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

K. T. Arasu, Riverside Research, Beavercreek, Ohio
(karasu@RiversideResearch.org)

Joint work with

Michael Clark, Riverside Research, Beavercreek, Ohio

and

Jeff Hollon, Applied Optimization, Fairborn, Ohio

CAZAC sequences - Introduction

RIVERSIDE RESEARCH

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) systems, radar, signal processing and code design.

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 – origins and uses

- The study of CAZAC property originates 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, P4, and Wiener sequences are three classes of sequences that are indeed CAZAC.
- They belong to a class of sequences known as chirp sequences.
- CAZAC sequences are used in 4G LTE (Long Term Evolution) wireless standard [4] and in the development of 5G wireless communication technology [5], [6].
- CAZAC sequences are important in waveform design because of their optimal transmission efficiency and tight time localization properties.
- There is an extensive literature on CAZACs because of the importance of such sequences in communications, coding theory, cryptology, and radar (see Benedetto et al. [2], [7] and references therein).

CAZAC sequences – our investigations

RIVERSIDE RESEARCH

- 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.
- For more details on the original Björck construction see [8], [9], [10].

GROUP RINGS

RIVERSIDE RESEARCH

- Let G be a multiplicatively written abelian group of order *v*. Let Z[G] denote the group ring of G over the ring Z of integers.

- A subset S of G is identified with the group ring element which is a formal sum of the elements of S (i.e. with coefficients 0 and 1); and for an element A of Z[G] and integer t, $A^{(t)}$ denotes the image of A under the group homomorphism *x* to x^t, extended linearly to all of Z[G].

Bjorck sequences - characterization

Theorem 1.

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

with |α|= 1 be the Björck sequence with the sets S and N representing the square and non-square entries of GF(q), where q ≡ 1 (mod 4). Then only the following constants α

$$\left\{ \frac{1}{\sqrt{q}+1} \pm \sqrt{\frac{1}{\left(\sqrt{q}+1\right)^2} - 1}\,, \qquad \frac{-1}{\sqrt{q}-1} \pm \sqrt{\frac{1}{\left(\sqrt{q}-1\right)^2} - 1} \right\}.$$

will provide perfect periodic auto-correlations for the sequence B. That is, BB^(−1) = q

Bjorck sequences – our results

RIVERSIDE RESEARCH

Remarks:

- (i) we show that Björck's theme for primes p with $p \equiv 1 \pmod 4$ would work for only two sets of parameters η
- (ii) Björck's theme for primes p with $p \equiv 1 \pmod 4$; 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 [11].
- (iii) Our analysis provides a second value for α

Björck-like Sequences with Constant Periodic Auto-Correlations

RIVERSIDE RESEARCH

- We next examine more closely the Bjorck-Like sequence defined by $B = 1 + \alpha S + \bar{\alpha} N$ where its periodic auto-correlation is given by $BB^{(-1)} = q + \epsilon(G - 1)$
- **Theorem 2.** 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

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

Restrictions on the Length q and Parameter for Björck-like Sequences

- **Theorem 3.** For a Björck-like sequence to exist with length q, with $q \equiv 1 \pmod 4$, and correlation parameter , the following four conditions are necessary and sufficient as a whole:
- $q \geq \epsilon$
- $q + q\epsilon - \epsilon \geq 0$
- $2 - q \leq \sqrt{q + q\epsilon - \epsilon} \leq q$
- $2 - q \leq -\sqrt{q + q\epsilon - \epsilon} \leq q$

When $|\epsilon| \leq 1$, all four conditions are valid.

The Case of Björck-like Sequences of Length $q \equiv 3 \pmod 4$

RIVERSIDE RESEARCH

- we look at the case of the Björck-like sequence but for lengths $q \equiv 3 \pmod 4$. We first examine $B = 1 + \alpha S + \bar{\alpha} N$ followed by the case of $B = i + \alpha S + \bar{\alpha} N$.
- **Theorem 4**. For length $q \equiv 3 \pmod 4$, the only Björck-like sequence, $B = 1 + \alpha S + \bar{\alpha} N$, with constant periodic auto-correlation is when $\alpha = \pm 1$.
- **Theorem 5.** For length $q \equiv 3 \pmod 4$, the only Björck-like sequence, $B = i + \alpha S + \bar{\alpha} N$, with constant periodic auto-correlation is when $\alpha = \pm 1$.

A New Björck-like Vari-Angular Sequence of Length $q \equiv 1 \pmod 4$

- 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 show that the parameter θ is free to vary but can be optimized to minimize the value of the correlations.
- **Theorem 6**. The three-valued unimodular sequence $B = e^{i\theta} + \alpha S + N$ of length $q \equiv 1 \pmod 4$ has constant periodic auto-correlations when $\alpha = 1$ or $e^{2i\theta}$.
- **Remarks**: What auto-correlation values this sequence achieves? :

$2\cos(\theta) + (q-1)/2 * \cos(2\theta) + (q-3)/2$ whose min value is $-q/(q-1)$ when $\cos(\theta) = -1/(q-1)$.

Remark: In Theorem 6 (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 introduce a new performance measure we term as cross merit factor which reduces to the classical GMF when a single sequence is employed. (we skip details in the interest of time).

Saffari's theme

RIVERSIDE RESEARCH

- Clever analysis of Saffari [9] fully settles the general parameter characterization of two-valued CAZAC sequences.
- We state it as a theorem:
- **Theorem 7.** (Saffari [9]) Two-valued CAZACs 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.
- **Remarks:** It follows that two-valued CAZACs cannot exist for lengths $N \equiv 1 \pmod 4$.
- In this case, Björck CAZAC sequences are almost two-valued.

Extending Saffari's theme

RIVERSIDE RESEARCH

- 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 $\beta = \overline{\alpha}$, we are able to provide a very satisfactory solution which, in spirit, resembles the aforementioned celebrated result of Saffari (Theorem 7 above).

Ingredients from theory of partial difference sets

We require some ingredients from the theory of PDS. PDS in abelian groups G have been thoroughly studied; see [14] for a survey of older results and [17], [18], [19], [20], [21], [22], [23], [24] (and references therein) for a number of very recent results.

Almost two-valued CAZACs fully characterized

RIVERSIDE RESEARCH

Theorem 8

- 1) Almost two valued CAZACs $X = 1 + \alpha D + \beta(G - D - 1)$ 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 $(v, (v-1)/2, (v-5)/4, (v-1)4)$, 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 1.
- 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 1.

Almost two-valued CASACs fully characterized

RIVERSIDE RESEARCH

- Adapting the proof of Theorem 8, we can now easily characterize almost two valued CASACs with similar parameters along the same vein.

Theorem 9.

- 1) Almost two-valued CASACs $X = 1 + \alpha D + \beta(G - D - 1)$ with $\beta = \alpha$ 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 $(v, (v-1)/2, (v-5)/4, (v-1)/4)$, 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 2.
- 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 2.

References

- [1] S. W. Golomb and G. Gong, Signal design for good correlation: for wireless communication, cryptography, and radar. Cambridge University 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, Volume 2. Springer, 2019, pp. 1–43.
- [3] M. Magsino, “Constant amplitude zero autocorrelation sequences and single pixel imaging,” Ph.D. dissertation, University of Maryland, College Park, 2018.
- [4] Z. Shen, A. Papasakellariou, J. Montojo, D. Gerstenberger, and F. Xu, “Overview of 3gpp lte-advanced carrier aggregation for 4g wireless communications,” IEEE Communications Magazine, vol. 50, no. 2, pp. 122–130, 2012.
- [5] K. Wesołowski, A. Langowski, and K. B ˛akowski, “A novel pilot scheme for 5g downlink transmission,” in 2015 International Symposium on Wireless Communication Systems (ISWCS). IEEE, 2015, pp. 161–165.
- [6] 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 2017 Opto-Electronics and Communications Conference (OECC) and Photonics Global Conference (PGC). IEEE, 2017, pp. 1–3.
- [7] J. J. Benedetto, R. L. Benedetto, and J. T. Woodworth, “Optimal ambiguity functions and weil’s exponential sum bound,” Journal of Fourier Analysis and Applications, vol. 18, no. 3, pp. 471–487, Jun 2012.
- [8] G. Björck, “Functions of modulus 1 on Zn whose fourier transforms have constant modulus, and “cyclic n-roots”,” in Recent Advances in Fourier Analysis and its Applications. Springer, 1990, pp. 131–140.
- [9] B. Saffari, “Some polynomial extremal problems which emerged in the twentieth century,” in Twentieth Century Harmonic AnalysisâA˘TA Celebration ˇ . Springer, 2001, pp. 201–233.
- [10] G. Björck and B. Saffari, “New classes of finite unimodular sequences with unimodular fourier transforms. circulant hadamard matrices with complex entries,” Comptes rendus de l’Académie des sciences. Série 1, Mathématique, vol. 320, no. 3, pp. 319–324, 1995.
- [11] K. T. Arasu, “Sequences and arrays with desirable correlation properties,” NATO Science for Peace and Security Series - D: Information and Communication Security, vol. 29, pp. 136 – 171, January 2011.
- [12] K.-U. Schmidt, “Sequences with small correlation,” Designs, Codes and Cryptography, vol. 78, no. 1, pp. 237–267, 2016.

References

- [13] J. J. Benedetto, I. Konstantinidis, and M. Rangaswamy, "Phase-coded waveforms and their design," IEEE Signal Processing Magazine, vol. 26, no. 1, pp. 22–31, 2009.
- [14] S. L. Ma, "Partial difference sets," Discrete Mathematics, vol. 52, no. 1, pp. 75–89, 1984.
- [15] R. E. A. C. Paley, "On orthogonal matrices," J. Math. Phys., vol. 12, pp. 311 – 320, 1933.
- [16] E. M. Gabidulin and V. V. Shorin, "New sequences with zero autocorrelation," Problems of Information Transmission, vol. 38, no. 4, pp. 255–267, 2002.
- [17] S. De Winter, E. Kamischke, and Z. Wang, "Automorphisms of strongly regular graphs with applications to partial difference sets," Designs, Codes and Cryptography, vol. 79, no. 3, pp. 471–485, 2016.
- [18] S. De Winter, E. Neubert, and Z. Wang, "Non-existence of two types of partial difference sets," Discrete Mathematics, vol. 340, no. 9, pp. 2130–2133, 2017.
- [19] S. De Winter and Z. Wang, "Classification of partial difference sets in abelian groups of order 4p 2 ," Designs, Codes and Cryptography, vol. 84, no. 3, pp. 451–461, 2017.
- [20] ——, "Non-existence of partial difference sets in abelian groups of order 8p 3 ," Designs, Codes and Cryptography, vol. 87, no. 4, pp. 757–768, 2019.
- [21] J. Polhill, "A new family of partial difference sets in 3-groups," Designs, Codes and Cryptography, vol. 87, no. 7, pp. 1639–1646, 2019.
- [22] ——, "Paley partial difference sets in groups of order n 4 and 9n 4 for any odd n > 1," Journal of Combinatorial Theory, Series A, vol. 117, no. 8, pp. 1027–1036, 2010.
- [23] Z. Wang, "New necessary conditions on (negative) latin square type partial difference sets in abelian groups," Journal of Combinatorial Theory, Series A, vol. 172, pp. 105–208, 2020.
- [24] ——, "Paley type partial difference sets in abelian groups," Journal of Combinatorial Designs, vol. 28, no. 2, pp. 149–152, 2020.
- [25] K. Arasu, D. Jungnickel, S. L. Ma, and A. Pott, "Strongly regular cayley graphs with $\lambda - \mu = -1$," Journal of Combinatorial Theory, Series A, vol. 67, no. 1, pp. 116–125, 1994