Ambiguity and sidelobe behavior of CAZAC coded waveforms

Andrew Kebo*, Ioannis Konstantinidis*, John J. Benedetto*, Michael R. Dellomo*
and Jeffrey M. Sieracki†
*Norbert Wiener Center
Department of Mathematics
University of Maryland
College Park, MD 20742
†SR2Group
P.O. Box 1011
College Park, MD 20741

***Abstract*— CAZAC (Constant Amplitude Zero Auto-Correlation) sequences are important in waveform design because of their optimal transmission efficiency and tight time localization properties. Certain classes of CAZAC sequences have been used in Radar processing for many years while recently discovered sequences invite further study. This paper compares several classes of CAZAC sequences with respect to both the periodic and aperiodic ambiguity function. Some computational results for different CAZAC classes are presented. In particular, we note the fact that so-called Björck CAZACs have sidelobes at different locations when different shifts are considered. We take advantage of this fact by using an averaging technique to lower sidelobe levels.**

Background: Let $u : \mathbb{Z}_K \to \mathbb{C}$ be a complex-valued periodic sequence of period K. Then u is a *constant amplitude zero-autocorrelation code* (CAZAC) *of length* K if

- for all $k \in \mathbb{Z}_K$, $|u[k]| = 1$, (CA - constant amplitude), and
- for all $m = 1, \dots, K-1$, (ZAC - periodic zero autocorrelation)

$$C_u[m] = \frac{1}{K}\sum_{k=0}^{K-1} u[m+k]\overline{u}[k] = 0,$$

where it is understood that the summation $m+k$ is modulo K. The aperiodic autocorrelation of u is given by $AC_u[m] = \frac{1}{K}\sum_{k=0}^{K-1-m} u[k+m]\overline{u[k]}$.

There are two different discrete ambiguity functions associated with a CAZAC sequence, the periodic, relevant to CW Radar analysis:

$$P_u[m,n] = \frac{1}{K}\sum_{k=0}^{K-1} u[k+m]\overline{u[k]}e^{\frac{2\pi i n k}{K}},$$

and the aperiodic, relevant to pulsed Radar analysis:

$$A_u[m,n] = \frac{1}{K}\sum_{k=0}^{K-1-m} u[k+m]\overline{u[k]}e^{\frac{2\pi i n k}{K}}.$$

Note that $AC_u[m] = A_u[m,0]$.

CAZAC sequences are typically used to code a digital QAM Radar signal, with sequence terms describing the phase information of the complex envelope of the signal. If the characteristic function $\mathbf{1}_{[-T,T]}$ of an interval centered at the origin defines the extent of each discrete range bin, then the aperiodic waveform $w : \mathbb{R} \to \mathbb{C}$ based on the CAZAC sequence u, is of the form,

$$w(t) = \sum_{k\in\mathcal{S}} u[k]\mathbf{1}_{[-T,T]}(t-2kT).$$

The summation is over the set $\mathcal{S} = \mathbb{Z}$ in CW Radar, and over the set $\mathcal{S} = 0, 1, \dots, K-1$ in pulsed Radar. The connection between AC_u and the (continuous) autocorrelation of the waveform w, i.e., that the latter is a complex linear interpolation of the former, is explained in [1].

Motivation: CAZAC sequences are important in waveform design because of their defining properties: CA ensures optimal transmission efficiency while ZAC provides tight time localization. In the aperiodic case, of course, ZAC is unattainable, but sidelobe levels can still be controlled. CAZACs have also been referred to in the Radar literature as generalized bent functions [2], perfect root-of-unity sequences [3], constant amplitude optimal sequences [4], or generalized chirp-like polyphase sequences [5]. Numerous well-known coding sequences used in Radar can be classified as CAZACs, such as the Barker sequences of length $K = 11, 13$, or the discretized quadratic chirps, an observation which goes back to the work of N. Wiener. We can also list Frank–Zadoff codes [6] and generalized Frank sequences [7], Chu codes [8], and Milewski sequences [9]. In addition, Björck [10] constructed families of small alphabet CAZACs for any prime length, which assume no more than three distinct values. To date, there is no complete classification of the set of CAZAC sequences, despite an expansive literature spanning not only Radar, but also coding, cryptography, and communications.

Examples: Given K odd, a *Wiener* CAZAC of length K is defined as $u[k] = \zeta^{k^2}$, $k \in \mathbb{Z}_K$, where $\zeta = e^{\frac{2\pi i}{K}}$. For K even, the corresponding Wiener CAZAC is defined by using $\zeta = e^{2\pi i/2K}$.

A different class of CAZAC is defined based on quadratic residue sequences. These are also called small alphabet CAZACs, because they assume at most three distinct values. Quadratic residue sequences of prime length p are defined in terms of the Legendre symbol:

$$\left(\frac{k}{p}\right) = \begin{cases} 1 & \text{if } k = 0 \ (mod\ p) \\ 1 & \text{if k is a square } (mod\ p) \\ -1 & \text{if k is not a square } (mod\ p) \end{cases}$$

Two-valued CAZACs have been classified by Saffari [11] in terms of Hadamard-Paley and Hadamard-Menon difference sets. The result of Saffari states that two-valued CAZACs exist for lengths $K \geq 3$ if and only if $K = 3 \mod 4$ and there exists a Hadamard-Paley difference set of length K or $K = 0 \mod 4$ and there exists a Hadamard-Menon difference set of length K. In either case, explicit formulas are provided for the construction of the CAZAC sequence. A similar classification exists for two-level autocorrelation Legendre sequences [12], with several results relating to the existence of Hadamard-Paley difference sets. Existence of Hadamard-Menon sets is rather more difficult to prove, as it relates to the Hadamard circulant conjecture.

It follows that two-valued CAZACs cannot exist for lengths $K = 1 \mod 4$. However, Björck [10] describes the following class of CAZACs, which are *almost* two-valued. Let $p = 1 \mod 4$ be prime. Then the sequence u defined by

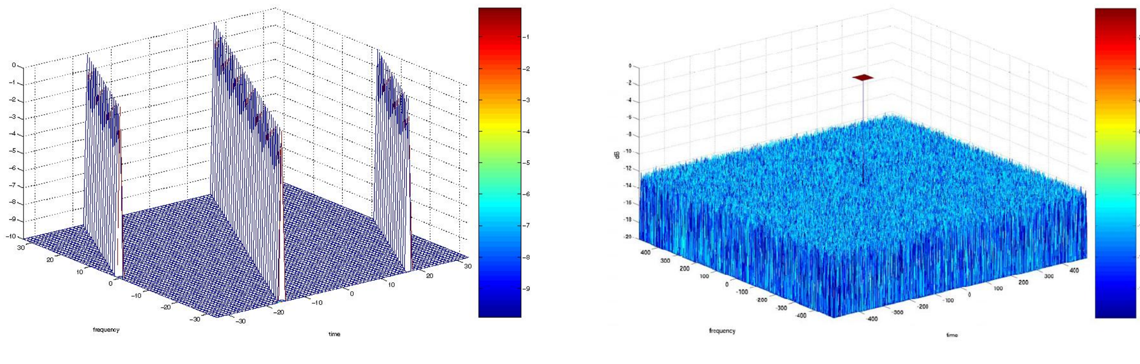
$$u[k] = e^{2\pi i \theta \left(\frac{k}{p}\right)}, \text{ where } \theta = \arccos\left(\frac{1}{1+\sqrt{p}}\right),$$

and $\left(\frac{k}{p}\right)$ is the Legendre symbol, is a Björck CAZAC sequence. Note that u takes 3 values.

Results: The set of CAZAC sequences is much richer than the set of quadratic chirps, with several nonequivalent families having been identified. In recent work, Benedetto and Donatelli [13] explore the intricacies of the effect different construction methods have on CAZAC sequence behavior in terms of the discrete periodic ambiguity function; and prove various ambiguity function properties by means of elementary number theory. Some computational results for different CAZAC classes are presented. In particular, we note the fact that Björck CAZACs have sidelobes at different locations when different shifts are considered. We take advantage of this fact by using an averaging technique to lower sidelobe levels.

Periodic Ambiguity: The support of the discrete periodic ambiguity function in the K even case is concentrated on a ridge along the main diagonal, providing a well-defined linear chirp comparable to a discrete LFM pulse. In contrast to that, the support of the discrete periodic ambiguity function in the K odd case is proven to be rapidly oscillating between two parallel ridges of slope equal to 2 (Figure 1(a)). Even though the crosscorrelation of a Wiener CAZAC sequence of odd length with any of its frequency shifts remains a Dirac delta function, this oscillating behavior results in poor frequency shift resilience.

The Milewski construction provides an example of a different vulnerability to frequency shift. Let c be a *seed* CAZAC of length M and fix $N \in \mathbb{N}$. Let ζ be a primitive MNth root of unity. For any fixed positive integer ℓ, there exist integers a and b, $b < N$, such that $\ell = aN + b$. Define the sequence $u[\ell] = u[aN+b] = c[a]\zeta^{ab}$ for $\ell = 0, \ldots, MN^2-1$.



a b

Fig. 1. Plot of the periodic ambiguity function of two different CAZAC sequences; a) Wiener of odd length and b) Björck (the peak has been marked with a red square for legibility).

Then the sequence u is a *Milewski* CAZAC of length MN^2. However, its discrete periodic ambiguity function is now supported on N different bands, parallel to the main diagonal. In this case, the introduction of frequency shifts in the return results in crosscorelations that are no longer free of sidelobes.

The Björck construction seems particularly well-suited to simultaneous range and range-rate information. Its discrete periodic ambiguity function now has full support, but is also a perfect "thumbtack" figure, localized at a single point at the origin. The "grass skirt" surrounding it fully covers the discrete time-frequency plane, but is uniformly flat (Figure 1(b)).

Aperiodic autocorrelation: The set of CAZAC sequences remains invariant under several operations.

• Shifts: $\forall n = 0, \ldots, N-1$ and $m \in \mathbb{Z}$,

$$u[n] = (\tau_m c)[n] = c[m+n].$$

• Cyclic permutations: for g with $gcd(g, N) = 1$,

$$u[n] = (\sigma_g c)[n] = c[gn].$$

• Multiplication by powers of Nth roots of unity: for ζ with $\zeta^N = 1$,

$$u[n] = c[n]\zeta^n.$$

In all these cases, u is a CAZAC sequence if c is also CAZAC. However, the behavior of sidelobes can differ drastically among the CAZAC families.

Figure 2 illustrates the different behavior of sidelobes with respect to shifts τ_m. In particular, Wiener CAZACs are not affected at all, whereas Björck sequences exhibit the most variability. This is analogous to results obtained for Legendre sequences [14], [15]. Milewski sequences fall in between, reflecting their mixed method of construction. We chose to plot results in terms of Peak Sidelobe Levels, but similar results arise when one considers other measures, such as the Merit Factor.

The variability in sidelobe behavior for Björck CAZACs is not limited to their energy levels. As Figure 3 shows, shifting also affects sidelobe location. By averaging the autocorrelation $AC_{\tau_k u}$ of several different shifts m of the same basis sequence u, we can obtain an overall lowering of the energy levels off of the main lobe. In this example, we present the noncoherent average over two selected shifts, i.e.

$$|AC_{\tau_{40}u}| + |AC_{\tau_{41}u}|$$

We notice that in the area near the main lobe we can improve over the shift that achieves the lowest PSL globally (shift by 28). The two different shifts plotted (shifts by 40 and 41) have complementary sidelobes near the origin, and further improvement is achieved by averaging them.

The same averaging technique can be used with the discrete ambiguity functions of shifted sequences $A_{\tau_k u}[m, n]$. Figures 4(a–c) plot the discrete aperiodic ambiguity functions of shifts of the Björck CAZAC of length 29 (by zero, 7, and 12, respectively), with a threshold of -10dB. The area plotted

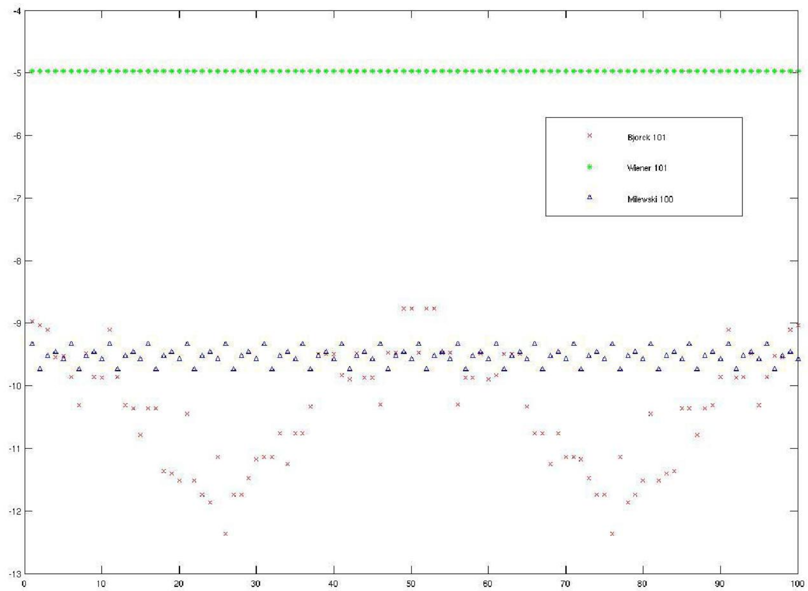


Fig. 2. Effect of cyclic shifts on the aperiodic autocorrelation of different CAZAC sequences; Peak Sidelobe Level (dB) vs. shift length. Red x: Björck of length 101, Blue triangles: Milewski of length 100, Green squares: Wiener of length 101.

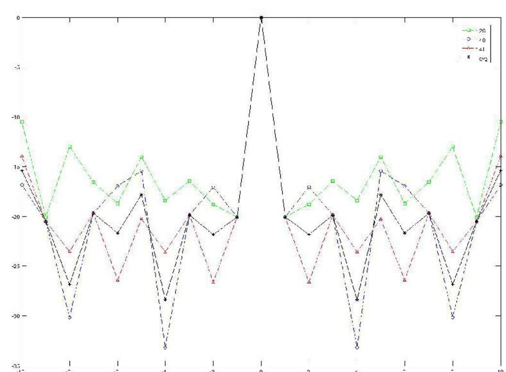


Fig. 3. Effect of cyclic shifts on the aperiodic autocorrelation function of Björck CAZAC sequences; Plot of absolute value (dB) in the area of the main lobe for two different shifts (by 40 and 41), and their average. Also plotted for reference is the shift that achieves the lowest PSL globally.

is centered at the origin. We observe that the peak locations vary, and by averaging all three we obtain Figure 4(d).

ACKNOWLEDGMENT

This work was supported in part by DARPA funding under NRL grant N00173–06–1–G006 and the Air Force Office of Scientific Research under MURI grant AFOSR–FA9550–05–1–0443.

REFERENCES

[1] N. Levanon and E. Mozeson, *Radar Signals*. Wiley, 2004.

[2] H. Chung and P. V. Kumar, "A new general construction for generalized bent functions," *IEEE Transactions on Information Theory*, vol. 35, no. 1, p. 206, 1989.

[3] W. Mow, "A new unified construction of perfect root-of-unity sequences," Germany, sep 1996, pp. 955–959.

[4] J. C. Ng, K. B. Letaief, and R. D. Murch, "Complex optimal sequences with constant magnitude for fast channel estimation initialization," *IEEE Transactions on Communications*, vol. 46, no. 3, pp. 305–308, 1998.

[5] B. Popović, "Generalized chirp-like polyphase sequences with optimum correlation properties," *IEEE Transactions on Information Theory*, vol. 38, no. 4, pp. 1406–1409, 1992.

[6] R. L. Frank and S. A. Zadoff, "Phase shift pulse codes with good periodic correlation properties," *IRE Trans. Inf. Theory,*, vol. 8, no. 6, pp. 381–382, 1962.

[7] P. Kumar, R. Scholtz, and L. Welch, "Generalized bent functions and their properties," *J. Combin. Theory*, vol. A, no. 40, pp. 90–107, 1985.

[8] D. C. Chu, "Polyphase codes with good periodic correlation properties," *IEEE Transactions on Information Theory*, vol. 18, pp. 531–532, 1972.

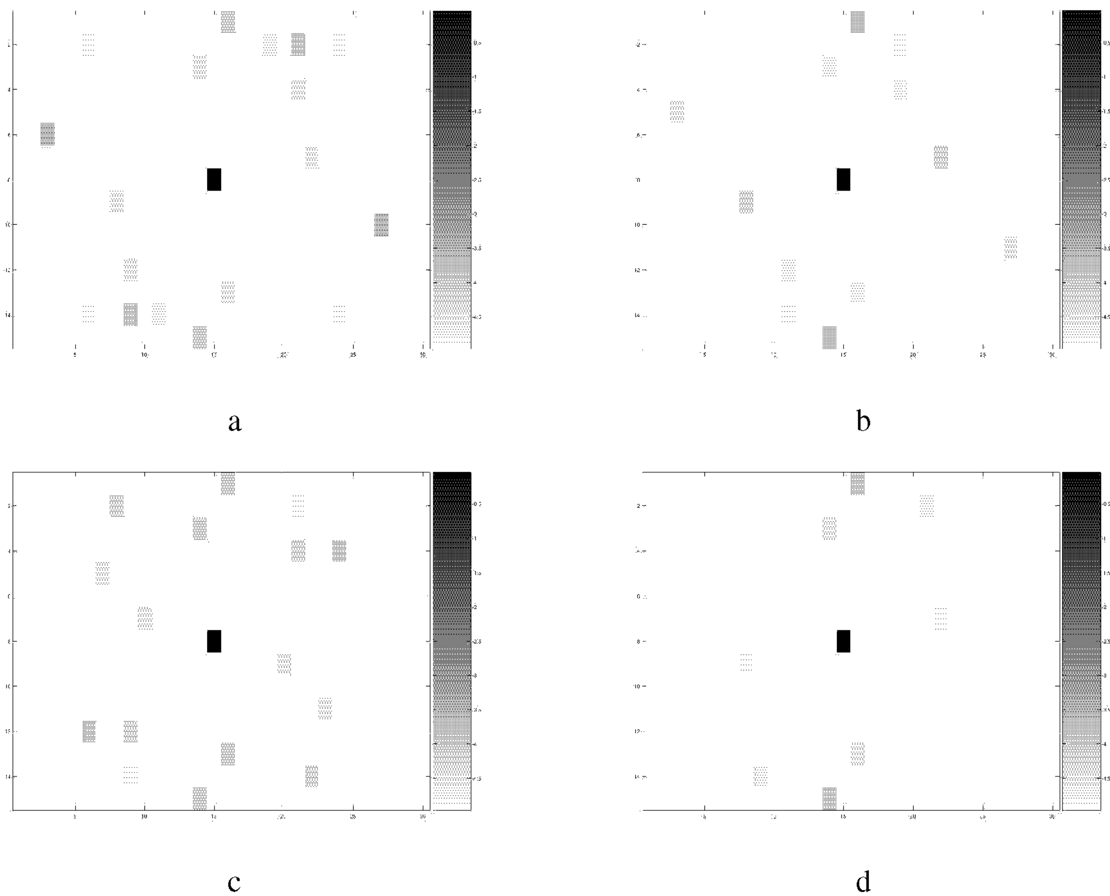


Fig. 4. Plot of the discrete aperiodic ambiguity function of shifts of the Björck CAZAC of length 29, thresholded at -10dB; darker color denotes higher value. a) zero shift, b) shift by 7, c) shift by 12, and d) their average.

[9] A. Milewski, "Periodic sequences with optimal properties for channel estimation and fast start-up equalization," *IBM J. Res. Develop.*, vol. 27, no. 5, pp. 426–431, 1983.

[10] G. Björck, "Functions of modulus one on $\mathbb{Z}_n$ whose fourier transforms have constant modulus, and cyclic n-roots," 1990, pp. 131–140.

[11] B. Saffari, "Some polynomial extremal problems which emerged in the twentieth century," 2001.

[12] S. Golomb and G. Gong, *Signal Design for Good Correlation*. Cambridge University Press, 2005.

[13] J. J. Benedetto and J. Donatelli, "Ambiguity function and frame theoretic properties of periodic zero-autocorrelation waveforms," *to appear, J. of Special Topics in Signal Processing*, 2007.

[14] L. Bömer and M. Antweiler, "Optimizing the aperiodic merit factor of binary arrays," *Signal Processing*, vol. 30, no. 1, pp. 1–13, 1993.

[15] P. Borwein, S. Choi, and S. Yazdani, "Extremal property of fekete polynomials," *Proceedings of the American Mathematical Society*, vol. 129, pp. 19–27, 2001.