Constant Amplitude and Zero Autocorrelation Sequences and Single Pixel Camera Imaging

Mark Magsino
mmagsino@math.umd.edu

Norbert Wiener Center for Harmonic Analysis and Applications
Department of Mathematics
University of Maryland, College Park

April 4, 2018

Frames

A *finite frame* for $\mathbb{C}^N$ is a set $\mathcal{F} = \{v_j\}_{j=1}^M$ such that there exists constants $0 < A \leq B < \infty$ where

$$A\|x\|_2^2 \leq \sum_{j=1}^{M} |\langle x, v_j \rangle|^2 \leq B\|x\|_2^2$$

for any $x \in \mathbb{C}^N$. $\mathcal{F}$ is called a *tight frame* if $A = B$ is possible.

Theorem

$\mathcal{F}$ is a frame for $\mathbb{C}^N$ if and only if $\mathcal{F}$ spans $\mathbb{C}^N$.

The Frame Operator

Let $\mathcal{F} = \{v_j\}_{j=1}^{M}$ be a frame for $\mathbb{C}^N$ and $x \in \mathbb{C}^N$.

(a) The *frame operator*, $S : \mathbb{C}^N \to \mathbb{C}^N$, is given by

$$S(x) = \sum_{j=1}^{M} \langle v_j, x \rangle v_j.$$

(b) Given any $x \in \mathbb{C}^N$ we can write x in terms of frame elements by

$$x = \sum_{j=1}^{M} \langle x, S^{-1} v_j \rangle v_j.$$

(c) If $\mathcal{F}$ is a tight frame with bound A, then $S = A\, Id_N$.

Norbert Wiener Center for Harmonic Analysis and Applications

Definition

(a) Let $\varphi \in \mathbb{C}^N$ and $\Lambda \subseteq (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})\widehat{}$. The *Gabor system*, (φ, Λ) is defined by

$$(\varphi, \Lambda) = \{e_\ell \tau_k \varphi : (k, \ell) \in \Lambda\}.$$

(b) If (φ, Λ) is a frame for $\mathbb{C}^N$ we call it a Gabor frame.

Time-Frequency Transforms

Definition

Let $\varphi, \psi \in \mathbb{C}^N$.

(a) The *discrete periodic ambiguity function* of φ, $A_p(\varphi)$, is defined by

$$A_p(\varphi)[k,\ell] = \frac{1}{N}\sum_{j=0}^{N-1} \varphi[j+k]\overline{\varphi[j]}e^{-2\pi i j\ell/N} = \frac{1}{N}\langle \tau_{-k}\varphi, e_\ell\varphi\rangle.$$

(b) The *short-time Fourier transform* of φ with window ψ, $V_\psi(\varphi)$, is defined by

$$V_\psi(\varphi)[k,\ell] = \langle \varphi, e_\ell \tau_k \psi\rangle.$$

Full Gabor Frames Are Always Tight

Theorem

Let $\varphi \in \mathbb{C}^N \setminus \{0\}$. *and* $\Lambda = (\mathbb{Z}/N\mathbb{Z}) \times (\widehat{\mathbb{Z}/N\mathbb{Z}})$. *Then,* (φ, Λ) *is always a tight frame with frame bound* $N\|\varphi\|_2^2$.

Janssen's Representation

Definition

Let $\Lambda \subseteq (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})\widehat{}$ be a subgroup. The *adjoint subgroup* of Λ, $\Lambda^\circ \subseteq (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})\widehat{}$, is defined by

$$\Lambda^\circ = \{(m,n) : e_\ell \tau_k e_n \tau_m = e_n \tau_m e_\ell \tau_k, \forall (k,\ell) \in \Lambda\}$$

Theorem

Let Λ be a subgroup of $(\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})\widehat{}$ and $\varphi \in \mathbb{C}^N$. Then, the (φ, Λ) Gabor frame operator has the form

$$S = \frac{|\Lambda|}{N} \sum_{(m,n)\in\Lambda^\circ} \langle \varphi, e_n \tau_m \varphi \rangle e_n \tau_m.$$

Norbert Wiener Center for Harmonic Analysis and Applications

Λ°-sparsity and Tight Frames

Theorem

Let $\varphi \in \mathbb{C}^N \setminus \{0\}$ and let $\Lambda \subseteq (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})\widehat{}$ be a subgroup. (φ, Λ) is a tight frame if and only if

$$\forall (m,n) \in \Lambda^\circ, (m,n) \neq 0, \quad A_p(\varphi)[m,n] = 0.$$

The frame bound is $|\Lambda| A_p(\varphi)[0,0]$.

Proof of Λ°-sparsity Theorem

By Janssen's representation we have

$$S = \frac{|\Lambda|}{N} \sum_{(m,n)\in\Lambda^\circ} \langle e_n \tau_m \varphi, \varphi \rangle e_n \tau_m = \sum_{(m,n)\in\Lambda^\circ} \langle \tau_m \varphi, e_{-n}\varphi \rangle e_n \tau_m$$

$$= |\Lambda| \sum_{(m,n)\in\Lambda^\circ} A_p(\varphi)[-m,-n] e_n\, \tau_m = |\Lambda| \sum_{(m,n)\in\Lambda^\circ} A_p(\varphi)[m,n] e_{-n}\tau_{-m}.$$

If $A_p(\varphi)[m,n] = 0$ for every $(m,n) \in \Lambda^\circ, (m,n) \neq 0$, then S is $|\Lambda| A_p(\varphi)[0,0]$ times the identity. and so (φ, Λ) is a tight frame.

Proof of Λ°-sparsity Theorem (con't)

To show this is a necessary condition, we observe that for S to be tight we need

$$S = |\Lambda| \sum_{(m,n)\in\Lambda^\circ} A_p(\varphi)[m,n] e_n \tau_m = A\, Id$$

which can be rewritten as

$$\sum_{(m,n)\in\Lambda^\circ\setminus\{(0,0)\}} |\Lambda| A_p(\varphi)[m,n] e_n \tau_m + (|\Lambda| A_p(\varphi)[0,0] - A) Id = 0.$$

CAZAC Definition

Let $\varphi \in \mathbb{C}^N$. φ is said to be a *constant amplitude zero autocorrelation (CAZAC) sequence* if

$$\forall j \in (\mathbb{Z}/N\mathbb{Z}), |\varphi_j| = 1 \tag{CA}$$

and

$$\forall k \in (\mathbb{Z}/N\mathbb{Z}), k \neq 0, \frac{1}{N}\sum_{j=0}^{N-1} \varphi_{j+k}\overline{\varphi_j} = 0. \tag{ZAC}$$

Examples

Quadratic Phase Sequences

Let $\varphi \in \mathbb{C}^N$ and suppose for each j, φ_j is of the form $\varphi_j = e^{-\pi i p(j)}$ where p is a quadratic polynomial. The following quadratic polynomials generate CAZAC sequences:

- Chu: $p(j) = j(j-1)$
- P4: $p(j) = j(j-N)$, N is odd
- Odd-length Wiener: $p(j) = sj^2$, $\gcd(s, N) = 1$, N is odd
- Even-length Wiener: $p(j) = sj^2/2$, $\gcd(s, 2N) = 1$, N is even

Norbert Wiener Center for Harmonic Analysis and Applications

Björck Sequences

Let p be prime and $\varphi \in \mathbb{C}^p$ be of the form $\varphi_j = e^{i\theta(j)}$. Then φ will be CAZAC in the following cases:

- If $p \equiv 1 \mod 4$, then,

$$\theta(j) = \left(\frac{j}{p}\right) \arccos\left(\frac{1-p}{1+\sqrt{p}}\right)$$

- If $p \equiv 3 \mod 4$, then,

$$\begin{cases} \arccos\left(\frac{1-p}{1+p}\right), & \text{if } \left(\frac{j}{p}\right) = -1 \\ 0, & \text{otherwise} \end{cases}$$

Norbert Wiener Center for Harmonic Analysis and Applications

Connection to Hadamard Matrices

Theorem

Let $\varphi \in \mathbb{C}^N$ and let H be the circulant matrix given by

$$H = \begin{bmatrix} \text{———} \ \varphi \ \text{———} \\ \text{———} \ \tau_1\varphi \ \text{———} \\ \text{———} \ \tau_2\varphi \ \text{———} \\ \cdots \\ \text{——} \ \tau_{N-1}\varphi \ \text{——} \end{bmatrix}$$

Then, φ is a CAZAC sequence if and only if H is Hadamard. In particular there is a one-to-one correspondence between CAZAC sequences and circulant Hadamard matrices.

Connection to Cyclic N-roots

Definition

$x \in \mathbb{C}^N$ is a cyclic N-root if it satisfies

$$\begin{cases} x_0 + x_1 + \cdots + x_{N-1} = 0 \\ x_0 x_1 + x_1 x_2 + \cdots + x_{N-1} x_0 = 0 \\ \cdots \\ x_0 x_1 x_2 \cdots x_{N-1} = 1 \end{cases}$$

Connection to Cyclic N-roots

Theorem

(a) *If $\varphi \in \mathbb{C}^N$ is a CAZAC sequence then,*

$$\left(\frac{\varphi_1}{\varphi_0}, \frac{\varphi_2}{\varphi_1}, \dots, \frac{\varphi_0}{\varphi_{N-1}}\right)$$

is a cyclic N-root.

(b) *If $x \in \mathbb{C}^N$ is a cyclic N-root then,*

$$\varphi_0 = x_0, \varphi_j = \varphi_{j-1} x_j$$

is a CAZAC sequence.

(c) *There is a one-to-one correspondence between CAZAC sequences which start with 1 and cyclic N-roots.*

5-Operation Equivalence

Proposition

Let $\varphi \in \mathbb{C}^N$ be a CAZAC sequence. Then, the following are also CAZAC sequences:

(a) $\forall c \in \mathbb{C}, |c| = 1,\ c\varphi$

(b) $\forall k \in \mathbb{Z}/N\mathbb{Z},\ \tau_k\varphi$

(c) $\forall \ell \in \widehat{(\mathbb{Z}/N\mathbb{Z})}, e_\ell\varphi$

(d) $\forall m \in \mathbb{Z}/N\mathbb{Z}, gcd(m, N) = 1,\ \pi_m\varphi[j]$

(e) $n = 0, 1,\ c_n\varphi$

The operation π_m is defined by $\pi_m\varphi[j] = \varphi[mj]$ and c_0, c_1 is defined by $c_0\varphi = \varphi$ and $c_1\varphi = \overline{\varphi}$.

Norbert Wiener Center for Harmonic Analysis and Applications

5-Operation Group Action

Let G be the set given by

$$\{(a,b,c,d,f) : a \in \{0,1\}, b,c,d,f \in \mathbb{Z}/p\mathbb{Z}, c \neq 0\}$$

and define the operation $\cdot : G \times G \to G$ by

$$(a,b,c,d,f) \cdot (h,j,k,\ell,m)$$

$$= (a+h, cj+b, ck, \ell + (-1)^h kd, m + (-1)^h (f - jc)).$$

Then, $(G, \cdot)$ is a group of size $2p^3(p-1)$.

Norbert Wiener Center for Harmonic Analysis and Applications

5-Operation Group Action (cont'd)

- To each element $(a, b, c, d, f) \in G$ we associate the operator $\omega_f e_d \pi_c \tau_b c_a$, which form a group under composition, where $\omega = e^{2\pi i/p}$.
- The composition is computed by the operation for $(G, \cdot)$ and obtaining the operator associated with the computed result.
- The group of operators under composition forms a group action for U_p^p, the set of p-length vectors comprised entirely of p-roots of unity.
- There are $p(p-1)$ many CAZACs in U_p^p which start with 1. Adding in any scalar multiples of roots of unity, there are $p^2(p-1)$ many.

Norbert Wiener Center for Harmonic Analysis and Applications

5-Operation Orbits

Theorem

Let p be an odd prime and let $\varphi \in U_p^p$ be the Wiener sequence $\varphi[n] = e^{2\pi i s n^2/p}$, where $s \in \mathbb{Z}/p\mathbb{Z}$. Denote the stabilizer of φ under the group $(G, \cdot)$ as G_φ. If $p \equiv 1 \mod 4$, then $|G_\varphi| = 4p$. If $p \equiv 3 \mod 4$, then $|G_\varphi| = 2p$. In particular, the orbit of φ has size $p^2(p-1)/2$ if $p \equiv 1 \mod 4$ and size $p^2(p-1)$ if $p = 3 \mod 4$.

Norbert Wiener Center for Harmonic Analysis and Applications

Sketch of Proof

- Take a linear operator $\omega_f e_d \pi_c \tau_b c_a$ and write the system of equations that would describe fixing each term of $\varphi[n]$.
- Use the $n = 0, 1$ cases to get expressions for f and d in terms of the other variables.
- Use any other $n > 1$ and substitute the expressions for f and d to obtain the condition

$$c^2 \equiv (-1)^a \mod p.$$

Sketch of Proof (con't)

- In the case $a = 0$, there are always the solutions $c \equiv \pm 1 \mod p$. If $a = 1$, then it depends if -1 is a quadratic residue modulo p. It is if $p \equiv 1 \mod 4$ and is not if $p \equiv 3 \mod 4$.
- All variables are solved for except b and the solutions leave it as a free parameter. Thus there are $4p$ and $2p$ stabilizers for the $p \equiv 1 \mod 4$ and $p \equiv 3 \mod 4$ cases respectively.

DPAF of Chu Sequence

$$A_p(\varphi_{\text{Chu}})[k,\ell]:$$

$$\begin{cases} e^{\pi i(k^2-k)/N}, & k \equiv \ell \bmod N \\ 0, & \text{otherwise} \end{cases}$$

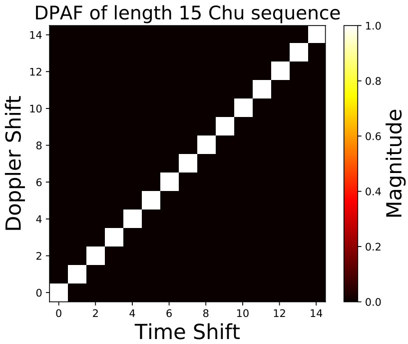


Figure: DPAF of length 15 Chu sequence.

Example: Chu/P4 Seqeunce

Proposition

Let $N = abN'$ where $\gcd(a, b) = 1$ and $\varphi \in \mathbb{C}^N$ be the Chu or P4 sequence. Define $K = \langle a \rangle$, $L = \langle b \rangle$ and $\Lambda = K \times L$.

(a) $\Lambda^\circ = \langle N'a \rangle \times \langle N'b \rangle$.

(b) (φ, Λ) *is a tight Gabor frame bound* NN'.

DPAF of Even Length Wiener Sequence

$$A_p(\varphi_{\text{Wiener}})[k,\ell]:$$
$$\begin{cases} e^{\pi i s k^2/N}, & sk \equiv \ell \bmod N \\ 0, & \text{otherwise} \end{cases}$$

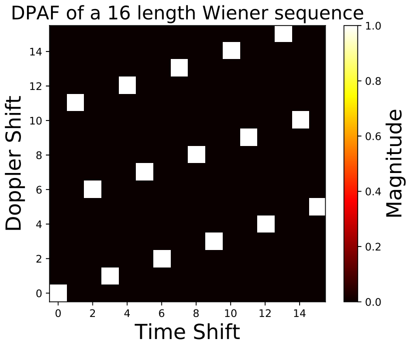


Figure: DPAF of length 16 P4 sequence.

DPAF of Björck Sequence

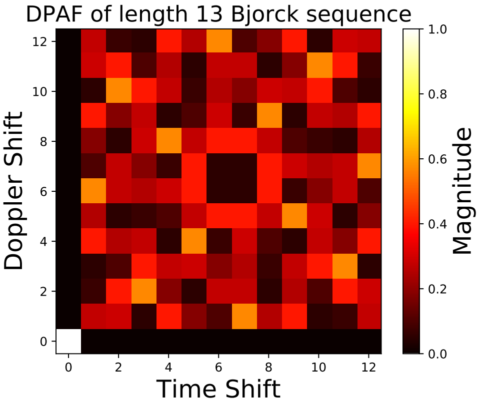


Figure: DPAF of length 13 Björck sequence.

Norbert Wiener Center for Harmonic Analysis and Applications

DPAF of a Kronecker Product Sequence

Kronecker Product:
Let $u \in \mathbb{C}^M, v \in \mathbb{C}^N$.
$(u \otimes v)[aM + b] = u[a]v[b]$

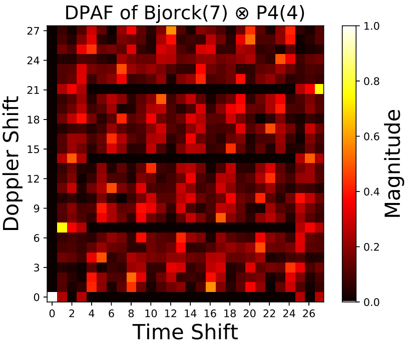


Figure: DPAF of Kroneker product of length 7 Bjorck and length 4 P4.

Example: Kronecker Product Sequence

Proposition

Let $u \in \mathbb{C}^M$ be CAZAC, $v \in \mathbb{C}^N$ be CA, and $\varphi \in \mathbb{C}^{MN}$ be defined by the Kronecker product: $\varphi = u \otimes v$. If $\gcd(M, N) = 1$ and $\Lambda = \langle M \rangle \times \langle N \rangle$, then (φ, Λ) is a tight frame with frame bound MN.

Gram Matrices and Discrete Periodic Ambiguity Functions

Definition

Let $\mathcal{F} = \{v_i\}_{i=1}^{M}$ be a frame for $\mathbb{C}^N$. The *Gram matrix*, G, is defined by

$$G_{i,j} = \langle v_i, v_j \rangle.$$

In the case of Gabor frames $\mathcal{F} = \{e_{\ell_m} \tau_{k_m} \varphi : m \in 0, \cdots, M-1\}$, we can write the Gram matrix in terms of the discrete periodic ambiguity function of φ:

$$G_{m,n} = N e^{-2\pi i k_n (\ell_n - \ell_m)/N} A_p(\varphi)[k_n - k_m, \ell_n - \ell_m]$$

Gram Matrix of Chu and P4 Sequences

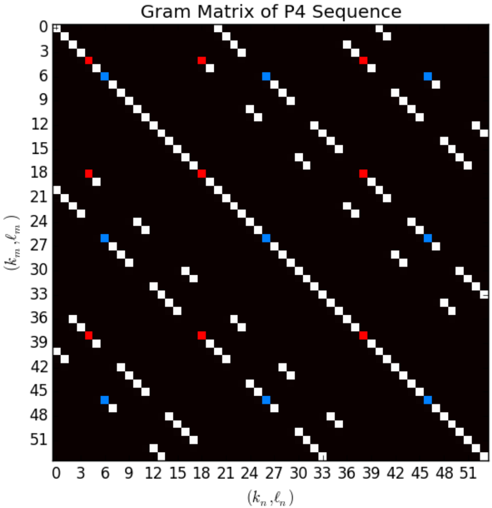
Lemma

Let $\varphi \in \mathbb{C}^N$ be the Chu or P4 sequence and let $N = abN'$ where $gcd(a, b) = 1$. Suppose G is the Gram matrix generated by the Gabor system $(\varphi, K \times L)$ where $K = \langle a \rangle$ and $L = \langle b \rangle$. Then,

(a) *The support of the rows (or columns) of G either completely conincide or are completely disjoint.*

(b) *If two rows (or columns) have coinciding supports, they are scalar multiples of each other.*

Example: P4 Gram Matrix



Tight Frames from Gram Matrix

Theorem

Let $\varphi \in \mathbb{C}^N$ be the Chu or P4 sequence and let $N = abN'$ where $gcd(a, b) = 1$. Suppose G is the Gram matrix generated by the Gabor system $(\varphi, K \times L)$ where $K = \langle a \rangle$ and $L = \langle b \rangle$. Then,

(a) $rank(G) = N$.

(b) G *has exactly one nonzero eigenvalue,* NN'.

In particular (a) and (b) together imply that the Gabor system $(\varphi, K \times L)$ is a tight frame with frame bound NN'.

Norbert Wiener Center for Harmonic Analysis and Applications

Proof

- $K \cap L = \langle ab \rangle$.
- $G_{mn} \neq 0$ if and only if $(\ell_n - \ell_m) \equiv (k_n - k_m) \mod N$.
- This can only occur at the intersection of K and L, i.e.,

$$\forall j \in (\mathbb{Z}/N'\mathbb{Z}),\ (\ell_n - \ell_m) \equiv (k_n - k_m) \equiv jab \mod N$$

- Fix an m, we can write k_n as $k_n = a(j_m + jb)$ for some j
- By the column ordering of G we can write the n-th column by

$$n = k_n N' + \ell_n / b.$$

Proof (con't)

- We want to look at the first N columns so we want $n < N$ and thus require $k_n < ab$.
- Thus, $(j_m + jb) < b$.
- There is exactly one such $j \in (\mathbb{Z}/N'\mathbb{Z})$ and it is $j = -\lfloor j_m/b \rfloor$.
- Consequently, for each row m, there is exactly 1 column $n \leq N$ where $G_{mn} \neq 0$ and the first N columns of G are linearly independent.
- $\text{rank}(G) = N$.

Norbert Wiener Center for Harmonic Analysis and Applications

Proof (con't)

- Let g_n be the n-th column of G, $n < N$.
- The goal is to show that $Gg_n = NN'g_n$.
- $Gg_n[m]$ is given by the inner product of row m and column n.
- The n-th column is the conjugate of the n-th row.
- If $Gg_n[m] \neq 0$, then $G_{mn} \neq 0$ and $G_{nn} \neq 0$.

Proof (con't)

- Lemma implies row m and n have coinciding supports and are constant multiples of each other thus, $G_{m(\cdot)} = C_m g_n^*$ where $|C_m| = 1$.
- Therefore, $Gg_n[m] = C_m \|g_n\|_2^2 = N^2 N' C_m$.
- $G_{nn} = N$, so $g_n[m] = NC_m$.
- Finally, $Gg_n[m] = (NN')(NC_m)$ and we conclude the first N columns of G are eigenvectors of G with eigenvalue NN'.

Future work: Continuous CAZAC Property

Is it possible to generalize CAZAC to the real line? The immediate problem is the natural inner product to use for autocorrelation is the $L^2(\mathbb{R})$ inner product, but if $|f(x)| = 1$ for every $x \in \mathbb{R}$, then clearly $f \notin L^2(\mathbb{R})$.

Norbert Wiener Center for Harmonic Analysis and Applications

Future work: Continuous CAZAC Property

Alternatives and ideas:

- Define a continuous autocorrelation on $L^2(\mathbb{T})$ and push torus bounds to infinity.
- Distribution theory, esp. using tempered distributions.
- Wiener's Generalized Harmonic Analysis, which includes a theory of mean autocorrelation on $\mathbb{R}$.

Future work: Single Pixel Camera

- My work on this is with John Benedetto and Alfredo Nava-Tudela and is an ongoing project.
- The original concept is due to Richard Baraniuk.
- The idea is to construct a camera using only a single light receptor or sensor.
- This is accomplished by filtering through a pixel grid that either admits or blocks light.
- Baraniuk's original design does this with digital micromirror devices.
- Several collections with different pixel grids are required but compressed sensing theory allows this to be done efficiently.

Norbert Wiener Center for Harmonic Analysis and Applications

Questions?

Norbert Wiener Center for Harmonic Analysis and Applications