_k|$ so that if $\{p_k\}$ is absolutely summable and $2\sum_{k=K+1}^{\infty} |p_k| < 1$ then

$$\forall \gamma \in \mathbb{T}, \quad P(\gamma) \geq 1 - 2\sum_{k=K+1}^{\infty} |p_k| > 0.$$

Hence, P is positive and $P \in A(\mathbb{T})$; in particular, $P^\vee = p >> 0$. □

Remark 2.2.

a) Since $P > 0$ on $\mathbb{T}$ in Lemma 2.1, we can use Wiener's lemma on the inversion of absolutely convergent Fourier series.

b) If $F \in A(\mathbb{T})$ then $\lim_{N\to\infty} \|F - S_N(F)\|_{L^\infty(\mathbb{T})} = 0$. In particular, if $F > 0$ on $\mathbb{T}$ then

$$\exists N \text{ such that } \forall n \geq N \text{ and } \forall \gamma \in \mathbb{T},$$

$$\sum_{|k|\leq n} F^\vee[k] e^{-2\pi i k\gamma} > 0.$$

Notationally we let L_n have the property that

$$\forall \gamma \in \mathbb{T}, \quad \sum_{|k|\leq L_n} F^\vee[k]e^{-2\pi ik\gamma} \geq \frac{1}{2}\inf\{F(\lambda) : \lambda \in \mathbb{T}\}.$$

Lemma 2.3. *Let $x : \mathbb{Z} \to \mathbb{C}$ be K-periodic. Then*

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

Proof: The result is a consequence of the following regrouping for a fixed k and a given N:

$$\begin{aligned}\sum_{|m|\leq N} x[k+m]\overline{x[m]} = &\sum_{m=1}^{K} + \sum_{m=K+1}^{2K} \\ &+ \cdots + \sum_{m=K(N_K-1)+1}^{KN_K} + \sum_{m=KN_K+1}^{N} + \sum_{m=-K+1}^{0} \\ &+ \cdots + \sum_{m=-KN_K+1}^{-K(N_K-1)} + \sum_{m=-N}^{-KN_K} \\ = &\, 2N_K\sum_{m=1}^{K} + \sum_{m=KN_K+1}^{N} + \sum_{m=-N}^{-KN_K},\end{aligned}$$

where N_K satisfies $KN_K \leq N < K(N_K+1)$. $\square$

Let $F \in A(\mathbb{T})$ have Fourier coefficients $p = \{p_k\}$, and for any K_n define the discrete measure

$$\mu_K = \sum_{j=0}^{K-1} \frac{1}{K}\left(\sum_{|k|\leq M_K} p_k e^{-2\pi ik(j/K)}\right)\delta_{j/K}, \tag{2.1}$$

where $\delta_{j/n}$ is the Dirac measure at $j/n \in \mathbb{T}$.

Lemma 2.4. *Let $F \in A(\mathbb{T})$ have Fourier coefficients $p = \{p_k\}$ and define μ_K as in (2.1). Assume $M_K \to \infty$ as $K \to \infty$. Then*

$$\forall f \in C(\mathbb{T}), \quad \lim_{K\to\infty}\int_{\mathbb{T}} f(\gamma)d\mu_K(\gamma) = \int_{\mathbb{T}} f(\gamma)F(\gamma)d\gamma.$$

Proof: We have the estimate

$$\left|\int_{\mathbb{T}} f(\gamma)d\mu_K(\gamma) - \int_{\mathbb{T}} f(\gamma)F(\gamma)d\gamma\right|$$
$$\leq \sum_{|k|>M_K} |p_k|\left(\frac{1}{K}\sum_{j=0}^{K-1}|f(\frac{j}{K})|\right)$$
$$+\sum_{k\in\mathbb{Z}}|p_k|\left|\int_0^1 f(\gamma)e^{-2\pi ik\gamma}d\gamma - \frac{1}{K}\sum_{j=0}^{K-1} f(\frac{j}{K})e^{2\pi ik(j/K)}\right|.$$

It is straightforward to check that the right side goes to 0 as $K\to\infty$. □

The following is immediate from the previous discussion.

Lemma 2.5. *Let $F\in A(\mathbb{T})$ have Fourier coefficients $p=\{p_k\}$ and define μ_K as in (2.1).*

a) $\mu_K^\vee : \mathbb{Z}\to\mathbb{C}$ *is K-periodic.*

b) $\forall k\in\mathbb{Z},\quad \mu_K^\vee[k] = \frac{1}{K}\sum_{j=0}^{K-1}\left(\sum_{|\ell|\leq M_K} p_\ell e^{-2\pi i\ell(j/K)}\right)e^{2\pi ik(j/K)}.$

c) If $F>0$ on $\mathbb{T}$, then for each fixed K we can choose L_K (see Remark 2.2b) such that

$$\forall j=0,1,\dots,K-1,$$
$$\left|\sum_{|\ell|\leq L_K} p_\ell e^{-2\pi i\ell(j/K)}\right| = \sum_{|\ell|\leq L_K} p_\ell e^{-2\pi i\ell(j/K)}.$$

§3. The Basic Problem and Wiener's GHA

Suppose we weaken the *basic problem* and pose the following problem: Let $p=\{p_k\}>>0$ have a prescribed zero set; construct a digital code $x:\mathbb{Z}\to\mathbb{C}$ such that $A_x=p$. We have temporarily dropped the constraint of unimodularity.

By the definition of autocorrelation it is not unreasonable to define x in terms of a square root, and in some sense this was the approach of Wiener in his original GHA on $\mathbb{R}$ [29].

Using the approach from Section 2, we set

$$\forall k\in\mathbb{Z},\quad x_K[k] = \sum_{j=0}^{K-1}\left(\sum_{|\ell|\leq L_K}\frac{p_\ell}{K}e^{-2\pi i\ell(j/K)}\right)^{1/2} e^{2\pi ik(j/K)}, \qquad (3.1)$$

where we have chosen L_K as in Lemma 2.5c.

The proof of the following result is straightforward.

Proposition 3.1. *Let $F \in A(\mathbb{T})$ be positive on $\mathbb{T}$ with Fourier coefficients $\{p_k\}$, and let $\mu_K^\vee$ and x_K be as in Lemma 2.5a (with L_K instead of M_K) and (3.1), respectively. Then $\mu_K^\vee, x_K : \mathbb{Z} \to \mathbb{C}$ are K-periodic and*

$$\forall k \in \mathbb{Z}, \quad A_{x_K}[k] = \mu_K^\vee[k].$$

Example 3.2. *Let $F = 1$ on $\mathbb{T}$. Then for any positive $K \in \mathbb{Z}$, $x_K[mK] = \sqrt{K}$ for all $m \in \mathbb{Z}$ and x_K vanishes otherwise.*

The methods to prove the following result go back to Wiener [29], cf., [6]. We shall only outline the proof because of the "non-unimodular" nature of the construction, *e.g.*, Example 3.2, and the subsequent approach with uniform distribution, *e.g.*, Sections 4 and 5.

Theorem 3.3. *Let $F \in A(\mathbb{T})$ be positive on $\mathbb{T}$ with Fourier coefficients $p = \{p_k\}$. There is a constructible sequence $x : \mathbb{Z} \to \mathbb{C}$ for which $A_x = p$. (x is not unimodular.)*

Outline of Proof.

Using the notation in Proposition 3.1 we can prove that there is an increasing positive sequence $\{L_K\}$, as $K \to \infty$, such that

$$\forall k \in \mathbb{Z} \text{ and } \forall N \geq L_K,$$
$$\left| \frac{1}{2N+1} \sum_{|m| \leq N} x_K[k+m]\overline{x_K[m]} - \mu_K^\vee[k] \right| < \frac{1}{2^{K+1}}.$$

It is advantageous to choose the smallest possible L_K at each step. Next, set

$$N_K = (L_1 + 1)(L_2 + 2) \dots (L_K + K).$$

Therefore $N_K \geq K!$, and the sequences $\{N_K\}$, $\{N_{K+1}/N_K\}$, and $\{N_{K+1} - N_K\}$ tend to infinity. Using the definition of x_K in (3.1) we define $x : \mathbb{Z} \to \mathbb{C}$ as follows: $x[k] = 0$ for $|k| < N_1$ and $x[k] = x_K[k]$ for $N_K \leq |K| < N_{K+1}$. It must now be checked that $A_x = p$.

§4. Uniform Distribution

A sequence $\{\theta_n : n = 1, \dots\} \subseteq \mathbb{R}$ is *uniformly distributed mod 1* if, for every interval $[a, b) \subseteq [0, 1)$,

$$\lim_{N \to \infty} \frac{\text{card}\,\{\theta_n : 1 \leq n \leq N, \theta_n - [\theta_n] \in [a, b)\}}{N} = b - a.$$

Here, "card" stands for "cardinality" and $[\theta]$ is the greatest integer less than or equal to $\theta \in \mathbb{R}$, the so-called *integer part* of θ. An excellent reference on uniform distribution is Kuipers and Niederreiter's book [18], cf., [21] for recent advanced results.

We shall need the following three theorems due to Hermann Weyl (1914 and 1916).

Theorem 4.1. *$\{\theta_n : n = 1, \ldots\} \subseteq \mathbb{R}$ is uniformly distributed mod 1 if and only if*

$$\forall f \in C(\mathbb{T}), \quad \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{K} f(\theta_n) = \int_0^1 f(x)dx.$$

Theorem 4.2. *$\{\theta_n : n = 1, \ldots\} \subseteq \mathbb{R}$ is uniformly distributed mod 1 if and only if*

$$\forall h \in \mathbb{Z}\backslash\{0\}, \quad \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i h\theta_n} = 0.$$

Theorem 4.3. *Let $Q(x) = c_m x^m + c_{m-1}x^{m-1} + \cdots + c_0$, $m \geq 1$, be a polynomial where each $c_j \in \mathbb{R}$ and where some $c_j, j > 0$, is irrational. Then $\{Q(n) : n = 1, \ldots\}$ is uniformly distributed mod 1.*

Remark 4.4. Van der Corput (1929 and 1931) gave a simpler proof than Weyl of Theorem 4.3, using the van der Corput difference theorem, see Remark 6.7.

§5. Constructive Approximation to Unimodular Solution

The purpose of this section is to illustrate our GHA – uniform distribution technique for the construction of unimodular digital codes u defined on $\mathbb{Z}$ whose autocorrelation is a prescribed positive definite sequence p.

For simplicity, we choose the particular sequence $p = F^\vee$ where $F = 1$ on $\mathbb{T}$. Thus, $F^\vee[k] = p_k = 0$ for all $k \neq 0$. We provide details to the approximation of unimodular u, in which $A_u = p = \{p_k\}$, for certain summands arising in the overall approximation of u. The remaining summands use uniform distribution discrepancy methods with additional complexity [11]. These will be presented in the sequel, combined with an error analysis of unimodular approximants whose autocorrelations are associated with a given positive definite sequence for which there is no exact solution to the basic problem on $\mathbb{Z}$.

Using the idea of Wiener's construction of x in terms of $\{x_K\}$, see Section 3, we let positive $K \in \mathbb{Z}$ be fixed and define

$$\forall k \in \mathbb{Z}, u_K[k] = \begin{cases} K^{1/2} & \text{if } k = mK, \text{ some } m \in \mathbb{Z}, \\ e^{2\pi i k^2 \gamma_K} & \text{if } k \neq qK \text{ for any } q \in \mathbb{Z}, \end{cases} \tag{5.1}$$

where each γ_K is irrational. Each u_K is "almost" unimodular, and it is not K periodic. Using Wiener's construction from Section 3, for u_K instead of x_K, the resulting digital code u will have longer and longer unimodular segments as $|k|$ increases. Since autocorrelations are characterized by their behavior at infinity this is what we shall mean by the unimodularity of u.

Setting

$$A_{N,y}[k] = \frac{1}{2N+1} \sum_{|m| \leq N} y[k+m]\overline{y[m]}, \tag{5.2}$$

we shall analyze a special but not untypical case of A_{N,u_k} as $N \to \infty$; and then, as mentioned above, we define unimodular u in terms of $\{u_K\}$ as was done for x and $\{x_K\}$ in Section 3.

Writing

$$\sum_{|m| \leq N} y[k+m]\overline{y[m]} = \sum^{(N)} y[k+m]\overline{y[m]}, \tag{5.3}$$

in (5.2), we have

$$A_{N,u_K}[k] = \frac{1}{2N+1} \sum_{m \neq qK}^{(N)} + \frac{1}{2N+1} \sum_{m = qK}^{(N)} = I_{1,K,N}(k) + I_{2,K,N}(k)$$

with u_K replacing y in (5.3). It is easy to check that

$$\lim_{N \to \infty} I_{2,K,N}(pK) = 1 = \mu_K^{\vee}[pK], \tag{5.4}$$

uniformly in $p \in \mathbb{Z}$, where the quadratic term in (5.1) can be replaced by any unimodular term. Also, using the irrationality of γ_K, we compute

$$\forall p \in \mathbb{Z} \backslash \{0\}, \quad \lim_{N \to \infty} I_{1,K,N}(pK) = 0; \tag{5.5}$$

and a direct computation shows that

$$\lim_{N \to \infty} I_{1,K,N}(0) = 1 - \frac{1}{K}. \tag{5.6}$$

Thus,

$$A_{u_K}[0] = \lim_{N \to \infty} A_{N,u_K}[0] = 2 - \frac{1}{K}.$$

With the flexibility of adding non-zero p_k for $|k|$ large, for a given non-negative $F \in A(\mathbb{T})$ with Fourier coefficients $p = \{p_k\}$, we can compute the desired $A_u[0] = 1$. It remains to evaluate

$$\forall k \neq pK, \quad \lim_{N \to \infty} I_{j,K,N}(k), \quad j = 1, 2. \tag{5.7}$$

We shall do the case $j = 2$.

Proposition 5.1. *If $k \neq pK$ then*

$$\lim_{N\to\infty} I_{2,K,N}(k) = 0 = \mu_K^{\vee}[k]. \tag{5.8}$$

Proof: First note that if $k \in \mathbb{Z}\backslash\{pK\}$, $p \in \mathbb{Z}$, then $\mu_K^{\vee}[k] = 0$. In fact, if $k/K \notin \mathbb{Z}$ then $k/K = m + \langle k/K \rangle$, where $\langle k/K \rangle \in (0,1)$ is the fractional part of k/K. Thus, $e^{2\pi ik/K} \neq 1$ and so

$$\begin{aligned} K\mu_K^{\vee}[k] &= \sum_{j=0}^{K-1} (e^{2\pi ik/K})^j \\ &= \frac{1 - e^{2\pi iK(\frac{k}{K} - m)}}{1 - e^{2\pi ik/K}} = 0. \end{aligned}$$

Next, for $k \in \mathbb{Z}\backslash\{pK\}$, we compute

$$\begin{aligned} I_{2,K,N}(k) &= \frac{1}{2N+1} \sum_{m=qK}^{(N)} e^{2\pi i(k+m)^2\gamma_K} \left(\sum_{j=0}^{K-1} \left(\frac{1}{K}\right)^{1/2} e^{-2\pi im(j/K)} \right) \\ &= \frac{K^{1/2}}{2N+1} \sum_{q}^{(N/K)} e^{2\pi i(k+qK)^2\gamma_K}, \end{aligned} \tag{5.9}$$

since $m = qK$ implies $k + m \neq \ell K$. $\{Q(q) = (k+qK)^2\gamma_K : q \in \mathbb{Z}\}$ is uniformly distributed mod 1 by Weyl's Theorem 4.3. The right side of (5.9) is

$$\approx \frac{K^{1/2}}{2N+1} \left(\frac{2N}{K} + 1\right) \frac{1}{2\left[\frac{N}{K}\right] + 1} \sum_{q}^{(N/K)} e^{2\pi iQ(q)},$$

and so it tends to 0 as $N \to \infty$ by Weyl's theorem. Equation (5.8) is proved. □

§6. Implications of Unimodularity

Proposition 6.1. *Let $p = \{p_k\} >> 0$ and assume*

$$\mathcal{Z} = \{k \in \mathbb{Z} : p_k = 0\} \neq \emptyset.$$

Let $\{x[n] = Ce^{i\theta_n} : C > 0\}$ have the property that

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

Then $p_0 = C^2$ *and* $\{\theta_n\}$ *can* not *have the property that*

$$\exists k \in \mathcal{Z} \ \text{ such that } \ \forall m \in \mathbb{Z}, \quad e^{i\theta_{k+m}} = e^{i\theta_k} e^{i\theta_m}. \tag{6.1}$$

Proof: Suppose there is k such that (6.1) holds. Take any $\epsilon > 0$ for which $C^2 \geq \epsilon$. By definition of $k \in \mathcal{Z}$,

$$\exists N_{\epsilon,k} \text{ such that } \forall N > N_{\epsilon,k}, \quad \left| \frac{1}{2N+1} \sum_{|m| \leq N} x[k+m]\overline{x[m]} \right| < \epsilon. \tag{6.2}$$

Equation (6.2) implies

$$\forall N > N_{\epsilon,k}, \quad \frac{C^2}{2N+1} \left| \sum_{|m| \leq N} e^{i\theta_{k+m}} e^{-i\theta_m} \right| < \epsilon$$

and so from (6.1) we have

$$\forall N > N_{\epsilon,k}, \quad \frac{C^2}{2N+1} \left| e^{i\theta_k} \sum_{|m| \leq N} 1 \right| < \epsilon,$$

i.e., $C^2 < \epsilon$, the desired contradiction. □

Given $\{\theta_m : m \in \mathbb{Z}\} \subseteq \mathbb{R}$ and consider the formal mean

$$\forall h, k \in \mathbb{Z}, \quad \rho_{h,k} = \lim_{N \to \infty} \frac{1}{2N+1} \sum_{|m| \leq N} e^{2\pi i h(\theta_{m+k} - \theta_m)}. \tag{6.3}$$

If h is fixed we write

$$\rho_{h,k} = p_h[k];$$

and if k is fixed we write

$$\rho_{h,k} = q_k[h].$$

Note that

$$\forall h, k \in \mathbb{Z}, \quad \rho_{0,k} = 1 \text{ and } \rho_{h,0} = 1. \tag{6.4}$$

Lemma 6.2. *Fix* $h \in \mathbb{Z}$ *and assume* $p_h[k]$ *exists for all* $k \in \mathbb{Z}$*. Then* $p_h >> 0$.

Proof: If $h = 0$ then $p_0[k] = 1$ for all $k \in \mathbb{Z}$ by (6.4). Thus, $p_0 >> 0$. In fact, $\delta_0^\vee = p_0$, and of course δ_0 is a positive measure.

Let $h \in \mathbb{Z}\backslash\{0\}$. Also consider the function $P_{\varphi,N} = \frac{1}{2N+1}(\varphi \mathbf{1}_N) * (\varphi \mathbf{1}_N)^\sim$, where $\varphi : \mathbb{Z} \to \mathbb{C}$, $\mathbf{1}_N : \mathbb{Z} \to \mathbb{C}$ is the characteristic function of $\{-N, \ldots, 0, 1, \ldots, N\}$, and $\sim$ designates involution. For this h set $\varphi[m] = \varphi_h[m] = e^{2\pi i h\theta_m}$. Since p_h exists on $\mathbb{Z}$ it can be shown that

$$\forall k \in \mathbb{Z}, \quad p_h[k] = \lim_{N \to \infty} P_{\varphi_h,N}[k].$$

Since

$$P^{\wedge}_{\varphi_h,N} = \frac{1}{2N+1}|(\varphi_h \mathbf{1}_N)^{\wedge}|^2 \geq 0$$

we have $p_h >> 0$. □

Lemma 6.3. *Fix $k \in \mathbb{Z}$ and assume $q_k[h]$ exists for all $h \in \mathbb{Z}$. Then $q_k >> 0$.*

Proof: If $h, \ell \in F \subseteq \mathbb{Z}$, F a finite set, and let $\{c_h : h \in F\} \subseteq \mathbb{C}$. By hypothesis, there exists

$$\sum_{h,\ell \in F} c_h \overline{c_\ell} q_k[h-\ell]$$

$$= \lim_{N\to\infty} \frac{1}{2N+1} \sum_{|m|\leq N} \sum_{h,\ell\in F} c_h \overline{c_\ell} e^{2\pi i(h-\ell)(\theta_{m+k}-\theta_m)}$$

$$= \lim_{N\to\infty} \frac{1}{2N+1} \sum_{|m|\leq N} \left| \sum_{h\in F} c_h e^{2\pi i h(\theta_{m+k}-\theta_m)} \right|^2 \geq 0. \quad \square$$

Lemma 6.4. *For all $h \in \mathbb{Z}$, assume $p_h : \mathbb{Z} \to \mathbb{C}$ exists, and for all $k \in \mathbb{Z}$, assume $q_k : \mathbb{Z} \to \mathbb{C}$ exists. Then for each $h, k \in \mathbb{Z}$, there exist positive measures $\mu_h, \nu_k \in M(\mathbb{T})$ such that*

$$\forall h, k \in \mathbb{Z}, \quad \mu_h^{\vee}[k] = p_h[k] = \rho_{h,k} = q_k[h] = \nu_k^{\vee}[h].$$

This is a consequence of Herglotz' theorem and Lemmas 6.2 and 6.3.

Lemma 6.5. *Let $x \in \ell^\infty(\mathbb{Z})$ and assume*

$$A_{x,\{N_m\}} : \mathbb{Z} \longrightarrow \mathbb{C}$$

exists, where $\{N_m\} \subseteq \mathbb{N}$ and

$$\forall k \in \mathbb{Z}, \quad A_{x,\{N_m\}}[k] = \lim_{N_m\to\infty} \frac{1}{2N_m+1} \sum_{|n|\leq N_m} x[k+n]\overline{x[n]}. \tag{6.5}$$

$A_{x,\{N_m\}} = \mu^{\vee}_{x,\{N_m\}} >> 0$, where $\mu = \mu_{x,\{N_m\}} \in M(\mathbb{T})$ is a non-negative Radon measure, and

$$\exists \lim_{N\to\infty} \frac{1}{2N+1} \sum_{|k|\leq N} A_{x,\{N_m\}}[k] = \mu(\{0\}) \geq 0, \tag{6.6}$$

where $\mu(\{0\})$ is the μ-measure of the Borel set $\{0\} \subseteq \mathbb{T}$. (Since $x \in \ell^\infty(\mathbb{Z})$ we know there is at least one subsequence $\{N_m\} \subseteq \mathbb{N}$ for which $A_{x,\{N_m\}}$ exists.)

Proof: The argument of Lemma 6.2 is easily extended to give $A_{x,\{N_m\}} >> 0$, so that by Herglotz' theorem we have $A_{x,\{N_m\}} = \mu^{\vee}$ for some non-negative Radon measure, and, in particular, $\mu(\{0\}) \geq 0$.

Next,

$$\frac{1}{2N+1}\sum_{|k|\le N} A[k] = \frac{1}{2N+1}\sum_{|k|\le N}\lim_{N_m\to\infty}\frac{1}{2N_m+1}\sum_{|n|\le N_m} x[k+n]\overline{x[n]}$$

$$= \frac{1}{2N+1}\sum_{|k|\le N}\mu^\vee[k] = \frac{1}{2N+1}\sum_{|k|\le N}\int_{\mathbb{T}} e^{2\pi ik\gamma}\,d\mu(\gamma)$$

$$= \int_{\mathbb{T}}\left(\frac{1}{2N+1}\sum_{|k|\le N} e^{2\pi ik\gamma}\right)d\mu(\gamma).$$

Therefore,

$$\lim_{N\to\infty}\frac{1}{2N+1}\sum_{|k|\le N} A[k] = \lim_{N\to\infty}\int_{\mathbb{T}}\left(\frac{1}{2N+1}\sum_{|k|\le N} e^{2\pi ik\gamma}\right)d\mu(\gamma)$$

$$= \int_{\mathbb{T}}\left(\lim_{N\to\infty}\frac{1}{2N+1}\sum_{|k|\le N} e^{2\pi ik\gamma}\right)d\mu(\gamma),$$

where the second equality is valid by the Lebesgue dominated convergence theorem. In fact, if

$$f_N(\gamma) = \frac{1}{2N+1}\sum_{|k|\le N} e^{2\pi ik\gamma},$$

then $|f_N(\gamma)| \le 1 \in L^1_\mu(\mathbb{T})$, $f_N(0)\to 1$, and $f_N(\gamma)\to 0$ for $\gamma\in[-1/2,1/2)\setminus\{0\}$. Because of this convergence we can also assert that the right side of the second equality is $\mu(\{0\})$. □

We have the following generalization of a theorem due to van der Corput, see [13].

Theorem 6.6. *Given $\{\theta_m\}\subseteq\mathbb{R}$ and the notation $\rho_{h,k}, p_h, q_k, \mu_h, \nu_k$ defined above. Assume $\rho_{h,k}$ exists for all $h,k\in\mathbb{Z}$. Also assume that*

$$\forall h\ne 0,\quad \lim_{K\to\infty}\frac{1}{2K+1}\sum_{|k|\le K}\left|\int_{\mathbb{T}} e^{2\pi ih\gamma}d\nu_k(\gamma)\right|^2 = 0. \tag{6.7}$$

Then $\{\theta_m\}$ is uniformly distributed mod 1.

Proof: Using Weyl's criterion, Theorem 4.2, we shall prove our result by proving that

$$\forall h\in\mathbb{Z}\setminus\{0\},\quad \lim_{N\to\infty}\frac{1}{2N+1}\sum_{|n|\le N} e^{2\pi ih\theta_n} = 0. \tag{6.8}$$

Suppose (6.8) is not true. We shall obtain a contradiction.

There is $h \in \mathbb{Z} \setminus \{0\}$ such that

$$\overline{\lim}_{N\to\infty} |M_N(\phi_h)| = r > 0, \tag{6.9}$$

where

$$M_N(\phi_h) = \frac{1}{2N+1} \sum_{|n|\le N} \phi_h[n] \quad \text{and} \quad \phi_h[n] = e^{2\pi i h \theta_n}.$$

Choose $\{N_m^{'}\} \subseteq \mathbb{N}$ such that

$$\lim_{N_m^{\prime}\to\infty} |M_{N_m^{\prime}}(\phi_h)| = r,$$

and, without loss of generality, assume that

$$\forall m, \quad \frac{r}{2} \le |M_{N_m^{\prime}}(\phi_h)| \le \frac{3r}{2}.$$

Thus, $\{M_{N_m^{\prime}}(\phi_h)\} \subseteq \{z \in \mathbb{C} : r/2 \le |z| \le 3r/2\}$, and so we can choose a subsequence $\{N_m\} \subseteq \{N_m^{'}\}$ for which

$$\exists \lim_{N_m\to\infty} M_{N_m}(\phi_h) = m(\phi_h) \in \mathbb{C}, \tag{6.10}$$

where $0 < r/2 \le |m(\phi_h)| \le 3r/2$.

For $h \in \mathbb{Z} \setminus \{0\}$ as in (6.9) and $\{N_m\}$ as in (6.10), we invoke Lemma 6.5 for the case $x = \phi_h$. Equation (6.5) is satisfied in this case by our hypothesis on the existence of p_h on $\mathbb{Z}$, since the limit is taken over all $N \in \mathbb{N}$ in (6.3). Thus, by Lemma 6.5, since

$$\forall k \in \mathbb{Z}, \quad \exists \lim_{N_m\to\infty} \frac{1}{2N_m+1} \sum_{|n|\le N_m} e^{2\pi i h(\theta_{n+k}-\theta_n)} = A[k],$$

we have $A = A_{\phi_h,\{N_m\}} >> 0$, $A = \mu^\vee = \mu^\vee_{\phi_h,\{N_m\}}$, $\mu \in M(\mathbb{T})$ is non-negative, and

$$\lim_{N\to\infty} \frac{1}{2N+1} \sum_{|n|\le N} A[n] = \mu(\{0\}) \ge 0.$$

Let $\psi_h = \phi_h - m(\phi_h)$ so that

$$\lim_{N_m\to\infty} M_{N_m}(\psi_h) = 0. \tag{6.11}$$

Also,

$$\phi_h[k+n]\overline{\phi_h[n]}$$
$$= |m(\phi_h)|^2 + \psi_h[k+n]\overline{\psi_h[n]} + m(\phi_h)\overline{\psi_h[n]} + \overline{m(\phi_h)}\psi_h[k+n]. \quad (6.12)$$

Since $A_{\phi_h,\{N_m\}}$ exists and because of (6.11), we obtain from (6.12) that $A_{\psi_h,\{N_m\}}$ exists and

$$\forall k \in \mathbb{Z}, \quad A_{\phi_h,\{N_m\}}[k] = |m(\phi_h)|^2 + A_{\psi_h,\{N_m\}}[k]. \quad (6.13)$$

Applying Lemma 6.5 to (6.13) we see that

$$\exists \lim_{N\to\infty} M_N(A_{\phi_h,\{N_m\}}) = |m(\phi_h)|^2 + \lim_{N\to\infty} M_N(A_{\psi_h,\{N_m\}})$$
$$= |m(\phi_h)|^2 + \mu_{\psi_h,\{N_m\}}(\{0\}) \geq |m(\phi_h)|^2. \quad (6.14)$$

Thus,

$$\mu_{\phi_h,\{N_m\}}(\{0\}) \geq |m(\phi_h)|^2,$$

and, in fact,

$$\mu_h(\{0\}) \geq |m(\phi_h)|^2 \quad (6.15)$$

since $\mu_{\phi_h,\{N_m\}} = \mu_h$ by our hypothesis on the existence of $p_h = \mu_h^\vee$.

Because of (6.7) and Lemma 6.4 we have

$$\forall j \neq 0, \quad \lim_{K\to\infty} \frac{1}{2K+1} \sum_{|k|\leq K} \left| \int_{\mathbb{T}} e^{2\pi i k\gamma} d\mu_j(\gamma) \right|^2 = 0.$$

We invoke Wiener's theorem characterizing continuous measures, *e.g.*, [17], page 42, cf., [5], pages 84 and 98, for an analogous result for continuous pseudo-measures. Thus, $\mu_j \in M_c(\mathbb{T})$ for $j \neq 0$, and of course we know that $\mu_0 = \delta_0 \notin M_c(\mathbb{T})$. Hence,

$$\forall j \neq 0 \text{ and } \forall \gamma \in \mathbb{T}, \quad \mu_j(\{\gamma\}) = 0. \quad (6.16)$$

Combining (6.15) and (6.16) we see that $m(\phi_h) = 0$, and this is the desired contradiction. □

Remark 6.7a. Besides the aforementioned work of Cigler, the argument of Theorem 6.6 has close connections to work of Bass [3], [4] and Bertrandias [9], [10]. Our point of view is to present it with an eye to generalization in terms of pseudo-measures to study further number theoretic properties in spectral synthesis, e.g., [5].

b. The proof of Wiener's theorem used in Theorem 6.6 involves the following elementary facts, *e.g.*, [17], page 42:

$$\forall \mu \in M(\mathbb{T}) \text{ and } \forall \gamma \in \mathbb{T}, \quad \mu(\{\gamma\}) = \lim_{N\to\infty} \frac{1}{2N+1} \sum_{|m|\leq N} \mu^\vee[m] e^{-2\pi i m\gamma}$$

and in particular

$$\sum_{\lambda\in\mathbb{T}} |\mu\{\gamma\}|^2 = \lim_{N\to\infty} \frac{1}{2N+1} \sum_{|m|\le N} |\mu^\vee[m]|^2.$$

c. Using (6.7) and its implication (6.16), we make the following calculation. By (6.16), for every $h \neq 0$,

$$\begin{aligned}
0 &= \mu_h(\{0\}) \\
&= \lim_{K\to\infty} \frac{1}{2K+1} \sum_{|k|\le K} \mu_h^\vee[k] \\
&= \lim_{K\to\infty} \frac{1}{2K+1} \sum_{|k|\le K} \int_{\mathbb{T}} e^{2\pi ik\gamma} d\mu_h(\gamma) \\
&= \lim_{K\to\infty} \frac{1}{2K+1} \sum_{|k|\le K} \rho_{h,k} \\
&= \lim_{K\to\infty} \frac{1}{2K+1} \sum_{|k|\le K} \lim_{N\to\infty} \frac{1}{2N+1} \sum_{|m|\le N} e^{2\pi ih(\theta_{m+k}-\theta_m)} \\
&= \lim_{N\to\infty} \frac{1}{2N+1} \sum_{|m|\le N} e^{-2\pi ih\theta_m} \left(\lim_{K\to\infty} \frac{1}{2K+1} \sum_{|k|\le K} e^{2\pi ih\theta_{m+k}} \right) \\
&= \lim_{N\to\infty} \frac{1}{2N+1} \sum_{|m|\le N} e^{-2\pi ih\theta_m} \left(\lim_{K\to\infty} \frac{1}{2K+1} \sum_{p=-K+m}^{K+m} e^{2\pi ih\theta_p} \right) \\
&= \left| \lim_{N\to\infty} \frac{1}{2N+1} \sum_{|m|\le N} e^{2\pi hi\theta_m} \right|^2.
\end{aligned}$$

If this calculation were valid we would have

$$\forall h \neq 0, \quad \lim_{N\to\infty} \frac{1}{2N+1} \sum_{|m|\le N} e^{2\pi ih\theta_m} = 0;$$

and so, by Weyl's theorem (Theorem 4.2), we would obtain the assertion of Theorem 6.6 that $\{\theta_m\}$ is uniformly distributed mod 1. This direct calculational "proof" of Theorem 6.6 is flawed by the fact that we have not been able to verify the interchange of limits in the middle of the calculation.

Remark 6.8. Fix $k \neq 0$. Suppose

$$\forall h \neq 0, \quad q_k[h] = 0. \tag{6.17}$$

Equation (6.17) is the assertion that

$$\forall h \neq 0, \quad \lim_{N\to\infty} \frac{1}{2N+1} \sum_{|m|\leq N} e^{2\pi i h(\theta_{m+k}-\theta_m)} = 0,$$

i.e., by Weyl's theorem, (6.17) is the assertion that for this $k \neq 0$, $\{\theta_{m+k} - \theta_m\}_{m\in\mathbb{Z}}$ is uniformly distributed mod 1. Further, if (6.17) is valid for all $k \neq 0$, then

$$\forall h \neq 0, \quad \lim_{K\to\infty} \frac{1}{2K+1} \sum_{|k|\leq K} \left| \int_{\mathbb{T}} e^{-2\pi i h\gamma} d\nu_k(\gamma) \right|^2 = 0. \tag{6.18}$$

In fact, for $h \neq 0$ and $k \neq 0$,

$$\int_{\mathbb{T}} e^{-2\pi i h\gamma} d\nu_k(\gamma) = q_k[h] = 0.$$

Thus, we have shown that *if* $\{\theta_{m+k}-\theta_m\}_{m\in\mathbb{Z}}$ *is uniformly distributed mod 1 for each* $k \neq 0$ *then* (6.18) *is valid.* Hence the hypothesis of Theorem 6.6 is more general than assuming $\{\theta_{m+k} - \theta_m\}_{m\in\mathbb{Z}}$ is uniformly distributed mod 1 for each $k \neq 0$; *but we must prove this is strict generality.*

Van der Corput's original formulation of Theorem 6.6 assumed that $\{\theta_{m+k} - \theta_m\}_{m\in\mathbb{Z}}$ is uniformly distributed mod 1 for each $k \neq 0$; and his proof used his so-called "fundamental inequality", *e.g.*, [18], page 25. This formulation is called the *van der Corput difference theorem*: *Let* $\{\theta_m\}_{m\in\mathbb{Z}} \subseteq \mathbb{R}$. *If for each* $k \in \mathbb{Z}\backslash\{0\}$, $\{\theta_{m+k} - \theta_m\}_{m\in\mathbb{Z}}$ *is uniformly distributed mod 1, then* $\{\theta_m\}_{m\in\mathbb{Z}}$ *is uniformly distributed mod 1.*

As mentioned in Remark 4.4, a consequence of the van der Corput difference theorem is Weyl's *uniform distribution* theorem for polynomials (Theorem 4.3), which we used in our unimodular argument. This is *Theorem 3.2* of [18].

§7. Periodic CAZAC codes

We now list some K-periodic CAZAC codes that we have computed "by hand" using an algebraic method introduced by Milewski [20]. Recall from Section 1 that the usefulness of CAZAC codes often depends on cross-correlation properties of sets of such codes having the same length K. These properties, along with critical symmetry and anti-symmetry properties, are not included in this section and will appear in forthcoming work. Let $e(x) = e^{2\pi i x}$. For several values of $K \geq 3$, an associated CAZAC code is listed.

$K = 3:$

$$1, 1, e(1/3).$$

$K = 4:$

$$1, 1, 1, -1.$$

$K = 8:$

$$1, 1, e(1/4), -1, 1, -1, e(1/4), 1.$$

$K = 12:$

$$1, 1, 1, e(1/6), e(1/3), e(2/3), 1, -1, 1, e(2/3), e(1/3), e(1/6).$$

$K = 27:$

$$1, 1, 1, 1, e(1/9), e(2/9), e(1/3), e(5/9), (7/9),$$
$$1, e(1/3), e(2/3), 1, e(4/9), e(8/9), e(1/3), e(8/9), e(4/9),$$
$$1, e(2/3), e(1/3), 1, e(7/9), e(5/9), e(1/3), e(2/9), e(1/9).$$

$K = 48:$

$$1, 1, 1, 1, 1, e(1/12), e(1/6), e(1/4), e(1/3), -1, e(2/3), e(5/6),$$
$$1, e(1/4), -1, e(3/4),$$
$$1, e(1/3), e(2/3), 1, e(1/3), e(3/4), e(1/6), e(7/12),$$
$$1, -1, 1, -1, 1, e(7/12), e(1/6), e(3/4),$$
$$e(1/3), 1, e(2/3), e(1/3), 1, e(3/4), -1, e(1/4),$$
$$1, e(5/6), e(2/3), -1, e(1/3), e(1/4), e(1/6), e(1/12).$$

Inspired by Milewski's procedure, we have constructed user friendly computer software with the following properties:

- It is a CAZAC code generator for codes of arbitrary length;
- It provides automatic autocorrelation and crosscorrelation computation;
- It provides computation and graphics for analyzing the behavior of CAZAC codes under doppler shifts and for some additive noises. The associated computer program can be accessed at

  http://www.math.umd.edu/∼jjb /cazac,

  and the associated documentation and report is [8].

Acknowledgments. The author gratefully acknowledges support from NSF DMS Grant 0139759 and ONR Grant N000140210398.

References

1. Alltop, W. O., Complex sequences with low periodic correlations, IEEE Trans. Info. Theory **26** (1980), 350–354.

2. Auslander, L. and Barbano, P. E., Communication codes and Bernoulli transformations, Appl. and Comp. Harm. Anal. **5** (1998), 109–128.
3. Bass, J., Suites uniformément denses, moyennes trigonométriques, fonctions pseudo-aléatoires, Bull. Soc. Math. France **87** (1959), 1–64.
4. Bass, J., *Fonctions de Corrélation, Fonctions Pseudo-Aléatoires, et Applications*, Masson, Paris, 1984.
5. Benedetto, J. J., *Spectral Synthesis*, Academic Press, New York, 1975.
6. Benedetto, J. J., A multidimensional Wiener-Wintner theorem and spectrum estimation, Trans. Amer. Math. Soc. **327** (1991), 833–852.
7. Benedetto, J. J., *Harmonic Analysis and Applications*, CRC Press, Boca Raton, FL, 1997.
8. Benedetto, J. J. and Ryan, J. F., Implementation and applications of CAZAC codes, University of Maryland Technical Report, 2004.
9. Bertrandias, J.-P., Fonctions pseudo-aléatoires, et fonctions presque périodiques, C. R. Acad. Sci., Paris, **255** (1962), 2226–2228.
10. Bertrandias, J.-P., et al., *Espaces de Marcinkiewicz, Corrélations, Mesures, Systèmes Dynamiques*, Masson, Paris, 1987.
11. Chazelle, B., *The Discrepancy Method: Randomness and Complexity*, Cambridge University Press, 2000.
12. Chu, D. C., Polyphase codes with good periodic correlation properties, IEEE Trans. Inform. Theory **18** (1972), 531–532.
13. Cigler, J., Über eine Verallgemeinerung des Hauptsatzes der Theorie der Gleichverteilung, J. Reine Angew. Math. **210** (1962), 141–147.
14. Frank, R. L. and Zadoff, S. A., Phase shift pulse codes with good periodic correlation properties, IRE Trans. Inform. Theory **8** (1962), 381–382.
15. Heimiller, R. C., Phase shift pulse codes with good periodic correlation properties, IRE Trans. Inform. Theory **6** (1961), 254–257.
16. Helleseth, T. and Kumar, P. V., Sequences with low correlation, in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, editors, Elsevier Publishers, 1998, Chapter 21.
17. Katznelson, Y., *An Introduction to Harmonic Analysis*, Dover Publications, New York, 1976 (1968).
18. Kuipers, L. and Niederreiter, H., *Uniform Distribution of Sequences*, John Wiley & Sons, NY, 1974.
19. Long, M. L., *Radar Reflectivity of Land and Sea*, Artech House, 2001.
20. Milewski, A., Periodic sequences with optimal properties for channel estimation and fast start-up equalization, IBM J. Res. Dev. **27** (1983), 426–430.

21. Montgomery, H. L., *Ten Lectures on the Interface between Analytic Number Theory and Harmonic Analysis*, American Mathematical Society–CBMS, number 84, Providence, RI, 1994.

22. Nathanson, F. E., *Radar Design Principles-Signal Processing and the Environment*, SciTech Publishing Inc., Mendham, NJ, 1999.

23. Rohrs, U. H. and Linde, L. P., Some unique properties and applications of perfect squares minimum phase CAZAC sequences, in *Proc. South African Symp. on Communications and Signal Processing* 1992, 155–160.

24. Stein, E. M. and Weiss, G., *An Introduction to Fourier Analysis on Euclidean Spaces*, Princeton University Press, Princeton, NJ, 1971.

25. Stimson, G. W., *Introduction to Airborne Radar*, 2nd edition, SciTech Publishing, Inc., Mendham, NJ, 1998.

26. Turyn, R., Sequences with small correlations, in *Error Correcting Codes*, H. B. Mann (ed.), John Wiley & Sons, Inc., New York, 1968, 195–228.

27. Ulukus, S. and Yates, R. D., Iterative construction of optimum signature sequence sets in synchronous CDMA systems, IEEE Trans. Inform. Theory **47** (2001), 1989–1997.

28. Verdú, S., *Multiuser Detection*, Cambridge University Press, Cambridge, UK, 1998.

29. Wiener, N., Generalized harmonic analysis, Acta Math. **55** (1930), 117–258.

John J. Benedetto
Department of Mathematics
University of Maryland
College Park, Maryland 20742
jjb@math.umd.edu
http://www.math.umd.edu/~jjb/