On Constant Amplitude Zero Autocorrelation Sequences of length p

{Katherine Cordwell*, Mark Magsino**} The Norbert Wiener Center
**Daniel Sweet Research Undergraduate Fellow; **Doctoral Candidate

Introduction

Define a function $u : \mathbb{Z}_n \to \mathbb{C}$.
We define the inner product

$$\langle u(k), u(m) \rangle = u(k)\overline{u(m)}.$$

We say that u is **unimodular** if

$$\langle u(k), u(k) \rangle^{1/2} = 1.$$

We define the **autocorrelation** $A_u(m)$ of u for $m \in \mathbb{Z}_n$ as

$$A_u(m) = \frac{1}{n}\sum_{k=0}^{n-1}\langle u(m+k), u(k) \rangle.$$

We say that u is a **CAZAC (Constant Amplitude Zero Autocorrelation) sequence** of length d if it is unimodular and if it satisfies $A_u(m) = 0$ for all $m \in \mathbb{Z}_n \setminus \{0\}$. CAZAC sequences are defined to be **equivalent** under rotation, translation, decimation, linear frequency modulation, and conjugation.

Example

Define $u : \mathbb{Z}_3 \to \mathbb{C}$ by $u(0) = -e^{ib+\pi i/3}$, $u(1) = e^{ib}$, $u(2) = e^{ib}$. For short, we denote this as

$$u = e^{ib}(-e^{\pi i/3}, 1, 1).$$

We see immediately that u is unimodular, since multiplying e^j by its complex conjugate gives 1 for any j.
To check that u has zero autocorrelation, we compute: $A_u(1) = \frac{1}{3}(\langle u(1), u(0) \rangle + \langle u(2), u(1) \rangle + \langle u(0), u(2) \rangle) = \frac{1}{3}(-e^{-\pi i/3} + 1 - e^{\pi i/3}) = 0$.
Also, $A_u(2) = \frac{1}{3}(\langle u(2), u(0) \rangle + \langle u(0), u(1) \rangle + \langle u(1), u(2) \rangle) = A_u(1) = 0$.
Thus u has zero autocorrelation and is a CAZAC sequence.

Hadamard Matrices

As defined in Benedetto and Datta, a complex Hadamard matrix is a square matrix with unimodular entries and mutually orthogonal rows. Benedetto and Datta further showed there is a 1-1 correspondence between CAZAC sequences and circulant Hadamard matrices.

Previous Results

Using the characterization of 3×3 Hadamard matrices as documented by Bruzda, Tadej, and Życzkowski, we have that all 3×3 complex Hadamard matrices are equivalent to

$$F_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix},$$

where $\omega = e^{2\pi i/3}$ and **equivalent** means that they can be written as $D_1 P_1 F_3 P_2 D_2$ where P_1 and P_2 are permutation matrices and D_1 and D_2 are diagonal unitary matrices.
For 5×5 matrices, using some results by Haagerup, all 5×5 Hadamard matrices are equivalent to

$$F_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega & \omega^3 \\ 1 & \omega^3 & \omega & \omega^4 & \omega^2 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix},$$

where $\omega = e^{2\pi \cdot i/5}$.
Classifying $n \times n$ Hadamard matrices for arbitrary n is an open problem. The catalogue maintained by Bruzda et al. only contains entries for $n \leq 16$. According to Bengtsson, this problem has been open for about 100 years, but only a few facts are known about arbitrary Hadamard matrices; for example, that the Fourier matrix exists for all n.

Previous Results, Ctd.

Letting

$$A = \begin{pmatrix} e^{ia} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{ic} \end{pmatrix}$$

and

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{ix} & 0 \\ 0 & 0 & e^{iy} \end{pmatrix},$$

and

$$F_3' = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \end{pmatrix},$$

where $a, b, c, x, y \in [0, 2\pi)$ and $\omega = \frac{2\pi i}{3}$, Bruzda, Tadej, and Życzkowski further claim that the set of 3×3 Hadamard matrices is

$$\{A \cdot F_3 \cdot B\} \cup \{A \cdot F_3' \cdot B\}.$$

Results

Using the first form in the characterization of 3×3 Hadamard matrices by Bruzda et al., and imposing conditions to make the matrix circulant, we obtain the following equations, all $\mod 2\pi$:

$$a = \tfrac{2\pi}{3} + b + x = \tfrac{2\pi}{3} + c + y$$
$$c = (a + x) = \tfrac{4\pi}{3} + b + y$$
$$a + y = b = \tfrac{4\pi}{3} + c + x$$

We simplify this further to the following equations (still mod 2π),

$$a = \tfrac{2\pi}{3} + b + x$$
$$c = \tfrac{2\pi}{3} + b + 2x$$
$$y = \tfrac{4\pi}{3} + c + x - a = \tfrac{4\pi}{3} + (\tfrac{2\pi}{3} + b + 2x) + x - (\tfrac{2\pi}{3} + b + x) = 4/3\pi + 2x$$
$$b = c + y - x = (\tfrac{2\pi}{3} + b + 2x) + (\tfrac{4\pi}{3} + 2x) - x = 2\pi + b + 3x.$$

Results, Ctd.

To solve this system of equations, we need that $3x = 0 \mod 2\pi$, which means that x is $2\pi/3$. So, overall, we get x is $2\pi/3$, b is indeterminate, $a = 4/3\pi + b$, $c = b$, and $y = 2\pi/3$. Then, taking the matrix product, we get a matrix with first row $e^{ib}(-(-1)^{1/3}, 1, 1)$. The cube roots of -1 are -1, $e^{\pi \cdot i/3}$, and $e^{-\pi \cdot i/3}$, so we have three possible CAZACs.
Working with the second form in the characterization of 3×3 Hadamard matrices similarly, we get the following system of equations:

$$a = \tfrac{4\pi}{3} + b + x = \tfrac{4\pi}{3} + c + y$$
$$c = (a + x) = \tfrac{2\pi}{3} + b + y$$
$$a + y = b = \tfrac{2\pi}{3} + c + x$$

Solving, we get that x is $\frac{2}{3}\pi$, b is arbitrary, $a = b$, $c = 2/3\pi + b$, $y = 1$. The first row of this circulant Hadamard matrix is $e^{ib}(1, (-1)^{2/3}, 1)$, which also gives three possible CAZACs.
In total, we obtain the following four CAZACs: $e^{ib}(-e^{\pi i/3}, 1, 1)$
$e^{ib}(e^{\pi i/3} - 1, 1, 1)$
$e^{ib}(1, e^{2\pi i/3}, 1)$
$e^{ib}(1, (e^{\pi i/3} - 1)^2, 1)$.

Discussion

Surprisingly, two of the first rows of the matrices were not CAZACs. One would also expect there to be 6 CAZACs of length 3, based on work by Haagerup.
A similar approach makes sense to find length 5 CAZACs. Bruzda et al. do not have a special simplified characterization for 5×5 Hadamard matrices, so the work is slightly more difficult.
It should be noted that in general, it is not known how many CAZACs of length p there are for arbitrary p, although Haagerup showed that $\binom{2p-2}{p-1}$ is an upper bound on this number, and thus it is finite.