Unimodular Perfect and Nearly Perfect Sequences: A Variation of Björck's Scheme

K. T. Arasu, *Member, IEEE*, Michael R. Clark, *Member, IEEE*, and Jeffrey R. Hollon

***Abstract*— Constant Amplitude (CA), Zero Auto Correlation (ZAC) sequences (or CAZAC sequences, aka perfect sequences) have numerous applications. We generalize the CAZAC notion to what we term as CASAC by permitting small autocorrelations (SAC). We extend Björck's classification result of two-valued CAZAC sequences by providing a complete classification of all almost 2-valued (i.e., two-valued except for the first position which uses a third value) CASAC sequences. While Björck's original work dealt only with primes p, we extend his ideas to any abelian group of order $v \equiv 1 \pmod 4$, as opposed to restricting just to the prime fields GF(p). Björck sequences have better ambiguity function than Zadoff-Chu sequences, making them suitable for radar and communications applications in the presence of high Doppler shifts. In fact, the discrete narrow band ambiguity function has an optimal bound in case of Björck sequences (as opposed to Gauss sequences). A one-parameter infinite family of CASAC we construct would have applications in Multiple-Input Multiple-Output (MIMO) areas. Toward MIMO applications, we introduce a performance measure we term as cross merit factor to study cross correlation behavior, generalizing the well-known notion of Golay Merit Factor (GMF).**

***Index Terms*— Unimodular sequences, perfect sequences, Legendre sequences, CAZAC sequences, Björck sequences, merit factor, zero autocorrelation, Paley type partial difference sets.**

I. Introduction

SEQUENCES, whose entries are complex unimodular values with near perfect auto-correlation properties, have many applications in communication systems such as Code Division Multiple Access (CDMA) and radar systems. Sequences and their higher dimensional counterparts (arrays) are critical in today's technological world where they are used in radar, error correction, digital communication, etc. A good treatise on sequences with good correlation properties was written by Golomb and Gong [1].

Constant Amplitude (CA), *Zero Auto Correlation* (ZAC) sequences (or CAZAC sequences) are sometimes referred to as *perfect* sequences (because of the ZAC property) with *unit magnitude* (because of the CA property) [2], [3]. CAZAC sequences have numerous applications: linear system parameter identification [4], [5], real-time channel evaluation [6], synchronization, timing measurements [7], direct-sequence spread-spectrum multiple access (DS/SSMA) and frequency hopped spread-spectrum multiple access (FH/SSMA) [1], [8]. The study of CAZAC property originated in radar and communication theory. The constant amplitude part of the property ensures the ability to transmit signals at peak power constantly, while the zero autocorrelation part of the property ensures that returning radar signals do not interfere with outgoing signals. Frank-Zadoff-Chu [9], [10], P4 [11], and Wiener sequences [12] are three classes of sequences that are certainly CAZAC. They belong to a class of sequences known as chirp-like sequences [13]. CAZAC sequences are used in 4G LTE (Long Term Evolution) wireless standard [14] and in the development of 5G wireless communication technology [15], [16]. CAZAC sequences are important in waveform design because of their optimal transmission efficiency and tight time localization properties. There is an extensive literature on CAZAC sequences because of the importance of such sequences in communications, coding theory, cryptology, and radar (see Benedetto et al. [2], [17], and references therein).

The work presented herein has resulted in the discovery of new infinite sets of pairs of sequences all of whose out-of-phase periodic auto-correlation values may be set to an arbitrary and desirable (small) value. The motivation of our constructions stems from the Björck sequence and we call the constructed sequences Björck-like sequences. The importance of Björck sequences has been stressed in [17], where the authors show for these sequences (as opposed to Gauss sequences) the discrete narrow band ambiguity function has an optimal bound. In [18], it is established that Björck sequences have better ambiguity function than Frank-Zadoff-Chu sequences, making them suitable for radar and communications applications in the presence of high Doppler shifts. For more details on the original Björck construction see [19], [20], and [21].

In this paper, we employ algebraic methods to expand the perfect Björck sequences into infinite sets of nearly-perfect sequences.

In Section II, we provide basic definitions and algebraic preliminaries that pertain to group rings [22], [23] and combinatorial structures like Paley difference sets [23] and partial

Manuscript received 4 March 2021; revised 3 October 2022; accepted 29 November 2022. Date of publication 9 December 2022; date of current version 17 March 2023. *(Corresponding author: K. T. Arasu.)*

K. T. Arasu and Michael R. Clark are with Riverside Research, Beavercreek, OH 45431 USA (e-mail: karasu@riversideresearch.org; mclark@RiversideResearch.org).

Jeffrey R. Hollon is with Radiance Technologies, Beavercreek, OH 45431 USA (e-mail: jeffrey.hollon@radiancetech.com).

Communicated by K.-U. Schmidt, Associate Editor for Sequences.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIT.2022.3228166.

Digital Object Identifier 10.1109/TIT.2022.3228166

difference sets [23]. Section III deals with our new construction methods of what we call *Björck-like sequences*. Section IV shows some numerical simulations to support the optimality of our Björck-like sequences.

We summarize our contributions below:

- We analyze, extend and characterize the construction Björck [19] employed to construct CAZAC sequences. While Björck's original work dealt only with primes p, we extend his ideas to several infinite families of groups of order $v \equiv 1 \pmod 4$), where v need not be a prime power, which yield what we term as CAZAC arrays (as in [22]), whose one-dimensional instance would reduce to sequences.
- We also relax *ZAC* to *SAC* (zero auto correlation to small auto correlation which we denote by ϵ). In Theorems 4 and 6, we obtain full characterization in this *CASAC* case (we call them *Björck-like*) and construct infinite families of such nearly-perfect sequences. These might be useful in MIMO and CDMA sort of applications.
- We show that the corresponding generalization for $q \equiv 3 \pmod 4$ does not yield any interesting sequences (Theorems 7 and 8).
- We construct a three-valued (almost 2-valued as one value $e^{i\theta}$ occurs only once and the other two values $e^{2i\theta}$ and 1 occur equally often) CASAC. This one-parameter infinite family (θ being the parameter) may be of interest in MIMO type applications (e.g. massive MIMO radar study). Prior families (like binary perfect sequences) with perfect periodic autocorrelations contain only a handful for a given length and their lengths also have restrictions.
- We carry out the analogous investigation that parallels the analysis of Saffari [20] who fully settled the general parameter characterization of two-valued CAZAC sequences. M-sequences exist only for lengths $n \equiv 3 \pmod 4$ and Saffari has fully solved the problem for that case. While two-valued CAZAC sequences cannot exist for lengths $n \equiv 1 \pmod 4$, almost two-valued (i.e., two-valued except for the first position which uses a third value) Björck-like CAZACs are of interest. In Theorems 15 and 16, we fully characterize their spectrum under a modest hypothesis (the general problem is still unresolved); in particular, we prove that Björck's original CAZAC sequences (and CASAC sequences) are the only such objects under that hypothesis.
- We examine the Golay Merit Factor and bandwidth of the new sequences as well as propose a measure of performance for a set of sequences akin to the Golay Merit Factor. This new performance measure is what we call "cross merit factor" which enables the study of cross correlation behaviors that are useful in MIMO applications.

The remainder of this paper is organized as follows: Section II provides algebraic preliminaries, Section III deals with our new construction methods, Section IV gives computer simulation results to support the optimality of our sequences and introduces a new performance measure to study cross correlation behaviors and Sections V concludes the paper and discusses open problems for future work.

II. Preliminaries

A sequence $\mathbf{a} = (a_i)$ is called periodic with period n provided that $a_i = a_{i+n}$ for all i. The periodic cross-correlation function of the sequences **a** and **b** is defined by:

$$C(t) = \sum_{i=0}^{n-1} a_i b^*_{(i+t) \bmod n} \tag{1}$$

where b_i^* represents the complex conjugate of b_i. In this definition, if $\mathbf{a} = \mathbf{b}$, we call it the periodic auto-correlation function (ACF) of **a**. Note that the sequence $C = C(t)$ is also periodic with period n, so that it suffices to consider the auto-correlation coefficients $C(t)$ for $t \in \{0, 1, \ldots, n-1\}$. The ACF measures how much the original sequence differs from its translates. Furthermore, we now present the aperiodic version of the ACF as well as a common measure of sequence performance known as the Golay Merit Factor. For more on Golay Merit Factor, refer to Schmidt's work [24] and references therein.

Definition 1: The aperiodic cross-correlation function of two sequences **a** and **b**, C_{aper}, is defined by

$$C_{aper}(l) = \sum_{i=0}^{n-1-l} a_i b^*_{i+l}$$

where a_i^* represents the complex conjugate of a_i and $0 \leq l < n$. If $\mathbf{a} = \mathbf{b}$, then this is referred to as the aperiodic auto-correlation function.

Definition 2: The Golay Merit Factor (GMF) of a sequence **a** is defined by

$$GMF = \frac{C^2_{aper}(0)}{2\sum_{l=1}^{n-1} |C_{aper}(l)|^2}.$$

The classical notion of bi-unimodular sequences dates back to Gauss, but the term *bi-unimodular sequence* was coined by Björck and Saffari (see [21]):

Definition 3: A bi-unimodular sequence is a unimodular finite vector, whose Discrete Fourier Transform is also unimodular.

The following characterization of CAZAC sequences is given as Proposition 1.2.1 in [2].

Theorem 1: A sequence S is CAZAC if and only if S is bi-unimodular.

The Björck sequences introduced in [19], [21], and [2] are bi-unimodular vectors of a prime length p.

For $p \equiv 3 \pmod 4$ their coefficients are either 1 or $e^{i\theta}$ with $\theta = \arccos \frac{1-p}{1+p}$.

For $p \equiv 1 \pmod 4$ their coefficients are either 1, $e^{i\eta}$, or $e^{-i\eta}$ with $\eta = \arccos \frac{1}{\sqrt{p}+1}$.

A more formal definition of Björck sequences is given in the following definition.

Definition 4: Given a prime p, the function $u : \mathbb{Z}_p \to \mathbb{C}$ defined by $u(m) = e^{i\theta_p(m)}$, $0 \leq m \leq p-1$, is a Björck sequence if

For $p \equiv 1 \pmod 4$, we have $\theta_p(m) = \left(\frac{m}{p}\right) \arccos \frac{1}{\sqrt{p}+1}$; (Here $\left(\frac{m}{p}\right)$ is the classical 3-valued Legendre symbol)

For $p \equiv 3 \pmod 4$, we have $\theta_p(m) = \arccos\frac{1-p}{1+p}$ or 0, depending on whether m is a quadratic non-residue modulo p or not.

The following theorem is due to Björck, see [19] and [21].

Theorem 2: Björck sequences are CAZAC sequences.

Two-valued CAZACs have been classified by Saffari [20]. The result of Saffari states that two-valued CAZACs exist for lengths $n \geq 3$ if and only if a) $n \equiv 3 \pmod 4$ and there exists a Hadamard-Paley difference set in a cyclic group of order n, or b) $n \equiv 0 \pmod 4$ and there exists a Hadamard-Menon difference set in a cyclic group of order n. For more difference sets and related topics refer to [22]. In either case, explicit formulas are provided for the construction of the CAZAC sequence. It follows that two-valued CAZAC sequences cannot exist for lengths $n \equiv 1 \pmod 4$. However, note that in this case, Björck CAZAC sequences are almost two-valued (i.e., two-valued except for the first position which uses a third value).

A most fertile general setting in which to study Björck sequences and their variations is the group ring RG, where R is a ring with unity and G is a finite abelian group. In this paper R will usually be the field of complex numbers $\mathbb{C}$, one of its cyclotomic subfields or the ring of integers in one of these subfields.

Definition 5: Let G be an arbitrary finite group which we denote multiplicatively. The *group ring* of G over the field of complex numbers $\mathbb{C}$, denoted $\mathbb{C}G$, is comprised of all formal sums

$$A = \sum_{g\in G} a_g g, \quad a_g \in \mathbb{C},$$

with addition defined component-wise; i.e.

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g := \sum_{g\in G} (a_g + b_g) g,$$

and multiplication defined by *convolution*; i.e.

$$\begin{aligned}\left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g\right) &:= \sum_{g,h\in G} a_g b_h gh \\ &= \sum_{g\in G}\left(\sum_{hk=g} a_h b_k\right) g \\ &= \sum_{g\in G}\left(\sum_{h\in G} a_{gh} b_{h^{-1}}\right) g.\end{aligned}$$

Definition 6: If $W = \sum_{g\in G} a_g g$ is an element of $R[G]$ and t is any integer, then

$$\left(\sum_{g\in G} a_g g\right)^{(t)} = \sum_{g\in G} a_g g^t.$$

A k-element subset D of a finite group G of order v is called a (v,k,λ)-difference set if for every non-identity element $g \in G$, there are exactly λ elements $(d_1, d_2) \in D \times D$ such that $d_1 d_2^{-1} = g$

A subset $S \subseteq G$ can be identified with the element, denoted again by S,

$$S = \sum_{g\in S} g \in \mathbb{Z}[G].$$

The following is an easy consequence of the above definition.

Lemma 1: Let D a k-subset of an abelian group G of order v. Then D is a (v,k,λ) difference set if and only if

$$DD^{(-1)} = k - \lambda + \lambda G \ in \ \mathbb{Z}[G].$$

Remark: Difference sets are studied in the more general group (not necessarily cyclic) theoretic context. Since we are primarily dealing with sequences, we restrict our attention to cyclic groups $\mathbb{Z}_v$. We use the term "array", when the group in question is non-cyclic. For more on these and related studies that pertain to sequences and arrays and their interplay with combinatorial designs, refer to the survey article [22].

Example 1 (Hadamard-Paley Difference Set): Let q be a prime power and $q \equiv 3\,(mod\,4)$. Let $GF(q)$ denote the finite field with q elements and α be a primitive element of $GF(q)$. Define:

$$\begin{cases} S = \{\alpha^{2i} | i = 0, 1, \ldots, \frac{q-3}{2}\} \\ N = \{\alpha^{2j+1} | j = 0, 1, \ldots, \frac{q-3}{2}\} \end{cases}$$

i.e. S and N consist precisely of the square and non-square elements of $GF(q) \setminus \{0\}$. Then S and N are themselves difference sets in the group $G = (GF(q), +)$ with parameters $(v,k,\lambda) = (q, \frac{q-1}{2}, \frac{q-3}{4})$. Hence the following equations hold in the group ring $\mathbb{Z}[G]$:

$$\begin{gathered} SS^{(-1)} = NN^{(-1)} = \left(\frac{q+1}{4}\right) + \left(\frac{q-3}{4}\right) G \\ N = S^{(-1)} \\ S = N^{(-1)} \\ 1 + S + N = G \end{gathered}$$

The next example gives rise to the so called partial difference set. For more on partial difference sets, refer to [23].

Definition 7: Let G be a multiplicative group of order v. A subset $D \subseteq G$ of size k is said to be a (v,k,λ,μ) partial difference set (PDS) in G if

1) $1 \notin D$
2) $D = D^{(-1)}$
3) $DD^{(-1)} = D^2 = k + \lambda D + \mu(G - D - 1)$ in ZG.

Example 2: Paley Partial Difference Set for prime power $q \equiv 1\,(mod\,4)$

Let q be a prime power, $q \equiv 1\,(mod\,4)$. Let $GF(q)$ denote the finite field with q elements. Fix a primitive element α of $GF(q)$ and define:

$$\begin{cases} S = \{\alpha^{2i} | i = 0, 1, \ldots, \frac{q-3}{2}\} \\ N = \{\alpha^{2j+1} | j = 0, 1, \ldots, \frac{q-3}{2}\}. \end{cases}$$

Thus, S and N consist precisely of the square and non-square elements of $GF(q) \setminus \{0\}$. It is well known that S and N are themselves partial difference sets in the group $G = (GF(q), +)$ with parameters $(v,k,\lambda,\mu) = (q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$.

Lemma 2: Let q be a prime power satisfying $q \equiv 3(mod 4)$. Then $SN^{(-1)} = \left(\frac{q+1}{4}\right) G - \left(\frac{q+1}{4}\right) - S$.

Proof: By Equation (2), $SN^{(-1)} = SS$. Further, $SS = S(G-N-1)$ by Equation (2) and $N = S^{(-1)}$ by Equation (2). Simple calculation using these gives the result. □

In a similar manner, we obtain:

Lemma 3: Let q be a prime power, where $q \equiv 3\ (mod\ 4)$. Then $S^{(-1)}N = \left(\frac{q+1}{4}\right) G - \left(\frac{q+1}{4}\right) - N$.

Analogous result for $q \equiv 1\ (mod\ 4)$ is given below, without proof.

Lemma 4: Let q be a prime power with $q \equiv 1\ (mod\ 4)$. Then $SN = \left(\frac{q-1}{4}\right) G - \left(\frac{q-1}{4}\right)$.

Remark: Though Example 2 and Lemma 4 are stated only for $GF(q)$, the performed calculations are only based on parameters (without the need to allude to any combinatorial designs) and hence work for all PDS with Paley parameters $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$ in any abelian group of order v. We shall exploit this generalization in Section III-A in conjunction with Theorem 3 and in Section III-E.

More on the Paley sequences can be found in [25]. The main focus of this paper, the Björck sequence/array, is a complex valued, prime power length $q \equiv 1\ (mod\ 4)$, sequence/array whose auto-correlation is constant. If we let B represent the Björck sequence/array, then the sequence/array B itself is defined as

$$B = 1 + \alpha S + \bar{\alpha} N \tag{2}$$

for some complex number α and its complex conjugate $\bar{\alpha}$. The sets S and N correspond to the non-zero square and non-square elements of $GF(q)$ respectively. Definition 4 and Theorem 2 yield the following facts: The value of α is given as

$$\alpha = \frac{1}{\sqrt{q}+1} + i\frac{\sqrt{q+2\sqrt{q}}}{\sqrt{q}+1} \tag{3}$$

and can be shown to be both unimodular and provide a perfect periodic auto-correlation function satisfying

$$BB^{(-1)} = q. \tag{4}$$

More on the Björck sequence can be found in [19], [20], and [21].

III. New Families of Björck-Like Sequences

In this section we dissect and analyze the importance of the unimodularity of α (i.e. $|\alpha| = 1$) and attempt to generalize the notion of Björck sequence.

Throughout this section, we shall let q denote a prime power.

A. More Perfect Sequences Utilizing Other Values for α

In Theorem 3 below, we show that Björck's construction for primes p with $p \equiv 1\ (\mathrm{mod}\ 4)$ would work for only two sets of parameters η: one given in Definition 4 above and another when $\eta = \arccos\frac{-1}{\sqrt{p}-1}$. We actually prove this result for all prime powers q by working in $GF(q)$ and the resulting *higher dimensional arrays* could hence be termed as *Björck arrays* as in the terminology of [22].

As a first step, we ask ourselves if other values for α exist which will hold the perfect property of the Björck sequence (Equation 4) beyond the canonical one given in Equation 3. The result of this analysis provides a second value for α and is described next.

Theorem 3: Let $B = 1 + \alpha S + \bar{\alpha} N$ with $|\alpha| = 1$ be the Björck sequence, where the sets S and N are respectively the square and non-square elements of $GF(q)$ with $q \equiv 1\ (\mathrm{mod}\ 4)$. Then only the following two constants

$$\alpha = \frac{1}{\sqrt{q}+1} + i\frac{\sqrt{q+2\sqrt{q}}}{\sqrt{q}+1}$$

and

$$\alpha = \frac{-1}{\sqrt{q}-1} + i\frac{\sqrt{q-2\sqrt{q}}}{\sqrt{q}-1}$$

will provide perfect periodic auto-correlations for the sequence B; i.e. $BB^{(-1)} = q$.

Proof: Let $B = 1 + \alpha S + \bar{\alpha} N$, then the periodic auto-correlation function can be calculated, explicitly, by

$$\begin{aligned} BB^{(-1)} =& (1 + \alpha S + \bar{\alpha} N)(1 + \alpha S + \bar{\alpha} N)^{(-1)} \\ =& (1 + \alpha S + \bar{\alpha} N)\overline{(1 + \alpha S + \bar{\alpha} N)} \\ =& (1 + \alpha S + \bar{\alpha} N)(1 + \bar{\alpha} S + \alpha N) \\ =& 1 + \bar{\alpha} S + \alpha N + \alpha S + S^2 + \alpha^2 SN + \bar{\alpha} N \\ & + \bar{\alpha}^2 SN + N^2. \end{aligned}$$

Next, we use the well-known properties of the difference sets S and N which give the following substitutions for S^2, N^2, and SN. Note that $G - 1 = S + N$.

$$\begin{cases} S^2 = \frac{q-1}{2} + \left(\frac{q-5}{4}\right) S + \left(\frac{q-1}{4}\right) N \\ N^2 = \frac{q-1}{2} + \left(\frac{q-5}{4}\right) N + \left(\frac{q-1}{4}\right) S \\ SN = \left(\frac{q-1}{4}\right) (G-1). \end{cases} \tag{5}$$

Substituting these three expressions into $BB^{(-1)}$ and simplifying yield

$$\begin{aligned} BB^{(-1)} = q + \left(\bar{\alpha} + \alpha + \frac{2q-6}{4} + \left(\frac{q-1}{4}\right)(\bar{\alpha}^2 + \alpha^2)\right) \\ (S+N). \end{aligned}$$

For this sequence to be perfect, we require $BB^{(-1)} = q$ implying that the coefficient of $S+N$ is 0. Hence we continue by solving

$$\bar{\alpha} + \alpha + \frac{2q-6}{4} + \left(\frac{q-1}{4}\right)(\bar{\alpha}^2 + \alpha^2) = 0 \tag{6}$$

under the constraint that $|\alpha| = 1$. We let $\beta = \alpha + \bar{\alpha}$. This allows for Equation 6 to be transformed into standard quadratic form in β by

$$\left(\frac{q-1}{4}\right)\beta^2 + \beta - 1 = 0.$$

This is now solvable for β with the quadratic formula yielding the two solutions

$$\beta = \left\{\frac{2}{\sqrt{q}+1}, \frac{-2}{\sqrt{q}-1}\right\}.$$

Now, with the knowledge of β, we can solve for α as $\beta = \alpha + \bar{\alpha}$. This is equivalent to $\beta = \alpha + \frac{1}{\alpha}$ and is now quadratic in α. Again, using the quadratic formula gives us the desired result. □

As explained in Section II, a sequence (also an array) can be regarded as a group ring element. Two group ring elements are equivalent if and only if one can be obtained from the other by some combination of group automorphism, group translation and automorphism of the coefficient ring. Two sequences/arrays are equivalent if their corresponding group elements are; else they are considered inequivalent.

This section shows that there exists a pair of inequivalent Björck sequences which achieve perfect auto-correlations with the coefficient parameter satisfying $|\alpha| = 1$.

Remark: Since Example 2 and Lemma 4 work for all PDS with Paley parameters $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$ and the performed calculations in Theorem 3 are only based on parameters, the stated conclusions hold true for all PDS with the aforementioned Paley parameters in any abelian group of order v with $v \equiv 1 \pmod 4$.

B. Björck-Like Sequences With Constant Periodic Auto-Correlations

In this section, we investigate a relaxing of the perfect condition of the Björck sequence. That is, we consider what happens if we allow for the auto-correlation to be any constant, say ϵ, instead of forcing $\epsilon = 0$ as before. The Björck-like sequence is constructed in the typical way,

$$B = 1 + \alpha S + \bar{\alpha} N$$

and $|\alpha| = 1$, but now with a new right hand side, the periodic auto-correlation, given by

$$BB^{(-1)} = q + \epsilon(G - 1).$$

While we can show that the parameter ϵ may be chosen arbitrarily, except with certain restrictions given in Theorem 6, we will proceed under the assumption that small auto-correlation values are desirable and emphasize the particular case when $|\epsilon| < 1$. We now state, without proof, the following generalization of the previous theorem which dealt with the special case $\epsilon = 0$. We single out by separating these two results due to their applications.

Theorem 4: A pair of Björck-like sequences of length q, with $q \equiv 1 \pmod 4$, exists such that for any ϵ and the sequence $B = 1 + \alpha S + \bar{\alpha} N$ satisfying $BB^{(-1)} = q + \epsilon(G-1)$, exists if and only if

$$\alpha = \frac{\beta \pm \sqrt{\beta^2 - 4}}{2}$$

and

$$\beta = \frac{-2 \pm 2\sqrt{q(1+\epsilon) - \epsilon}}{q-1}.$$

Remark: Since Example 2 and Lemma 4 work for all PDS with Paley parameters $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$ and the performed calculations in Theorem 4 are only based on parameters, the stated conclusions hold true for all PDS with the aforementioned Paley parameters in any abelian group of order v with $v \equiv 1 \pmod 4$.

We now complete this section with two subsections. First, we demonstrate that we can optimize over the parameter ϵ to find the sequence pairs which minimize the bandwidth (phase angle) between them and second find necessary and sufficient conditions on sequence length q and parameter ϵ which must be satisfied for these Björck-like sequence pairs to exist.

1) Optimizing the Choice of ϵ by Bandwidth: The bandwidth of a signal (sequence) is proportional to the phase of its entry $\alpha = x + iy$, for $x, y \in \mathbb{R}$, as the two entries in the sequence B are either α or its conjugate whose phase angle is equal but opposite to α. The phase angle of α is defined to be $\theta(\epsilon) = \arctan \frac{y}{x}$ and we consider only small auto-correlation values for this analysis. That is, we assume $|\epsilon| \leq 1$. First, we must get the correct form of the phase angle.

Corollary 1: The phase angle of $\alpha = x + iy$ is given by $\arctan \frac{y}{x} = \arctan \frac{\sqrt{4-\beta^2}}{\beta}$.

Proof: To show this, we note that $|\beta| \leq 2$ where $\beta = \frac{-2 \pm 2\sqrt{q(1+\epsilon)-\epsilon}}{q-1}$. (This follows easily using $\sqrt{q(1+\epsilon)-\epsilon} \leq (2q-1)$ for $\epsilon \in [-1, 1]$). Hence we can re-write α as

$$\alpha = \frac{\beta \pm i\sqrt{4-\beta^2}}{2}.$$

Thus we have that the phase angle of α is $\arctan \frac{\sqrt{4-\beta^2}}{\beta}$. □

Now that we have an expression for the phase angle of the signal (sequence), we can proceed by minimizing its value. As $\arctan$ is an increasing function, this is equivalent to minimizing its argument which we call $Z(\epsilon) = \frac{\sqrt{4-\beta^2}}{\beta}$. Using elementary calculus with some tedious calculations, we obtain the following theorem - we state it without proof.

Theorem 5: The bandwidth (phase angle) of the Björck-like sequence is minimized when $\epsilon = 1$.

2) Restrictions on the Length q and Parameter ϵ for Björck-Like Sequences: During numerical studies of these sequences it was noticed that not any combination of sequence length, q, and parameter ϵ were sufficient to guarantee a Björck-like sequence. Here we investigate the necessary and sufficient conditions for which these sequences exist.

Theorem 6: For a Björck-like sequence to exist with length q, with $q \equiv 1 \pmod 4$, and correlation parameter $\epsilon \in [-1, 1]$, the following four conditions are necessary and sufficient as a whole:

1) $q \geq \epsilon$
2) $q(1+\epsilon) - \epsilon \geq 0$
3) $2 - q \leq \sqrt{q(1+\epsilon) - \epsilon} \leq q$
4) $2 - q \leq -\sqrt{q(1+\epsilon) - \epsilon} \leq q$

Proof: Let χ be a non-principle character of the cyclic group G. From the group ring equation, $BB^{(-1)} = q + \epsilon(G-1)$, and utilizing that $|\alpha| = |x + iy| = x^2 + y^2 = 1$, we find that

$$\chi(BB^{(-1)}) = \chi(q + \epsilon(G-1))$$

$$\|1 + \alpha\frac{-1+\sqrt{q}}{2} + \bar{\alpha}\frac{-1-\sqrt{q}}{2}\|^2 = q - \epsilon$$

from which we get

$$(q-1)x^2 + 2x - 1 - \epsilon = 0$$

which can be solved for x by the quadratic formula giving

$$x = \frac{-1 \pm \sqrt{q(1+\epsilon) - \epsilon}}{q-1}.$$

The first two conditions come from the following arguments: First, $q-\epsilon$ is a sum of two squares thus $q-\epsilon \geq 0$ and second, the values of x and y are both real numbers so the discriminant must satisfy $q(1+\epsilon)-\epsilon \geq 0$. The last two conditions come from that $|x| \leq 1$ as otherwise $|\alpha| \nleq 1$. Since $|x| \leq 1$, then

$$-1 \leq \frac{-1 \pm \sqrt{q(1+\epsilon) - \epsilon}}{q-1} \leq 1$$

which upon rewriting gives the last two conditions as

$$2 - q \leq \pm\sqrt{q(1+\epsilon) - \epsilon} \leq q.$$

This completes the proof of necessity. Sufficiency follows from the construction provided in Theorem 4. □

C. The Case of Björck-Like Sequences of Length $q \equiv 3 \ (mod\ 4)$

In this section we look at the case of the Björck-like sequence but for lengths $q \equiv 3 \ (mod\ 4)$. We first examine $B = 1+\alpha S+\bar{\alpha}N$ followed by the case of $B = i+\alpha S+\bar{\alpha}N$.

Theorem 7: For length $q \equiv 3 \ (mod\ 4)$, the only Björck-like sequence, $B = 1 + \alpha S + \bar{\alpha}N$, with constant periodic auto-correlation is when $\alpha = \pm 1$.

Proof: Let $B = 1 + \alpha S + \bar{\alpha}N$ be the sequence for length $q \equiv 3 \ (mod\ 4)$. Then we continue by expanding and simplifying the expression for the periodic auto-correlation $BB^{(-1)}$.

$$\begin{aligned} BB^{(-1)} =& (1 + \alpha S + \bar{\alpha}N)(1 + \alpha S + \bar{\alpha}N)^{(-1)} \\ =& q + \left(2\alpha + \frac{q-3}{2} + \frac{q-3}{4}\alpha^2 + \frac{q+1}{4}\bar{\alpha}^2\right) S \\ &+ \left(2\bar{\alpha} + \frac{q-3}{2} + \frac{q+1}{4}\alpha^2 + \frac{q-3}{4}\bar{\alpha}^2\right) N. \end{aligned}$$

We now use the fact that the coefficient of S and N must be equal and obtain (after some elementaty algebra):

$$2\alpha - \alpha^2 = 2\bar{\alpha} - \bar{\alpha}^2$$

Now, we write $\alpha = x + iy$ and use $|\alpha| = 1$ to obtain

$$y - xy = -y + xy$$

If $y = 0$ then $\alpha = x = \pm 1$ by the assumption $|\alpha| = 1$ or otherwise $1 - x = -1 + x$ giving $x = 1$ and $y \neq 0$ which is a contradiction to the unimodularity of α. Thus, the only solution is $\alpha = \pm 1$. □

Aling the same lines of the above result, we can prove the following:

Theorem 8: For length $q \equiv 3 \ (mod\ 4)$, the only Björck-like sequence, $B = i + \alpha S + \bar{\alpha}N$, with constant periodic auto-correlation is when $\alpha = \pm 1$.

We have shown with the two previous theorems that the Björck-like sequences of length $q \equiv 3 \ (mod\ 4)$ are not as interesting as the rich class of sequences which form from the $q \equiv 1 \ (mod\ 4)$ lengths.

D. A New Björck-Like Vari-Angular Sequence of Length $q \equiv 1 \ (mod\ 4)$

Here we examine a unimodular three-valued Björck-like sequence of the form

$$B = e^{i\theta} + \alpha S + N$$

which has constant periodic auto-correlations. We will show that the parameter θ is free to vary but can be optimized to minimize the value of the correlations.

Theorem 9: The three-valued unimodular sequence $B = e^{i\theta} + \alpha S + N$ of length $q \equiv 1 \ (mod\ 4)$ has constant periodic auto-correlations when $\alpha = 1$ or $e^{2i\theta}$.

Proof: Let $B = e^{i\theta} + \alpha S + N$ of length $q \equiv 1 \ (mod\ 4)$. Then the periodic auto-correlation function can be computed as

$$\begin{aligned} BB^{(-1)} =& \left(e^{i\theta} + \alpha S + N\right)\left(e^{i\theta} + \alpha S + N\right)^{(-1)} \\ =& q + \left(\bar{\alpha}e^{i\theta} + \alpha e^{-i\theta} + (\alpha + \bar{\alpha})\frac{q-1}{4} + \frac{q-3}{2}\right) S \\ &+ \left(e^{i\theta} + e^{-i\theta} + (\alpha + \bar{\alpha})\frac{q-1}{4} + \frac{q-3}{2}\right) N. \end{aligned}$$

Now, we wish for the auto-correlation to be constant so we set the coefficients of S and N equal to one another and solve for α by first writing it in quadratic form.

$$\begin{aligned} \bar{\alpha}e^{i\theta} + \alpha e^{-i\theta} + (\alpha + \bar{\alpha})\frac{q-1}{4} + \frac{q-3}{2} \\ = e^{i\theta} + e^{-i\theta} + (\alpha + \bar{\alpha})\frac{q-1}{4} + \frac{q-3}{2} \\ \alpha^2 - \alpha\left(e^{2i\theta} + 1\right) + e^{2i\theta} = 0. \end{aligned}$$

Now, using the quadratic formula, we can solve for the two roots of α.

$$\alpha = \frac{e^{2i\theta} + 1 \pm \left(e^{2i\theta} - 1\right)}{2}$$

giving the two roots as $\alpha = 1$ or $e^{2i\theta}$. □

Note that in the case of $\alpha = 1$ the sequence is not very interesting. We continue by focusing on the case of $\alpha = e^{2i\theta}$ giving the interesting sequence of

$$B = e^{i\theta} + e^{2i\theta}S + N.$$

We wish to further examine what auto-correlation values this sequence achieves. Using the expansion of $BB^{(-1)}$, the non-identity correlations will be given by

$$e^{i\theta} + e^{-i\theta} + (e^{2i\theta} + e^{-2i\theta})\frac{q-1}{4} + \frac{q-3}{2}$$

which is equivalent to

$$2cos(\theta) + \frac{q-1}{2}cos(2\theta) + \frac{q-3}{2}$$

after applying Euler's identity. If we consider this a function of θ then we may examine it for critical values. That is, let $f(\theta) = 2\,cos(\theta) + \frac{q-1}{2}cos(2\theta) + \frac{q-3}{2}$ and determine the critical values from solving $f'(\theta) = 0$. We proceed to do just that:

$$\begin{aligned} f'(\theta) =& -2sin(\theta) - 2(q-1)sin(2\theta) \\ =& -2sin(\theta) - 2(q-1)sin(\theta)cos(\theta) \\ =& -2sin(\theta)\left(1 + (q-1)cos(\theta)\right) \end{aligned}$$

and by setting this to 0, we find two roots for θ being when $sin(\theta) = 0$ or $cos(\theta) = \frac{-1}{q-1}$. If $sin(\theta) = 0$ then we get that $\theta = 0$ which results in a maximal correlation as

$$\begin{aligned} f(\theta = 0) =& 2cos(0) + \frac{q-1}{2}cos(0) + \frac{q-3}{2} \\ =& q. \end{aligned}$$

On the other hand, the minimal correlation occurs when $cos(\theta) = \frac{-1}{q-1}$ when the correlations themselves are

$$\begin{aligned} f(\theta) =& 2\ cos(\theta) + \frac{q-1}{2}\left(2cos^2(\theta) - 1\right) + \frac{q-3}{2} \\ =& \frac{-q}{q-1}. \end{aligned}$$

This is the minimal value for the correlation and asymptotically, by length, approaches -1.

Remark: In Theorem 9 (for the case $q \equiv 1 \pmod 4$), we obtain a three-valued (almost 2-valued as one value $e^{i\theta}$ occurs only once and the other two values $e^{2i\theta}$ and 1 occur equally often) unimodular nearly perfect family of sequences. This one-parameter infinite family (θ being the parameter) may be of interest in MIMO type applications. Toward that, we shall introduce (in Section IV) a new performance measure we term as *cross merit factor* which reduces to the classical GMF when a single sequence is employed.

E. Extending Saffari's Construction

Clever analysis of Saffari [20] fully settles the general parameter characterization of two-valued CAZAC sequences. We state it as a theorem:

Theorem 10 (Saffari [20]): Two-valued CAZAC sequences exist for lengths $n \geq 3$ if and only if a) $n \equiv 3 \pmod 4$ and there exist a Hadamard-Paley difference set of length n, or b) $n \equiv 0 \pmod 4$ and there exists a Hadamard-Menon difference set of length n.

It follows that two-valued CAZAC sequences cannot exist for lengths $n \equiv 1 \pmod 4$. In this case, Björck CAZAC sequences are almost two-valued. Analogous analysis to obtain parameter characterizations for this almost two-valued case is the task we now undertake. We wish to solve the problem of finding abelian groups G of order v that contain a suitable subset D such that the group ring element $X = 1 + \alpha D + \beta(G - D - 1)$ (for suitable unimodular complex numbers α and β) satisfies XX^* is a constant (i.e., X gives rise to a G-developed CAZAC and reduce to CAZAC sequences when G is cyclic). This problem, in its full generality, seems a bit too hard. With an additional modest assumption when $\beta = \bar{\alpha}$, we are able to provide a very satisfactory solution which, in spirit, resembles the aforementioned celebrated result of Saffari (Theorem 10 above).

We require some ingredients from the theory of PDS. PDS in abelian groups G have been thoroughly studied; see [23] for a survey of older results and [26], [27], [28], [29], [30], [31], [32], [33] (and references therein) for a number of very recent results.

Parameters (v, k, λ, μ) of PDS satisfying $\beta = \lambda - \mu = -1$ have been characterized in the following theorem using well-known equivalence of PDSs and strongly regular Caley graphs.

Theorem 11: [34], Let Γ be a strongly regular Cayley graph based on an abelian group G with parameters (v, k, λ, μ) satisfying $\beta = \lambda - \mu = -1$. Then, up to complementation, Γ is either: i) of Paley type, i.e., it has the parameters of the type $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$; or ii) it has parameters $(243, 22, 1, 2)$.

Theorem 12: [23], If G is cyclic of order $v \equiv 1 \pmod 4$, then G contains a Paley PDS D if and only if v is prime and D is the set of quadratic residues modulo p (i.e., D is the classical Paley PDS).

Theorem 13: [31], Let n be a positive odd number with $n > 1$. Then there is a Paley type partial difference set in a group of order n^4 and $9n^4$.

Theorem 14: [33], Let v be an odd positive integer > 1. Then there exists a Paley type PDS in some abelian group G of order v if and only if v is a prime power and $v \equiv 1 \pmod 4$, or $v = n^4$ or $9n^4$, which $n > 1$ an odd positive integer.

We state our result now:

Theorem 15:
1) Almost two valued CAZAC sequences $X = 1 + \alpha D + \beta(G - D - 1)$ with $\beta = \bar{\alpha}$ exist in an abelian group G of order v if and only if $v \equiv 1 \pmod 4$ and D is a partial difference set in G with Paley type parameters $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$, and hence v is a prime power and $v \equiv 1 \pmod 4$, or $v = n^4$ or $9n^4$, with $n > 1$ an odd positive integer.
2) The only permissible values of α are those given in Theorem 3.
3) Furthermore, if G is cyclic, then v must be a prime (call it p) and D must be the classical Paley PDS (consisting of quadratic residues mod p), whence our almost two-valued CAZAC sequences X must be precisely Björck's original sequences characterized in Theorem 3.

Proof: [Proof of Theorem 15] Let G be an abelian group of order v and D a subset of G of size k. Let α be a unimodular complex number. We wish to investigate the group ring element $X = 1 + \alpha D + \bar{\alpha}(G - D - 1)$ that satisfies XX^* is a constant. Rewriting $X = (1 - \bar{\alpha}) + (\alpha - \bar{\alpha})D + \bar{\alpha}G$, we have $X^* = (1 - \alpha) + (\bar{\alpha} - \alpha)D^{(-1)} + \alpha G$. Simple calculation now yields:

$$\begin{aligned} XX^* = &(1-\alpha)(1-\bar{\alpha}) + (1-\bar{\alpha})(\bar{\alpha}-\alpha)D^{(-1)} \\ &+ (1-\alpha)(\alpha-\bar{\alpha})D - (\alpha-\bar{\alpha})^2 DD^{(-1)} + \gamma G \quad (7) \end{aligned}$$

where $\gamma = (\alpha - 1) + (\alpha^2 - 1)k + (\bar{\alpha} - 1) + (\bar{\alpha}^2 - 1)k + v$.

Recall our hypothesis that XX^* is a constant. We then claim that $D = D^{(-1)}$ (i.e., D is reversible, meaning closed under inversion). To establish this claim, we proceed via contradiction. Denial of $D = D^{(-1)}$ would imply the existence of two elements g and h in G such that: g is in D but not in $D^{(-1)}$ and h is in $D^{(-1)}$ but not in D. Let X_g and X_h denote the respective coefficient of g and h of the RHS of equation (7) above.

Then X_g is one of two possible values: $(1-\alpha)(\alpha-\bar{\alpha}) + \gamma$ or $(1-\alpha)(\alpha-\bar{\alpha}) + \gamma - (\alpha-\bar{\alpha})^2$.

Likewise X_h takes on one of two possible values: $(1 - \bar{\alpha})(\bar{\alpha} - \alpha) + \gamma$ or $(1-\bar{\alpha})(\bar{\alpha}-\alpha) + \gamma - (\alpha-\bar{\alpha})^2$.

Since XX^* is a constant, (7) implies that $X_g = X_h$. Straightforward analysis of each of the four possible cases yields the constraint that $\alpha = 1$, showing X is not almost two-valued, contrary to the hypothesis. This establishes the claim that $D = D^{(-1)}$.

Using the info $D = D^{(-1)}$ in (7), we obtain:

$$XX^* = (1-\alpha)(1-\bar{\alpha})+((1-\bar{\alpha})(\bar{\alpha}-\alpha)+(1-\alpha)(\alpha-\bar{\alpha}))D - (\alpha-\bar{\alpha})^2 DD^{(-1)} + \gamma G \quad (8)$$

$$= (1-\alpha)(1-\bar{\alpha})\text{-}(\alpha-\bar{\alpha})^2(D+DD^{(-1)}) + \gamma G \quad (9)$$

Since XX^* is a constant, all the coefficients of (non-identity) elements of G must be the same on the RHS of (9), hence for the group ring element $D + DD^{(-1)}$, i.e., $D + DD^{(-1)} = a + bG$ for some integers a and b. This, in conjunction with $D = D^{(-1)}$ implies that $D^{(2)} = a + bG - D$ in the group ring $\mathbb{Z}[G]$. This precisely means that D is a PDS in G with parameters (v, k, λ, μ) satisfying $\beta = \lambda - \mu = -1$. Appealing to Theorems 11 and 14, our proof of Theorem 15, part 1) is now complete, noting that the sporadic case $(243, 22, 1, 2)$ does not yield almost two-valued CAZAC sequences. Simple triangle inequality on the coefficients on the RHS of (9) would show that zero autocorrelation is impossible. To prove part 2), we compute the constant coefficient of non-identity elements (i.e., out-of-phase autocorrelation coefficients of X) on the RHS of (9) above and set it to zero. This coincides with (6) of Theorem 3, completing the proof of part 2). Part 3) is immediate from Theorem 12. □

Adapting the proof of Theorem 15, we can now easily characterize almost two valued CASACs with similar parameters along the same vein.

Theorem 16: 1) Almost two-valued CASAC sequences $X = 1 + \alpha D + \beta(G - D - 1)$ with $\beta = \bar{\alpha}$ exists in an abelian group G of order v if and only if $v \equiv 1 \pmod 4$ and D is a partial difference set in G with Paley type parameters $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$, and hence v is a prime power and $v \equiv 1 \pmod 4$, or $v = n^4$ or $9n^4$, with $n > 1$ an odd positive integer.

2) The only permissible values of α are those given in Theorem 4.

3) Furthermore, if G is cyclic, then v must be a prime (call it p) and D must be the classical Paley PDS (consisting of quadratic residues mod p), whence our almost two-valued CASAC sequences X must be precisely Björck's original sequences characterized in Theorem 4.

Proof: Identical to Proof of Theorem 15 – the only difference coming in adapting the proofs of parts 2) and 3) toward finding the two feasible values of α when we require the out-of-phase autocorrelation values take on the constant ϵ. □

IV. Numerical Measures of Performance for Sequence Sets

A. The Golay Merit Factor

Here we examine the Golay Merit Factors for the Björck-like sequences. We note that asymptotically they appear to reach a $GMF \approx 6$ which is not surprising as the sequences are similar in structure to the Paley sequence type. Figure 1 does indicate that larger GMFs may favor smaller ϵ values.

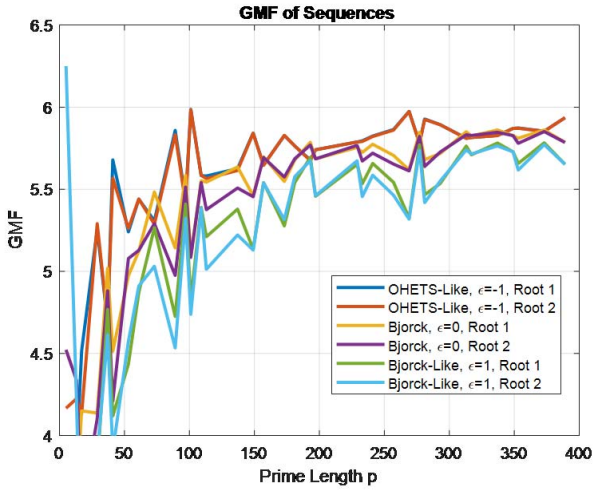

Fig. 1. Golay Merit Factors of the Björck-like sequences by choice of ϵ.

B. The Cross Merit Factor

In the effort to find optimal sets of sequences for use, for example in MIMO radar, we propose a measure derived from the Golay Merit Factor which is commonly used to measure the performance of a single sequence. The measure we call Cross Merit Factor, XMF, satisfies the following:

1) Gives a numerical measure of performance for any number of sequences, $N > 0$, each of length $L > 0$.
2) Reduces to the common Golay Merit Factor when $N = 1$.
3) Returns a set of N sequence shifts, one per input sequence, to indicate the optimal set.
4) The optimal set will be a set of sequences providing maximal GMFs and minimal cross-correlation values.

The proposed measure is defined using the aperiodic cross-correlation between any two sequences in the set. We define the aperiodic cross-correlation between two sequences, S_1 and S_2, to be

$$X(S_1, S_2, t) = \sum_{i=0}^{L-t-1} S_1(i)S_2^*(i+t) \; for \; t = 0, 1, \ldots, L-1.$$

The set of equal length sequences, which are the input to the XMF, is represented by

$$\Gamma = \begin{bmatrix} S_1(0) & S_1(1) & \cdots & S_1(L-1) \\ \vdots & & & \vdots \\ S_N(0) & S_N(1) & \cdots & S_N(L-1) \end{bmatrix}.$$

A computer algorithm, developed in MATLAB, examines all possible cyclic shifts of the sequences in Γ, denoted by the integers $\phi(\Gamma) = \{\phi_1, \phi_2, \cdots, \phi_N\}$. The output of the code is the set of best possible shifts which maximize $XMF(\Gamma)$.

Note that in the case of a single sequence, $N = 1$, of length L, then

$$\Gamma = \begin{bmatrix} S_1(0) & S_1(1) & \cdots & S_1(L-1) \end{bmatrix}$$

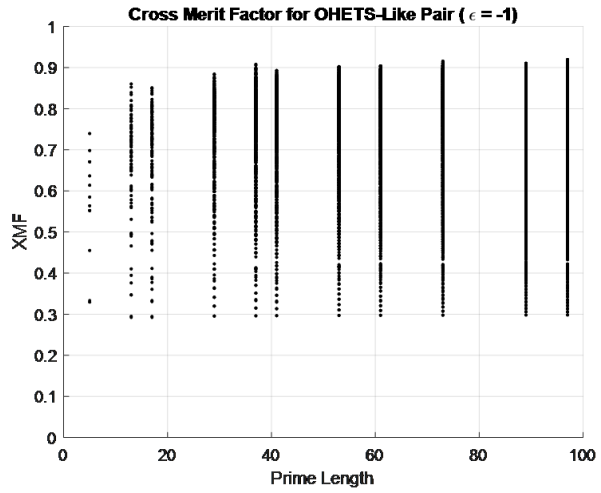

Fig. 2. Cross Merit Factors of all shifts of the Björck-like sequences for $\epsilon = -1$.

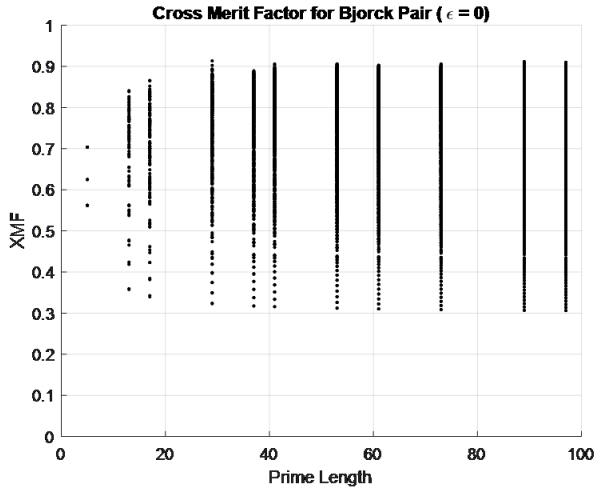

Fig. 3. Cross Merit Factors of all shifts of the Björck-like sequences for $\epsilon = 0$.

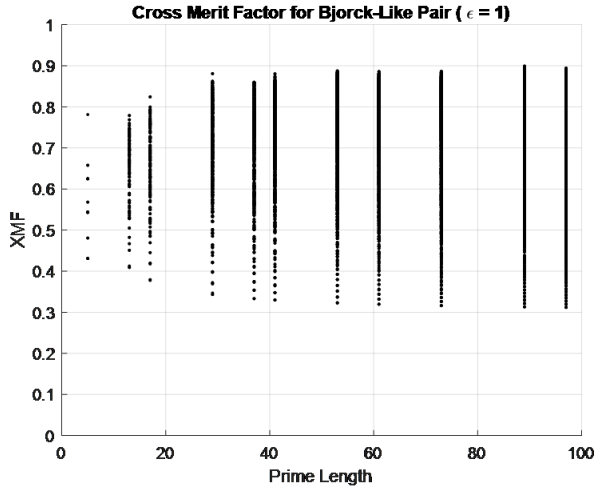

Fig. 4. Cross Merit Factors of all shifts of the Björck-like sequences for $\epsilon = 1$.

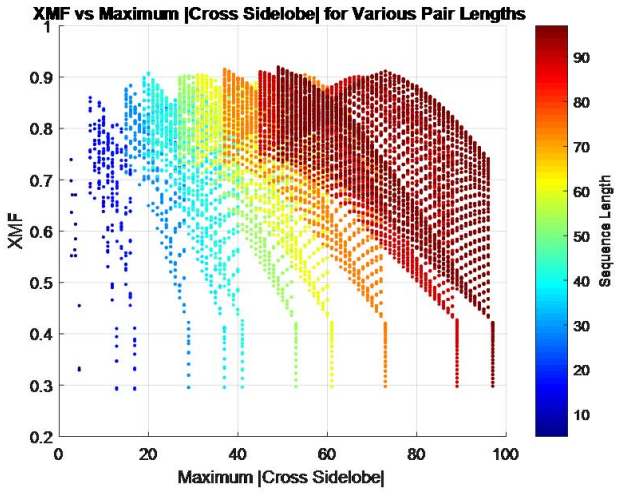

Fig. 5. Cross Merit Factors plotted versus the maximum sidelobe value.

and the XMF collapses down to the GMF. We skip the proof of this assertion.

We now discuss a few numerical testings we performed on Cross Merit Factor. First we attempt to show that optimizing the XMF is a reasonable and possible action for a set of sequences. For the Björck-like sequences we compute all possible XMF for $\epsilon \in \{-1, 0, 1\}$ to examine the distribution of values (to visually see if optimization is reasonable). The next three Figures, Figures 2, 3, and 4, show that a wide variety of XMF exist implying that an optimal set of sequences can be found.

Further evidence suggests that our algorithm's maximizing of the XMF is also able to minimize the magnitude of the side lobes of the sequence set. Based on the numerical evidence in Figure 5, we can see that for a fixed sequence length the maximal XMF tends to occur alongside the minimal maximum sidelobe magnitudes.

C. Testing of the Phase Angle Bandwidth

By computing the phase angle of α for various Björck-like sequences, we show numerically that the optimum (minimal) bandwidth is achieved when ϵ is largest. In this case, restricting our ϵ in $[-1, 1]$, the best bandwidth is given when $\epsilon = 1$.

Definition 8: The Cross Merit Factor for a set of N sequences of length L, represented by Γ, is given by

$$XMF(\Gamma) = \frac{\sum_{i=1}^{N} |X(S_i, S_i, 0)|^2}{2\left(\sum_{i=1}^{N}\sum_{j=1, i\neq j}^{N}\sum_{t=0}^{L-1} |X(S_i, S_j, t)|^2 + \sum_{i=1}^{N}\sum_{j=1, i\neq j}^{N}\sum_{t=0}^{L-1} |X(S_j, S_i, t)|^2 + \sum_{i=1}^{N}\sum_{t=1}^{L-1} |X(S_i, S_i, t)|^2\right)}$$

the goal of which is to find the maximal XMF.

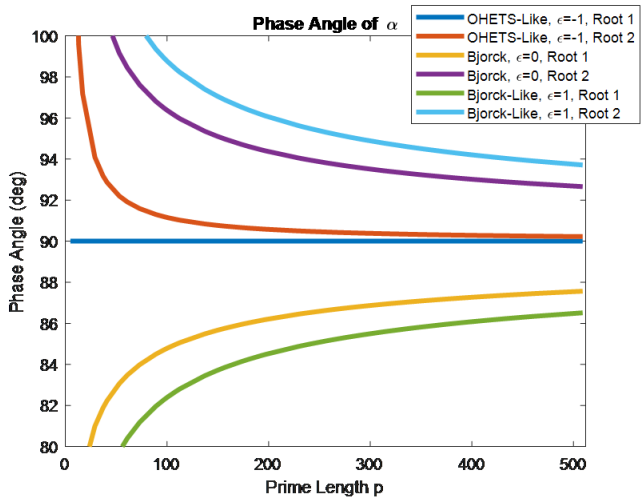

Fig. 6. Phase Angle of the Björck-like sequences by choice of ϵ.

See Figure 6 as evidence of this by looking at the top (light blue) and bottom (dark green) curves which are associated with $\epsilon = 1$ and are furthest from 90 degrees.

V. Conclusion

In this paper, we have studied unimodular sequences with constant but small (preferably zero) out-of-phase autocorrelations. These so-called CAZAC or CASAC sequences that arise via a construction of Björck have been characterized for the two-valued and almost two-valued (i.e., two-valued except for the first position which uses a third value) cases. The latter is not fully solved as we could only tackle the case where the two values used are complex conjugates. We leave the general problem as an open question: i.e Obtain a similar characterization as Theorems 15 and 16, without assuming the hypothesis $\beta = \bar{\alpha}$.

We also obtain a one-parameter infinite family of CASAC which may have applications in MIMO applications. Toward this, we introduce a performance measure we term as cross merit factor (XMF) to study cross correlation behavior, generalizing the celebrated notion of Golay Merit Factor (GMF). The newly introduced notion XMF is still at its infancy. We leave further investigation of the proposed XMF metric to future work, where we will develop a full fledged theory akin to GMF. This will be useful in various applications such as MIMO.

Acknowledgment

The authors would like to thank an editor and an anonymous referees for their thoughtful suggestions to improve its presentation. They are also cognizant and grateful for their patience.

References

[1] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[2] J. J. Benedetto, K. Cordwell, and M. Magsino, "CAZAC sequences and Haagerup's characterization of cyclic N-roots," in *New Trends in Applied Harmonic Analysis*, vol. 2. Cham, Switzerland: Springer, 2019, pp. 1–43.

[3] M. Magsino, "Constant amplitude zero autocorrelation sequences and single pixel imaging," Ph.D. dissertation, Dept. Math., Univ. Maryland, College Park, MD, USA, 2018.

[4] I. Arriaga-Trejo, J. Flores-Troncoso, J. Villanueva, and J. Simón, "Design of unimodular sequences with real periodic correlation and complementary correlation," *Electron. Lett.*, vol. 52, no. 4, pp. 319–321, 2016.

[5] I. A. Arriaga-Trejo, A. G. Orozco-Lugo, A. Veloz-Guerrero, and M. E. Guzman, "Widely linear system estimation using superimposed training," *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5651–5657, Nov. 2011.

[6] S. Hu, Q. Luo, F. Li, Z. Liu, Y. Gao, and J. Wu, "Practical implementation of multi-user transform domain communication system for control channels in cloud-based cognitive radio networks," *IEEE Access*, vol. 6, pp. 17010–17021, 2018.

[7] Z. Li, P. Li, X. Hao, and X. Yan, "Optimal unimodular sequences design method for active sensing systems," *Math. Problems Eng.*, vol. 2018, pp. 1–13, 2018.

[8] R. J. Turyn, "Sequences with small correlation, error correcting codes," in *Proc. Symp. Conducted Math. Res. Center*, Madison, WI, USA, 1968, pp. 195–228.

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

[10] D. Chu, "Polyphase codes with good periodic correlation properties (Corresp.)," *IEEE Trans. Inf. Theory*, vol. IT-18, no. 4, pp. 531–532, Jul. 1972.

[11] F. F. Kretschmer and K. Gerlach, "Low sidelobe radar waveforms derived from orthogonal matrices," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 27, no. 1, pp. 92–102, Jan. 1991.

[12] N. Wiener, "Generalized harmonic analysis," *Acta Math.*, vol. 55, no. 1, pp. 117–258, Dec. 1930.

[13] B. M. Popovic, "Generalized chirp-like polyphase sequences with optimum correlation properties," *IEEE Trans. Inf. Theory*, vol. 38, no. 4, pp. 1406–1409, Jul. 1992.

[14] Z. Shen, A. Papasakellariou, J. Montojo, D. Gerstenberger, and F. Xu, "Overview of 3GPP LTE-advanced carrier aggregation for 4G wireless communications," *IEEE Commun. Mag.*, vol. 50, no. 2, pp. 122–130, Feb. 2012.

[15] K. Wesolowski, A. Langowski, and K. Bakowski, "A novel pilot scheme for 5G downlink transmission," in *Proc. Int. Symp. Wireless Commun. Syst. (ISWCS)*, Aug. 2015, pp. 161–165.

[16] L. Li, M. Bi, W. Jia, X. Miao, and W. Hu, "Improvement of optical modulation depth tolerance in analog RoF by employing CAZAC and nonlinearity compensation," in *Proc. Opto-Electronics Commun. Conf. (OECC) Photon. Global Conf. (PGC)*, Jul. 2017, pp. 1–3.

[17] J. J. Benedetto, R. L. Benedetto, and J. T. Woodworth, "Optimal ambiguity functions and Weil's exponential sum bound," *J. Fourier Anal. Appl.*, vol. 18, no. 3, pp. 471–487, Jun. 2012.

[18] J. J. Benedetto, I. Konstantinidis, and M. Rangaswamy, "Phase-coded waveforms and their design," *IEEE Signal Process. Mag.*, vol. 26, no. 1, pp. 22–31, Jan. 2009.

[19] G. Björck, "Functions of modulus 1 on $\mathbb{Z}_n$ whose Fourier transforms have constant modulus, and 'CYCLIC n-ROOTS"' in *Recent Advances in Fourier Analysis and Its Applications*. Dordrecht, The Netherlands: Kluwer, 1990, pp. 131–140.

[20] B. Saffari, "Some polynomial extremal problems which emerged in the twentieth century," in *20th Century Harmonic Analysis—A Celebration*. Dordrecht, The Netherlands: Springer, 2001, pp. 201–233.

[21] G. Björck and B. Saffari, "New classes of finite unimodular sequences with unimodular Fourier transforms. Circulant Hadamard matrices with complex entries," *Comp. Rendus l'Académie des Sci. Mathématique*, vol. 320, no. 3, pp. 319–324, 1995.

[22] K. T. Arasu, *Sequences and Arrays With Desirable Correlation Properties* (NATO Science for Peace and Security Series—D: Information and Communication Security), vol. 29. Jan. 2011, pp. 136–171.

[23] S. L. Ma, "Partial difference sets," *Discrete Math.*, vol. 52, no. 1, pp. 75–89, 1984.

[24] K.-U. Schmidt, "Sequences with small correlation," *Des., Codes Cryptogr.*, vol. 78, no. 1, pp. 237–267, 2016.

[25] R. E. A. C. Paley, "On orthogonal matrices," *J. Math. Phys.*, vol. 12, pp. 311–320, Apr. 1933.

[26] S. De Winter, E. Kamischke, and Z. Wang, "Automorphisms of strongly regular graphs with applications to partial difference sets," *Des., Codes Cryptogr.*, vol. 79, no. 3, pp. 471–485, Jun. 2016.

[27] S. De Winter, E. Neubert, and Z. Wang, "Non-existence of two types of partial difference sets," *Discrete Math.*, vol. 340, no. 9, pp. 2130–2133, Sep. 2017.
[28] S. De Winter and Z. Wang, "Classification of partial difference sets in Abelian groups of order $4p^2$," *Des., Codes Cryptogr.*, vol. 84, no. 3, pp. 451–461, 2017.
[29] S. De Winter and Z. Wang, "Non-existence of partial difference sets in Abelian groups of order $8p^3$," *Des., Codes Cryptogr.*, vol. 87, no. 4, pp. 757–768, Apr. 2019.
[30] J. Polhill, "A new family of partial difference sets in 3-groups," *Des., Codes Cryptogr.*, vol. 87, no. 7, pp. 1639–1646, Jul. 2019.
[31] J. Polhill, "Paley partial difference sets in groups of order n^4 and $9n^4$ for any odd $n > 1$," *J. Combinat. Theory A*, vol. 117, no. 8, pp. 1027–1036, 2010.
[32] Z. Wang, "New necessary conditions on (negative) Latin square type partial difference sets in abelian groups," *J. Combinat. Theory A*, vol. 172, pp. 105–208, May 2020.
[33] Z. Wang, "Paley type partial difference sets in abelian groups," *J. Combinat. Des.*, vol. 28, no. 2, pp. 149–152, Feb. 2020.
[34] K. Arasu, D. Jungnickel, S. L. Ma, and A. Pott, "Strongly regular Cayley graphs with $\lambda - \mu = -1$," *J. Combinat. Theory A*, vol. 67, no. 1, pp. 116–125, 1994.

K. T. Arasu (Member, IEEE) received the B.S. and M.S. degrees in mathematics from Panjab University, India, and the Ph.D. degree from The Ohio State University. He is currently a Senior Research Scientist at the Riverside Research's Secure and Resilient Systems Group. Prior to joining Riverside Research, he was a Professor with the Department of Mathematics and Statistics, Wright State University, for 35 years. He investigates novel techniques on error correcting codes, cryptography, data security and privacy, as well as topics at the intersection of machine learning, security, and information theory. He has published over 110 research papers. During his time as a Professor at Wright State University, he was presented the Teaching Excellence Award from the College of Science and Mathematics, the Presidential Research Excellence Award, and the Trustee's Award for Faculty Excellence. He serves on the editorial board of several technical international journal publications.

Michael R. Clark (Member, IEEE) received the B.S. degree in computer science from Brigham Young University, the M.S. degree in computer science from The University of Utah, and the Ph.D. degree in computer science from the Air Force Institute of Technology. He is currently the Associate Director at the Riverside Research's Secure and Resilient Systems Group. He has experience in software development, software testing, vulnerability analysis, reverse engineering, cryptanalysis, and cybersecurity education and training. He conducts research in the areas concerning security of distributed and cyber-physical systems and cryptographic secure computation, communications systems, and using modeling and simulation to understand system security.

Jeffrey R. Hollon received the B.S. and M.S. degrees in mathematics and the Ph.D. degree in interdisciplinary applied science and mathematics from Wright State University in 2018, under his advisor of Dr. K. T. Arasu. After graduating in 2010, he taught at the Sinclair Community College before going back for his Ph.D. studies. He is currently a Machine Learning Engineer at Radiance Technologies. Before joining Radiance Technologies, he was a Senior Applied Mathematician at Applied Optimization, Inc., where he led research and development on many statistical techniques for automating and detecting real-time changes in space objects utilizing a combination of non-resolved photometry and radar. He applies statistical and machine learning techniques to problems relating to space domain awareness that enable confident characterization and automated change detection capabilities for U.S. Warfighter. He has several publications spanning subjects from combinatorial designs, radar processing, machine learning, and space domain awareness.