J Fourier Anal Appl (2012) 18:471–487
DOI 10.1007/s00041-011-9204-3

Optimal Ambiguity Functions and Weil's Exponential Sum Bound

John J. Benedetto · Robert L. Benedetto · Joseph T. Woodworth

Received: 6 July 2011 / Published online: 5 November 2011
© Springer Science+Business Media, LLC 2011

Abstract Complex-valued periodic sequences, u, constructed by Göran Björck, are analyzed with regard to the behavior of their discrete periodic narrow-band ambiguity functions $A_p(u)$. The Björck sequences, which are defined on $\mathbb{Z}/p\mathbb{Z}$ for $p > 2$ prime, are unimodular and have zero autocorrelation on $(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$. These two properties give rise to the acronym, CAZAC, to refer to constant amplitude zero autocorrelation sequences. The bound proven is $|A_p(u)| \leq 2/\sqrt{p} + 4/p$ outside of $(0, 0)$, and this is of optimal magnitude given the constraint that u is a CAZAC sequence. The proof requires the full power of Weil's exponential sum bound, which, in turn, is a consequence of his proof of the Riemann hypothesis for finite fields. Such bounds are not only of mathematical interest, but they have direct applications as sequences in communications and radar, as well as when the sequences are used as coefficients of phase-coded waveforms.

Keywords Discrete narrow-band ambiguity function · Weil's Riemann hypothesis · Kloosterman sums · Constant amplitude zero autocorrelation sequences

Mathematics Subject Classification (2010) Primary 42A99 · Secondary 11T23 · 11T24 · 94A12

Communicated by Thomas Strohmer.

J.J. Benedetto (✉) · J.T. Woodworth
Norbert Wiener Center, Department of Mathematics, University of Maryland, College Park, MD 20742, USA
e-mail: jjb@math.umd.edu
url: http://www.math.umd.edu/~jjb

J.T. Woodworth
e-mail: joseph.woodworth@gmail.com

R.L. Benedetto
Department of Mathematics, Amherst College, Amherst, MA 01002, USA
e-mail: rlb@math.amherst.edu
url: http://www.cs.amherst.edu/~rlb

1 Introduction

1.1 Purpose

Let $\mathbb{Z}$ denote the ring of integers and let $\mathbb{C}$ denote the field of complex numbers. Given an integer N, form the ring $\mathbb{Z}/N\mathbb{Z}$ of integers modulo N.

Definition 1.1 Let $u : \mathbb{Z}/N\mathbb{Z} :\to \mathbb{C}$ be an N-periodic sequence. The *discrete narrow band ambiguity function*, $A_N(u) : \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$, is defined to be

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

for all $(m,n) \in \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

The *discrete autocorrelation* of u is the function $A_N(u)[\cdot,0] : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$.

The ambiguity function in Definition 1.1 stems from P.M. Woodward's definition of the *narrow band ambiguity function* defined on $\mathbb{R} \times \mathbb{R}$ [37].

Definition 1.2 An N-periodic sequence $u : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ is *constant amplitude zero autocorrelation* (*CAZAC*) if it satisfies the following properties:

$$\text{(CA)} \quad |u[k]| = 1 \quad \text{for all } k \in \mathbb{Z}/N\mathbb{Z}, \quad \text{and}$$

$$\text{(ZAC)} \quad C(u)[m] = \frac{1}{N}\sum_{k=0}^{N-1} u[m+k]\overline{u[k]} = 0 \quad \text{for all } m \in \mathbb{Z}/N\mathbb{Z} \smallsetminus \{0\}.$$

Clearly, $C(u)[m] = A_N(u)[m,0]$ for each $m \in \mathbb{Z}/N\mathbb{Z}$. Equation (CA) is the condition that u has constant amplitude 1. Equation (ZAC) is the condition that u has zero autocorrelation.

Our setting is almost exclusively limited to the case that $N = p$ is prime. As such, $\mathbb{Z}/p\mathbb{Z}$ is a field.

We shall use a remarkable construction of *CAZAC* sequences u_p of prime length p to prove optimal behavior of $A_p(u_p)$. The construction is due to Göran Björck [8, 9]. By *optimal behavior*, we mean that if p is an odd prime, then

$$|A_p(u_p)[m,n]| < \frac{2}{\sqrt{p}} + \frac{4}{p} \quad \text{for all } (m,n) \in (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \smallsetminus \big\{(0,0)\big\}, \qquad (1)$$

see Theorem 3.8. By comparison, a short and elementary calculation shows that for any *CAZAC* u,

$$\max\big\{|A_p(u)[m,n]| : (m,n) \in (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \smallsetminus \big\{(0,0)\big\}\big\} \geq \frac{1}{\sqrt{p-1}},$$

and therefore the bound (1) above is indeed of optimal order of magnitude.

Remark 1.3 The proof of Theorem 3.8 requires André Weil's exponential sum bound, [35], which is a consequence of his proof of the Riemann Hypothesis for curves over finite fields, [36], announced in the Comptes Rendus in 1940. Further, it seems unlikely that there are more elementary means to prove the inequality (1). In fact, in estimating $A_p(u_p)$, the critical term to estimate is a Kloosterman sum; and, if there were an easier way to bound it by $C/\sqrt{p}$, then there would be an easier way to prove Weil's bound for Kloosterman sums, which is an essential consequence of [35] and which has withstood the test of time vis a vis evolutionary simplification.

Remark 1.4 Notwithstanding the level of mathematics required to prove the inequality (1), as noted in Remark 1.3, we emphasize that our coding and implementation of Björck's *CAZAC* sequences is truly elementary. In this regard, see [7], as well as earlier Björck experiments and constructions by one of the authors, e.g., see [6] and references therein, cf. Remark 1.5. In the parlance of waveform design, Theorem 3.8 is an ideal discrete "thumbtack" narrow band ambiguity function which can be used to design ideal phase-coded waveforms devoid of any substantial time or Doppler coupling in the continuous narrow band ambiguity function plane. With regard to hardware implementation of these phase-coded waveforms (as well as others stemming from low correlation sequences), the power, bandwidth, and hardware requirements will introduce noise. It is understood that modifications must be made to the formulation of a given low correlation sequence to permit implementation while controlling this noise.

1.2 Background

The study of *CAZAC* sequences and of other sequences related to optimal autocorrelation behavior has origins in several important applications, one of the most prominent being in the general area of waveform design associated with radar and communications, see, e.g., according to year of publication [2, 3, 6, 10–12, 16, 20–22, 24, 25, 27, 31, 33, 34]. There are hundreds of articles in this area and so this selection may seem arbitrary, although several of these references contain focused lists of contributions and specific applications. Also see Remark 1.5.

There are also purely mathematical origins for the construction of *CAZAC* sequences. One such origin is due to Norbert Wiener, e.g., see new related constructions in [4, 5]. Another may be said to have originated in a question by Per Enflo in 1983. This particular mathematical path has been documented and built upon by Bahman Saffari [28]. Enflo's question is the following for a given odd prime p. *Is it true that the Gaussian sequences*, $u : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$, *defined by*

$$u[k] = \zeta_p^{rk^2+sk}, \quad k = 0, 1, \ldots, p-1,$$

where $\zeta_p = e^{2\pi i/p}$, $r, s \in \mathbb{Z}$ *and* p *does not divide* r, *are the only unimodular sequences of length* p, *with* $u[0] = 1$, *whose Discrete Fourier Transform (DFT) has modulus* 1? This is equivalent to asking whether such sequences u with $u[0] = 1$ are the only bi-unimodular sequences of odd prime length. Enflo was interested in this because of a problem dealing with exponential sums.

Enflo's question has a positive answer for $p = 3$ and $p = 5$. In 1984, by computer search, Björck discovered counterexamples to the Enflo question for $p = 7$ and $p = 11$, see [8]. Later in 1985, Björck saw the role of Legendre symbols in his counterexamples, and this led to his theorems in [9]. It also led to a host of mathematical problems, many still unresolved, about the number of *CAZAC* sequences for a given length, see, [5–7, 14], as well as a several valuable oral and email communications by Saffari [29].

Remark 1.5 (a) It is relevant to mention a striking recent application of low correlation sequences to radar in terms of compressed sensing [17]. In this case, the authors use Alltop sequences [1] Theorem 2, cf. [32] Sect. 2.1.3. It then becomes natural to think in terms of frames generated by Björck sequences for extending the high-resolution radar/compressed sensing setting of the authors of [17].

In fact, the correlation result we prove in Theorem 3.8 is equivalent to the mutual coherence property of finite Gabor frames. This property is reflected by the maximal magnitude of the pairwise inner products of Gabor frame elements. Consequently, Theorem 3.8 can be interpreted as constructing a Gabor frame with essentially optimally low coherence. Naturally, this can lead to its effective numerical implementation using methods such as orthogonal matching pursuit (OMP). This approach is developed in [7].

(b) Another approach to the problem addressed in Sect. 1.1 is found in [13], cf. [23]. The authors obtain bounds comparable to those found herein, but their class of signals, called the oscillator system, is not necessarily *ZAC* although excellent cross-correlation criteria are obtained, something we have not pursued. More important, from the point of view of application, the characterization and construction of the oscillator system are decidedly representation theoretic. As such an explicit algorithm associated with the collection of split tori in Sp requires a Bruhat decomposition.

(c) The companion, [7], of this paper not only exhibits the simplicity of implementation stressed in Remark 1.4, but also reflects the combinatorial and geometrical complexity in the ambiguity function domain due to the role of the Legendre symbol in defining Björck sequences. Some of this complexity is characterized by intricate Latin and magic square patterns. Further, the simplicity of implementation gives rise to useful, efficient bounds off of small neighborhoods of $(0, 0)$ in the ambiguity function domain for compactly supported waveforms on $\mathbb{R}$ having p lags whose coefficients are the elements of a Björck sequence u_p. Also, it is not difficult to see that, as with the oscillator system, there is Fourier invariance of Björck sequences, most simply calculated in the $p \equiv 1 \pmod 4$ case, e.g., [26].

1.3 Outline

We define Björck sequences in Sect. 2. Properties of Kloosterman sums are proven in Sect. 3.1. These, in turn, are used along with Weil's results and the proper decomposition formula to express Björck sequences in the way that allows us to prove Theorem 3.8 in Sect. 3.2. Section 4 provides figures and data which motivated and guided us.

2 Björck Sequences and Multiplicative Characters

For each prime number p, recall that the *Legendre symbol* modulo p is the function $\chi = (\frac{\cdot}{p}) : \mathbb{Z}/p\mathbb{Z} \to \{+1, 0, -1\}$ given by

$$\chi[k] = \left(\frac{k}{p}\right) = \begin{cases} +1 & \text{if } k \equiv m^2 \pmod{p} \text{ for some } m \in \mathbb{Z}/p\mathbb{Z}^\times, \\ 0 & \text{if } k \equiv 0 \pmod{p}, \\ -1 & \text{if } k \not\equiv m^2 \pmod{p} \text{ for all } m \in \mathbb{Z}/p\mathbb{Z}. \end{cases}$$

The preimage of $+1$ under the Legendre symbol function is the set $\mathcal{Q}$ of nonzero *quadratic residues* modulo p; and the preimage of -1 under the Legendre symbol function is the set $\mathcal{Q}^C$ of *quadratic nonresidues* modulo p. Among the many properties of the Legendre symbol, we shall use the fact that it is a character of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. This means that χ, when restricted to $(\mathbb{Z}/p\mathbb{Z})^\times$, is a group homomorphism into $\mathbb{C}^\times$; see [15], Chaps. V and VI.

Definition 2.1 The *Björck sequence* of length p, where p is a prime and $p \equiv 1 \pmod 4$, is defined by

$$u[k] = \exp\big(i\theta\chi(k)\big) = \exp\left(i\theta\left(\frac{k}{p}\right)\right), \quad \text{where } \theta = \arccos\left(\frac{1}{1+\sqrt{p}}\right),$$

for all $k \in \mathbb{Z}/p\mathbb{Z}$.

The *Björck sequence* of length p, where p is a prime and $p \equiv 3 \pmod 4$, is defined by

$$u_p[k] = \begin{cases} \exp(i\phi) & \text{if } k \in \mathcal{Q}^C \subseteq (\mathbb{Z}/p\mathbb{Z})^\times, \text{ where } \phi = \arccos(\frac{1-p}{1+p}), \\ 1 & \text{otherwise,} \end{cases}$$

for all $k \in \mathbb{Z}/p\mathbb{Z}$.

In the case $p \equiv 1 \pmod 4$, Definition 2.1 is equivalent to the following definition for the Legendre symbol sequence $\{0, 1, \ldots, -1, \ldots, 1\}$ of length p. We replace the first term 0 by 1, every term 1 by

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

and every term -1 by the complex conjugate of η; see [28] for a modest generalization. As proven by Björck and differently in [7], we obtain a *CAZAC*, and hence biunimodular, sequence with three values, viz., 1 at $k = 0$, and η and $\overline{\eta}$ at $k \in (\mathbb{Z}/p\mathbb{Z})^\times$.

In the case $p \equiv 3 \pmod 4$, Definition 2.1 is equivalent to the following definition for the Legendre symbol sequence $\{0, 1, \ldots, -1\}$ of length p. Replace the first term 0 by 1, and replace every -1 by

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

As proven by Björck and differently in [7], we obtain a *CAZAC*, and hence bi-unimodular, sequence with only two values, viz., 1 and ξ.

3 The Main Theorem

3.1 The Legendre Symbol and Kloosterman Sums

Definition 3.1 Let p be a prime. For any integers a, b, the quantity

$$K[a,b;p] = \sum_{x\in\mathbb{Z}/p\mathbb{Z}^\times} \exp\bigl(2\pi i\bigl(ax + bx^{-1}\bigr)/p\bigr),$$

where x^{-1} denotes the multiplicative inverse of x in the field $\mathbb{Z}/p\mathbb{Z}$, is a *Kloosterman sum.*

Kloosterman sums are always real-valued, as the following Lemma states.

Lemma 3.2 *Let p be a prime. Then $K[a,b;p] \in \mathbb{R}$ for all integers $a, b \in \mathbb{Z}$.*

Proof By the substitution $y = -x$, we have

$$\overline{K[a,b;p]} = \sum_{x\in\mathbb{Z}/p\mathbb{Z}^\times} e^{-2\pi i(ax+bx^{-1})/p} = \sum_{y\in\mathbb{Z}/p\mathbb{Z}^\times} e^{2\pi i(ay+by^{-1})/p} = K[a,b;p]. \qquad \square$$

The following classical description of certain Kloosterman sums was first observed by Hans Salié in (52) of [30], using a formula of Ernst Jacobsthal from a footnote on page 239 of [19]. Jacobsthal's footnote refers the reader to his 1906 Ph.D. thesis, but fortunately the proof of his formula is not difficult to derive.

Lemma 3.3 *Fix an odd prime p and an integer a not divisible by p. Let $\chi = (\frac{\cdot}{p})$ denote the Legendre symbol modulo p.*

(a) (Jacobsthal, 1907) *Let $F : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ be any function. Then*

$$\sum_{x\in\mathbb{Z}/p\mathbb{Z}^\times} F\bigl[x + ax^{-1}\bigr] = \sum_{x=0}^{p-1} F[x] + \sum_{x=0}^{p-1} \chi\bigl[x^2 - 4a\bigr]F[x].$$

(b) (Salié, 1932) $K[1,a;p] = \sum_{x=0}^{p-1} \chi[x^2 - 4a]e^{2\pi ix/p}$.

The formulas of Lemma 3.3 are known, but we include their proofs because of the role they play in our approach.

Proof (a). Let $g : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}/p\mathbb{Z}$ be the function $g[x] = x + ax^{-1}$. For each $t \in \mathbb{Z}/p\mathbb{Z}$, set

$$N[t] = \operatorname{card}\bigl\{x \in (\mathbb{Z}/p\mathbb{Z})^\times : g[x] = t\bigr\}.$$

The desired sum can now be written as

$$\sum_{x\in\mathbb{Z}/p\mathbb{Z}^\times} F\big[x+ax^{-1}\big] = \sum_{x\in\mathbb{Z}/p\mathbb{Z}^\times} F\big[g[x]\big] = \sum_{t\in\mathbb{Z}/p\mathbb{Z}} N[t]F[t].$$

Thus, it suffices to show that $N[t] = 1+\chi[t^2-4a]$.

Note that $g[x] = g[ax^{-1}]$. Conversely, for any $x, y \in (\mathbb{Z}/p\mathbb{Z})^\times$ with $g[x] = g[y]$, we must have either $y = x$ or $y = ax^{-1}$, since $0 = g[x]-g[y] = (x-y)(1-ax^{-1}y^{-1})$. Thus, $N[t] \le 2$ for all $t \in \mathbb{Z}/p\mathbb{Z}$, and $N[t] = 1$ if and only if $t = g[x]$ for a point $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $x = ax^{-1}$. This latter condition occurs if and only if $x^2 = a$ in $\mathbb{Z}/p\mathbb{Z}$; in that case, $t = g[x] = g[ax^{-1}] = 2x$, or equivalently, $t^2 = 4a$. Thus, if we set

$$S = \big\{g[x] : x \in (\mathbb{Z}/p\mathbb{Z})^\times, x^2 \ne a\big\},$$

then

$$N[t] = \begin{cases} 2 & \text{if } t \in S, \\ 1 & \text{if } t^2 = 4a, \\ 0 & \text{otherwise.} \end{cases}$$

Note, on the other hand, that

$$1+\chi\big[t^2-4a\big] = \begin{cases} 2 & \text{if } t^2-4a \text{ is a square in } (\mathbb{Z}/p\mathbb{Z})^\times, \\ 1 & \text{if } t^2-4a = 0 \text{ in } \mathbb{Z}/p\mathbb{Z}, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, it suffices to show that

$$S = \big\{t \in \mathbb{Z}/p\mathbb{Z} : t^2-4a \text{ is a square in } (\mathbb{Z}/p\mathbb{Z})^\times\big\}. \tag{2}$$

Given $t \in S$, pick $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $t = g[x]$. Then

$$t^2-4a = \big(x+ax^{-1}\big)^2-4a = x^2-2a+a^2x^{-2} = \big(x-ax^{-1}\big)^2.$$

In addition, since $t^2 \ne 4a$ for all $t \in S$, it follows that t^2-4a is a square in $(\mathbb{Z}/p\mathbb{Z})^\times$, proving the forward inclusion.

Conversely, given $t \in (\mathbb{Z}/p\mathbb{Z})$ for which there is some $z \in (\mathbb{Z}/p\mathbb{Z})^\times$ with $z^2 = t^2-4a$, set $x = (t+z)/2 \in (\mathbb{Z}/p\mathbb{Z})^\times$. Then $x(x-z) = (t^2-z^2)/4 = a$, and therefore $g(x) = x+ax^{-1} = 2x-z = t$. It follows that $t \in S$, proving (2) and hence part (a).

Part (b) is immediate by setting $F[x] = e^{2\pi ix/p}$ and noting that $\sum_{x=0}^{p-1} e^{2\pi ix/p} = 0$. □

Theorem 3.4 *Fix an odd prime p. Let $\chi = (\frac{\cdot}{p})$ be the Legendre symbol modulo p. Then*

$$e^{-\pi imn/p}A_p(\chi)[m,n] \in \mathbb{R}, \quad \text{and} \quad |A_p(\chi)[m,n]| \le \frac{2}{\sqrt{p}},$$

for all $m, n \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$.

Proof Fix $m, n \in \mathbb{Z}/p\mathbb{Z} \smallsetminus \{0\}$. Noting that χ is multiplicative and real-valued, we have

$$A_p(\chi)[m,n] = \frac{1}{p} \sum_{k \in \mathbb{Z}/p\mathbb{Z}} \chi[k+m]\overline{\chi[k]} e^{-2\pi i k n/p} = \frac{1}{p} \sum_{k \in \mathbb{Z}/p\mathbb{Z}} \chi\big[k(k+m)\big] e^{-2\pi i k n/p}.$$

Let $a = (mn)^2/16$, $b = m/2$, and $c = -1/n$, where we are doing the arithmetic in $\mathbb{Z}/p\mathbb{Z}$. Substituting $k = cx - b$, we have

$$\begin{aligned} A_p(\chi)[m,n] &= \frac{1}{p} \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \chi\big[(cx-b)(cx+b)\big] \exp\big(-2\pi i n(cx-b)/p\big) \\ &= \frac{e^{2\pi i b n/p}}{p} \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \chi\big[c^2x^2 - b^2\big] e^{2\pi i x/p} = \frac{e^{2\pi i b n/p}}{p} K[1, a; p], \end{aligned} \quad (3)$$

where the final equality is valid because $b^2 = 4ac^2$, and hence

$$\chi\big[c^2x^2 - b^2\big] = \chi\big[c^2\big(x^2 - 4a\big)\big] = \chi\big[c^2\big]\chi\big[x^2 - 4a\big] = \chi\big[x^2 - 4a\big].$$

Since $(e^{2\pi i b n/p})^2 = e^{2\pi i m n/p} = (e^{\pi i m n/p})^2$, we have $e^{2\pi i b n/p} = \pm e^{\pi i m n/p}$, and therefore by (3) and Lemma 3.2,

$$e^{-\pi i m n/p} A_p(\chi)[m,n] = \pm \frac{1}{p} K[1, a; p] \in \mathbb{R}.$$

Finally, because $a \in \mathbb{Z}/p\mathbb{Z} \smallsetminus \{0\}$, we have $|K[1, a; p]| \le 2\sqrt{p}$, by Weil's bound for Kloosterman sums in [35]. Thus, (3) gives $|A_p(\chi)[m,n]| \le 2/\sqrt{p}$, as desired. □

Remark 3.5 In [35], Weil proves his bound for $|K[a, b; p]|$ by first using Lemma 3.3 to rewrite $K[a, b; p]$ as $\sum \chi[x^2 - 4a] e^{2\pi i x/p}$ and then bounding the new sum. Philosophically, then, it would be more direct not to convert the sum to the form $\sum \exp(2\pi i(x + ax^{-1})/p)$. Nevertheless, we have applied the transformation in Lemma 3.3 because the latter form of Kloosterman sums is better known than are the details of Weil's proof.

3.2 Main Bound

We shall need the following technical lemma. It gives an exact formula, in terms of $A_p(\chi)$, for the ambiguity function of any sequence that is a function of the Legendre symbol χ.

Lemma 3.6 *Fix an odd prime p and complex numbers $r, s, t \in \mathbb{C}$. Let $\chi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ be the Legendre symbol modulo p, and let $U : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ be the function*

$$U[k] = \begin{cases} r & \text{if } \chi(k) = 1, \\ s & \text{if } \chi(k) = -1, \\ t & \text{if } k = 0. \end{cases}$$

Set $R = (r+s)/2$, $S = (r-s)/2$, $T = t - R$, *and* $\zeta_p = e^{2\pi i/p}$. *Then*

$$A_p(U)[m,n] = |S|^2 A_p(\chi)[m,n] + \frac{1}{p}\big(E_1[m,n] + E_2[m,n]\big)$$

for all $m, n \in \mathbb{Z}/p\mathbb{Z} \smallsetminus \{0\}$, *where* $E_1[m,n] = R\bar{T} + \bar{R}T\zeta_p^{mn}$, *and*

$$E_2[m,n] = \begin{cases} (S\bar{T} + \bar{S}T\zeta_p^{mn})\chi[m] + (R\bar{S} + \bar{R}S\zeta_p^{mn})\chi[n]\sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ (S\bar{T} - \bar{S}T\zeta_p^{mn})\chi[m] - (R\bar{S} + \bar{R}S\zeta_p^{mn})i\chi[n]\sqrt{p} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof For any two functions $F, G : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$, write

$$B_p(F,G)[m,n] = \frac{1}{p}\sum_{k\in\mathbb{Z}/p\mathbb{Z}} F[k+m]\overline{G[k]}e^{-2\pi ikn/p}.$$

Define functions $\eta, \delta : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ by

$$\eta[k] = 1 \quad \text{and} \quad \delta[k] = \begin{cases} 0 & \text{if } k \neq 0, \\ 1 & \text{if } k = 0. \end{cases}$$

Thus, $U = R\eta + S\chi + T\delta$, and hence

$$\begin{aligned} B_p(U,U) = {} & |R|^2 B_p(\eta,\eta) + |S|^2 B_p(\chi,\chi) + |T|^2 B_p(\delta,\delta) \\ & + R\bar{T}B_p(\eta,\delta) + \bar{R}TB_p(\delta,\eta) + S\bar{T}B_p(\chi,\delta) + \bar{S}TB_p(\delta,\chi) \\ & + R\bar{S}B_p(\eta,\chi) + \bar{R}SB_p(\chi,\eta). \end{aligned}$$

To compute $B_p(U,U)$, we shall compute each of these nine terms separately. Since $m \neq 0$, we have $B_p(\delta,\delta) = 0$. In addition, $B_p(\eta,\eta) = 0$, since $\sum_{k\in\mathbb{Z}/p\mathbb{Z}} e^{-2\pi ikn/p} = 0$ and $n \neq 0$. We also have $B_p(\chi,\chi) = A_p(\chi)$ by definition. Meanwhile, it is immediate that

$$\begin{aligned} & pB_p(\eta,\delta)[m,n] = 1, \qquad pB_p(\delta,\eta)[m,n] = \zeta_p^{mn}, \\ & pB_p(\chi,\delta)[m,n] = \chi[m], \quad \text{and} \quad pB_p(\delta,\chi)[m,n] = \zeta_p^{mn}\chi[-m]. \end{aligned}$$

Next, $pB_p(\eta,\chi)[m,n] = \tau[-n;p]$, where $\tau[a;p]$ is the Gauss sum

$$\tau[a;p] = \sum_{k\in\mathbb{Z}/p\mathbb{Z}} \chi[k]e^{2\pi iak/p}.$$

However, Gauss proved that $\tau[a;p] = \varepsilon\chi[a]\sqrt{p}$, where $\varepsilon = 1$ if $p \equiv 1 \pmod 4$, and $\varepsilon = i$ if $p \equiv 3 \pmod 4$; see, for example, Proposition 6.3.1 and Theorem 6.4.1 of [18]. Hence, $pB_p(\eta,\chi)[m,n] = \varepsilon\chi[-n]\sqrt{p}$. Similarly,

$$pB_p(\chi,\eta)[m,n] = \sum_{k\in\mathbb{Z}/p\mathbb{Z}} \chi[k+m]e^{-2\pi ikn/p} = \sum_{j\in\mathbb{Z}/p\mathbb{Z}} \chi[j]e^{-2\pi i(j-m)n/p}$$
$$= \zeta_p^{mn}\tau[-n;p] = \varepsilon\zeta_p^{mn}\chi[-n]\sqrt{p}.$$

Combining the nine computations above, and noting that

$$\chi[-k] = \chi[-1]\chi[k]\begin{cases}\chi[k] & \text{if } p\equiv 1 \pmod 4,\\ -\chi[k] & \text{if } p\equiv 3 \pmod 4,\end{cases}$$

we have $B_p(U,U) = |S|^2A_p(\chi) + (E_1+E_2)/p$, where E_1 and E_2 are the quantities in the statement of Lemma 3.6. □

The following elementary bound will be needed to prove the $p\equiv 3 \pmod 4$ case of Theorem 3.8.

Lemma 3.7 *Let $X, Y\in\mathbb{R}$, and let $z\in\mathbb{C}$ with $|z|=1$. Then*

$$|zX + (1-z^2)Y| \le \sqrt{X^2+4Y^2}.$$

Proof Noting that $z\overline{z}=1$, we have

$$\begin{aligned}|zX+(1-z^2)Y| &= \sqrt{\big(zX+(1-z^2)Y\big)\big(\overline{z}X+(1-\overline{z}^2)Y\big)}\\ &= \sqrt{X^2+\big(z(1-\overline{z}^2)+\overline{z}(1-z^2)\big)XY+(1-z^2)(1-\overline{z}^2)Y^2}\\ &= \sqrt{X^2+|1-z^2|^2Y^2} \le \sqrt{X^2+4Y^2},\end{aligned}$$

since $z(1-\overline{z}^2)+\overline{z}(1-z^2) = z-\overline{z}+\overline{z}-z = 0$ and $|1-z^2|\le 2$. □

We are now ready to state and prove our main result.

Theorem 3.8 *Let p be an odd prime, and let u_p be the Björck function for p. Then the ambiguity function, $A_p(u_p)$, defined on $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ as*

$$A_p(u_p)[m,n] = \frac{1}{p}\sum_{k\in\mathbb{Z}/p\mathbb{Z}} u_p[k+m]\overline{u_p[k]}e^{-2\pi ikn/p},$$

satisfies the estimate

$$|A(u_p)[m,n]| < \frac{2}{\sqrt{p}} + \begin{cases}\frac{4}{p} & \text{if } p\equiv 1 \pmod 4,\\ \frac{4}{p^{3/2}} & \text{if } p\equiv 3 \pmod 4,\end{cases}$$

for all $(m,n)\in(\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z})\setminus\{(0,0)\}$.

Proof Fix $(m,n) \in (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \setminus \{(0,0)\}$. If $m = 0$, then $n \neq 0$, and we have

$$A_p(u_p)[0,n] = \frac{1}{p} \sum_{k \in \mathbb{Z}/p\mathbb{Z}} u_p[k]\overline{u_p[k]} e^{-2\pi i k n/p} = \frac{1}{p} \sum_{k \in \mathbb{Z}/p\mathbb{Z}} e^{-2\pi i k n/p} = 0,$$

since $|u_p[k]| = 1$ for all $k \in \mathbb{Z}/p\mathbb{Z}$. On the other hand, if $n = 0$, then $m \neq 0$, and we have

$$A_p(u_p)[m,0] = \frac{1}{p} \sum_{k \in \mathbb{Z}/p\mathbb{Z}} u_p[k+m]\overline{u_p[k]} = 0,$$

because u_p has zero autocorrelation. Thus, by the fact that u_p is a *CAZAC*, we may assume for the remainder of the proof that $m, n \neq 0$.

If $p \equiv 1 \pmod 4$, then in the notation of Lemma 3.6, we have $r = (1+\sqrt{p})^{-1}(1 + i\sqrt{2\sqrt{p}+p})$, $s = (1+\sqrt{p})^{-1}(1 - i\sqrt{2\sqrt{p}+p})$, and $t = 1$. Thus,

$$R = \frac{r+s}{2} = \frac{1}{1+\sqrt{p}},$$

$$S = \frac{r-s}{2} = \frac{i\sqrt{2\sqrt{p}+p}}{1+\sqrt{p}} \quad \text{and} \quad T = t - R = \frac{\sqrt{p}}{1+\sqrt{p}}.$$

The quantities E_1 and E_2 in Lemma 3.6 are therefore

$$E_1[m,n] = \frac{\sqrt{p}(1+\zeta_p^{mn})}{(1+\sqrt{p})^2}$$

and

$$\begin{aligned} E_2[m,n] &= \frac{1}{(1+\sqrt{p})^2}\Big[\big(1-\zeta_p^{mn}\big)\sqrt{p}\sqrt{2\sqrt{p}+p}\cdot i\chi[m] \\ &\quad + \big(\zeta_p^{mn}-1\big)\sqrt{p}\sqrt{2\sqrt{p}+p}\cdot i\chi[n]\Big] \\ &= \frac{\sqrt{p}}{(1+\sqrt{p})^2}\Big[i\big(1-\zeta_p^{mn}\big)\big(\chi[m]-\chi[n]\big)\sqrt{2\sqrt{p}+p}\Big]. \end{aligned}$$

Noting that $|1+\zeta_p^{mn}|$, $|1-\zeta_p^{mn}|$, and $|\chi[m]-\chi[n]|$ are each less than or equal to 2 and that $\sqrt{2\sqrt{p}+p} < \sqrt{1+2\sqrt{p}+p} = 1+\sqrt{p}$, we obtain

$$|E_1[m,n] + E_2[m,n]| < \frac{2\sqrt{p}}{(1+\sqrt{p})^2} + \frac{4\sqrt{p}}{1+\sqrt{p}} < \frac{2\sqrt{p}}{(1+\sqrt{p})^2} + 4.$$

Hence, by Lemma 3.6 and Theorem 3.4, we have

$$\begin{aligned} &|A_p(u_p)[m,n]| \\ &\leq \frac{2}{\sqrt{p}}|S|^2 + \frac{2}{\sqrt{p}(1+\sqrt{p})^2} + \frac{4}{p} = \frac{2}{\sqrt{p}(1+\sqrt{p})^2}(2\sqrt{p}+p+1) + \frac{4}{p} \end{aligned}$$

$$= \frac{2}{\sqrt{p}(1+\sqrt{p})^2}(1+\sqrt{p})^2 + \frac{4}{p} = \frac{2}{\sqrt{p}} + \frac{4}{p}.$$

Similarly, if $p \equiv 3 \pmod 4$, then $r = 1$, $s = (1+p)^{-1}(1-p+2i\sqrt{p})$, and $t = 1$, and therefore

$$R = \frac{r+s}{2} = \frac{1}{1-i\sqrt{p}}, \qquad S = \frac{r-s}{2} = \frac{-i\sqrt{p}}{1-i\sqrt{p}}, \quad \text{and} \quad T = t - R = \frac{-i\sqrt{p}}{1-i\sqrt{p}}.$$

Thus, the quantities E_1 and E_2 in Lemma 3.6 are

$$E_1[m,n] = \frac{i\sqrt{p}(1-\zeta_p^{mn})}{p+1}$$

and

$$\begin{aligned} E_2[m,n] &= \frac{1}{p+1}\big[(p - p\zeta_p^{mn})\chi[m] - (i\sqrt{p} - \zeta_p^{mn} i\sqrt{p})i\chi[n]\sqrt{p}\big] \\ &= \frac{p(1-\zeta_p^{mn})}{p+1}\big[\chi[m] + \chi[n]\big]. \end{aligned}$$

Since $|S|^2 = p/(p+1)$, we have

$$||S|^2 A_p(\chi)[m,n] + \frac{1}{p}E_2[m,n]| = \frac{1}{p+1}|pA_p(\chi)[m,n] + (1-\zeta_p^{mn})(\chi[m]+\chi[n])|.$$

Setting $z = e^{\pi imn/p}$, $X = e^{-\pi imn/p} pA_p(\chi)[m,n]$, and $Y = \chi[m] + \chi[n]$, so that $X \in \mathbb{R}$ with $|X| \le 2\sqrt{p}$ by Theorem 3.4, $Y \in \mathbb{R}$ with $|Y| \le 2$, and $|z| = 1$, Lemma 3.7 tells us that

$$\left||S|^2 A_p(\chi)[m,n] + \frac{1}{p}E_2[m,n]\right| \le \frac{\sqrt{X^2+4Y^2}}{p+1} \le \frac{\sqrt{4p+16}}{p+1} = \frac{2\sqrt{p+4}}{p+1}.$$

Hence, by Lemma 3.6 and the fact that $|1-\zeta_p^{mn}| \le 2$, we obtain

$$\begin{aligned} |A_p(u_p)[m,n]| &\le \left||S|^2 A_p(\chi)[m,n] + \frac{1}{p}E_2[m,n]\right| + \left|\frac{1}{p}E_1[m,n]\right| \\ &\le \frac{2\sqrt{p+4}}{p+1} + \frac{2}{\sqrt{p}(p+1)} = \frac{2}{\sqrt{p}(p+1)}\big(\sqrt{p^2+4p}+1\big) \\ &\le \frac{2(p+3)}{\sqrt{p}(p+1)} = \frac{2}{\sqrt{p}} + \frac{4}{\sqrt{p}(p+1)} \le \frac{2}{\sqrt{p}} + \frac{4}{p^{3/2}}. \end{aligned}$$

□

Remark 3.9 The bounds in Theorem 3.8 may be improved very slightly but at the great expense of simplicity. For example, if $p \equiv 1 \pmod 4$, then the bounds $|1-\zeta_p^{mn}| \le 2$ and $|1+\zeta_p^{mn}| \le 2$ could be improved, as obviously these quantities cannot both be simultaneously close to 2. However, the resulting bound is far more

complicated to write, and the savings is only about $2p^{-3/2}$, as illustrated by considering ζ_p^{mn} very close to -1. Similarly, removing the simplification $4\sqrt{p}/(1+\sqrt{p}) < 4$ would also only save us about $4p^{-3/2}$. For further details, including the explicit formula of Lemma 3.6 in the case that $U = u_p$, we refer the reader to [7].

4 Figures and Table

Natural algebraic and analytic calculations convinced us that the proof of Theorem 3.8 depended on substantial number theoretic results. In parallel, Fig. 1 supported the truth of Theorem 3.8 before we proved it. The x-axis lists the primes between 1 and 1000. The y axis lists the values,

$$\max_{(m,n)\neq(0,0)} |A_p(u_p)[m,n]|. \tag{4}$$

Figure 1 also displays the curves $y = 2/\sqrt{p}$ and $y = 2/\sqrt{p} + 4/p$ for comparison. Figure 2, for the case $p = 13$, illustrates the symmetries inherent in the function $A_p(u_p)$ on $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. These are fully explained for all p in [7]; and they led to the realization of the complexity involved in proving Theorem 3.8, as well as to a host of geometrical and combinatorial phenomena and problems. Figure 3 illustrates Theorem 3.8 for the case $p = 503$.

Table 1 indicates some of the finer behavior of the quantity (4), over three different ranges of primes. This data suggested to us that $2/\sqrt{p}$ was very nearly the upper bound for $|A_p(u_p)[m,n]|$, $(m,n) \neq (0,0)$, and it helped lead us to the proof that $2/\sqrt{p} + 4/p$ is an upper bound. In addition, although a number of primes $p \equiv 1$

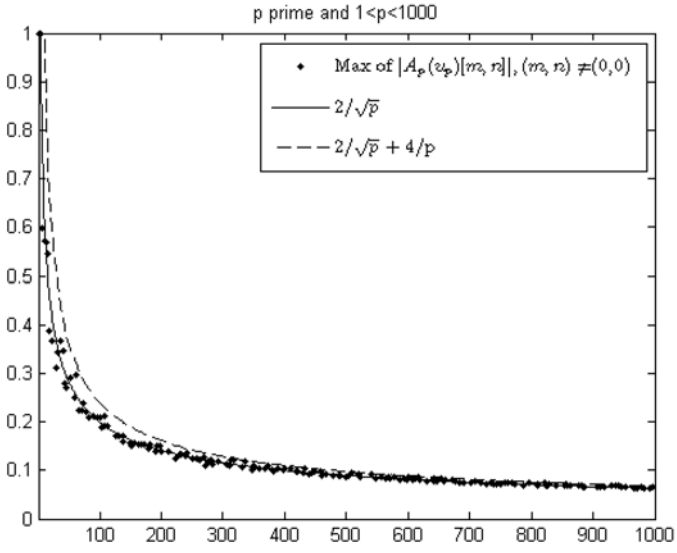

Fig. 1 p and $\max\{|A_p(u_p)[m,n]| : (m,n) \neq (0,0)\}$

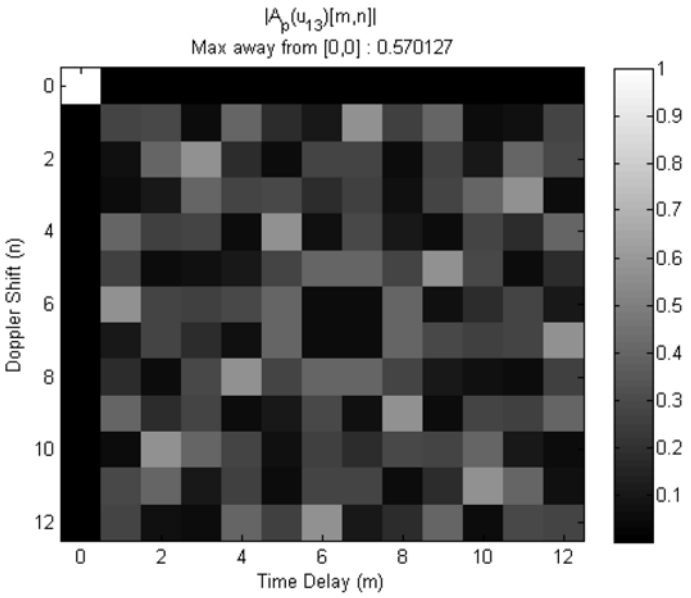

Fig. 2 $A_p(u_p)$ for $p = 13$

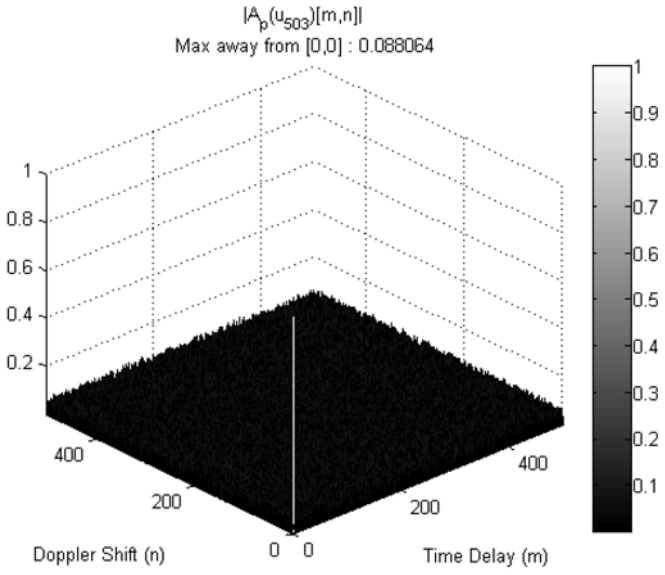

Fig. 3 $A_p(u_p)$ for $p = 503$

(mod 4) require a bound larger than $2/\sqrt{p}$, we noted that only very few primes $p \equiv 3$ (mod 4) allowed $|A_p(u_p)[m,n]| > 2/\sqrt{p}$ for $(m,n) \neq (0,0)$. For example, $p = 139$ is the only such prime in Table 1. Our broader calculations for other primes showed

Table 1 Comparison of $\max |A_p(u_p)|$ outside $(0,0)$ with $2/\sqrt{p}$

p	$\max \lvert A_p(u_p)\rvert$	$2/\sqrt{p}$	p	$\max \lvert A_p(u_p)\rvert$	$2/\sqrt{p}$
3	1	1.15470	1009	0.065505	0.062963
5	1	0.894427	1013	0.064300	0.062838
7	0.599074	0.755929	1019	0.060996	0.062653
11	0.572765	0.603023	1021	0.063567	0.062592
13	0.570127	0.554700	1031	0.061432	0.062287
17	0.544798	0.485071	1033	0.062460	0.062227
19	0.388357	0.458831	1039	0.061420	0.062047
23	0.365960	0.417029	1049	0.063469	0.061751
29	0.312280	0.371391	1051	0.060041	0.061692
101	0.208395	0.199007	1061	0.063533	0.061401
103	0.187876	0.197066	1063	0.060180	0.061343
107	0.192309	0.193347	1069	0.062845	0.061170
109	0.212120	0.191565	1087	0.059183	0.060662
113	0.191960	0.188144	1091	0.059923	0.060550
127	0.171881	0.177471	1093	0.060828	0.060495
131	0.170530	0.174741	1097	0.063115	0.060385
137	0.159752	0.170872	1103	0.059840	0.060220
139	0.171326	0.169638	1109	0.061014	0.060057
149	0.157303	0.163846	1117	0.062083	0.059842
151	0.149263	0.162758	1123	0.058489	0.059682
157	0.157840	0.159617	1129	0.062178	0.059523
163	0.154913	0.156652	1151	0.058290	0.058951
167	0.152243	0.154765	1153	0.061266	0.058900
173	0.152966	0.152057	1163	0.058550	0.058646
179	0.143966	0.149487	1171	0.056711	0.058446
181	0.154193	0.148659	1181	0.059624	0.058198
191	0.139244	0.144715	1187	0.057459	0.058050
193	0.151468	0.143963	1193	0.059935	0.057904
197	0.151479	0.142494	1201	0.057850	0.057711
199	0.138516	0.141776	1213	0.058716	0.057425

that the only such primes between 1000 and 5000 are 1259, 2111, and 3511; the only ones between 10000 and 24360 are 13879, 16091 and 23719; and there are none between 100000 and 105000. Moreover, for all seven of those primes, the maximum value of $|A_p(u_p)[m,n]| - 2/\sqrt{p}$ for $(m,n) \neq (0,0)$ is still far smaller than $4/p$, a fact which ultimately led us to the sharper bound for $p \equiv 3 \pmod 4$ in Theorem 3.8.

Acknowledgements The authors gratefully acknowledge the support of various grants. For the first-named author, the grants are ONR Grant N00014-09-1-0144 and MURI-ARO Grant W911NF-09-1-0383. For the second named author, the grant is NSF Grant DMS-0901494. The third-named author was supported by the Norbert Wiener Center as recipient of the Daniel Sweet Undergraduate Research Fellowship. Further, at the time of the first-named author's presentation of their results at SampTA2011 in Singapore, Professor Bruno Torresani kindly pointed out two references on which we comment in Sect. 1.2. Finally,

and although not represented explicitly in this paper, we have benefitted from expert advice on hardware implementation by Drs. Michael Dellomo, Joseph Lawrence, and George Linde.

References

1. Alltop, W.O.: Complex sequences with low periodic correlations. IEEE Trans. Inf. Theory **26**, 350–354 (1980)
2. Auslander, L., Barbano, P.E.: Communication codes and Bernoulli transformations. Appl. Comput. Harmon. Anal. **5**(2), 109–128 (1998)
3. Bell, M.R., Monrocq, S.: Diversity waveform signal processing for delay-Doppler measurement and imaging. Digit. Signal Process. **12**(2/3), 329–346 (2002)
4. Benedetto, J.J., Datta, S.: Construction of infinite unimodular sequences with zero autocorrelation. Adv. Comput. Math. **32**, 191–207 (2010)
5. Benedetto, J.J., Donatelli, J.J.: Ambiguity function and frame theoretic properties of periodic zero autocorrelation waveforms. IEEE J. Spec. Top. Signal Process. **1**, 6–20 (2007)
6. Benedetto, J.J., Konstantinidis, I., Rangaswamy, M.: Phase coded waveforms and their design—the role of the ambiguity function. IEEE Signal Process. Mag. **26**, 22–31 (2009)
7. Benedetto, J.J., Benedetto, R.L., Woodworth, J.T.: Björck CAZACs: theory, geometry, and waveform ambiguity behavior. Preprint (2011)
8. Björck, G.: Functions of modulus one on $\mathbf{Z}_p$ whose Fourier transforms have constant modulus. In: A. Haar Memorial Conference, Vols. I, II, Budapest, 1985. Colloq. Math. Soc. János Bolyai, vol. 49, pp. 193–197. North-Holland, Amsterdam (1987)
9. Björck, G.: Functions of modulus one on $\mathbb{Z}_n$ whose Fourier transforms have constant modulus, and cyclic n-roots. In: Proc. of 1989 NATO Adv. Study Inst. on Recent Advances in Fourier Analysis and its Applications, pp. 131–140 (1990)
10. Chu, D.C.: Polyphase codes with good periodic correlation properties. IEEE Trans. Inf. Theory **18**, 531–532 (1972)
11. Frank, R.L., Zadoff, S.A.: Phase shift pulse codes with good periodic correlation properties. IRE Trans. Inf. Theory **8**(6), 381–382 (1962)
12. Golomb, S.W., Gong, G.: Signal Design for Good Correlation. Cambridge University Press, Cambridge (2005)
13. Gurevich, S., Haddani, R., Sochen, N.: The finite harmonic oscillator and its applications to sequences, communication, and radar. IEEE Trans. Inf. Theory **54**, 4239–4253 (2008)
14. Haagerup, U.: Orthogonal maximal abelian $*$-subalgebras of the $n \times n$ matrices and cyclic n-roots. In: Operator Algebras and Quantum Field Theory, Rome, 1996, pp. 296–322. Int. Press, Cambridge (1997)
15. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers, 4th edn. Clarendon Press, Oxford (1965)
16. Helleseth, T., Kumar, P.V.: Sequences with low correlation. In: Pless, V.S., Huffman, W.C. (eds.) Handbook of Coding Theory, Vols. I, II, pp. 1765–1853. North-Holland, Amsterdam (1998)
17. Herman, M.A., Strohmer, T.: High-resolution radar via compressed sensing. IEEE Trans. Signal Process. **57**, 2275–2284 (2009)
18. Ireland, K., Rosen, M.: A Classical Introduction to Modern Number Theory, 2nd edn. Graduate Texts in Mathematics, vol. 84. Springer, New York (1990)
19. Jacobsthal, E.: Über die darstellung der primzahlen der form $4n + 1$ als summe zweier quadrate. J. Reine Angew. Math. **132**, 238–245 (1907)
20. Klauder, J.R.: The design of radar signals having both high range resolution and high velocity resolution. Bell Syst. Tech. J. **39**, 809–820 (1960)
21. Klauder, J.R., Price, A.C., Darlington, S., Albersheim, W.J.: The theory and design of chirp radars. Bell Syst. Tech. J. **39**, 745–808 (1960)
22. Levanon, N., Mozeson, E.: Radar Signals. Wiley Interscience, IEEE Press, New York (2004)
23. Mauduit, C., Sárközy, A.: On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol. Acta Arith. **82**(4), 365–377 (1997)
24. 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), September, pp. 955–959 (1996)

25. Popovic, B.M.: Generalized chirp-like polyphase sequences with optimum correlation properties. IEEE Trans. Inf. Theory **38**(4), 1406–1409 (1992)
26. Popovic, B.M.: Fourier duals of Björck sequences. In: SETA, pp. 253–258 (2010)
27. Richards, M.A., Scheer, J.A., Holm, W.A. (eds.): Principles of Modern Radar. SciTech Publishing, Raleigh (2010)
28. Saffari, B.: Some polynomial extremal problems which emerged in the twentieth century. In: Twentieth Century Harmonic Analysis—A Celebration, Il Ciocco, 2000. NATO Sci. Ser. II Math. Phys. Chem., vol. 33, pp. 201–233. Kluwer Academic, Dordrecht (2001)
29. Saffari, B.: Oral and email communications (2004–2010)
30. Salié, H.: Über die Kloostermanschen Summen $S(u, v; q)$. Math. Z. **34**(1), 91–109 (1932)
31. Skolnik, M.I.: Introduction to Radar Systems. McGraw-Hill, New York (1980)
32. Strohmer, T., Heath, R.W. Jr.: Grassmannian frames with applications to coding and communications. Appl. Comput. Harmon. Anal. **14**, 257–275 (2003)
33. Turyn, R.J.: Sequences with small correlation. In: Error Correcting Codes, Proc. Sympos. Math. Res. Center, Madison, Wis., 1968, pp. 195–228. Wiley, New York (1968)
34. Vakman, D.E.: Sophisticated Signals and the Uncertainty Principle in Radar. Springer, New York (1969)
35. Weil, A.: On some exponential sums. Proc. Natl. Acad. Sci. USA **34**, 204–207 (1948)
36. Weil, A.: Sur les courbes algébriques et les variétés qui s'en déduisent. In: Actualités Sci. et Ind. no. 1041. Hermann, Paris (1948)
37. Woodward, P.M.: Theory of radar information. IEEE Trans. Inf. Theory **1**(1), 108–113 (1953)