ABSTRACT

Title of dissertation: Constant Amplitude Zero
Autocorrelation Sequences
and Single Pixel Camera Imaging

Mark Magsino, Doctor of Philosophy, 2018

Dissertation directed by: Professor John Benedetto
Department of Mathematics

The primary focus is on Constant Amplitude Zero Autocorrelation sequences, or CAZAC sequences for short. We provide both an exposition and some new results relating to CAZAC sequences. We then apply them to Gabor frames and prove a condition for checking when Gabor systems generated by a CAZAC sequence are tight frames. We also construct multiple examples using this condition. Finally, we explore natural generalizations of CAZAC sequences to the torus and the real line and provide examples highlighting the differences between the generalizations. In the last section, we highlight some work done in image processing. In particular, we present results in single-pixel camera imaging and the demosaicing problem in image processing.

Constant Amplitude Zero Autocorrelation Sequences and Single Pixel Imaging

by

Mark Magsino

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2018

Advisory Committee:
Professor John Benedetto, Chair/Advisor
Professor Kasso Okoudjou
Professor Wojciech Czaja
Professor Radu Balan
Professor Ramani Duraiswami, Dean's Representative

Dedication

To my friends and family, who have all supported me throughout my graduate studies.

Acknowledgments

First and foremost, I would like to thank my thesis advisor, Dr. John Benedetto. For one, the Norbert Wiener Center, through which I have done all of my research, would not exist without him. He has also been an excellent mentor, both mathematically and professionally. Under his apprenticeship and encouragement, I now have the courage and skills to proceed forward on the academic career path to an exciting postdoctoral opportunity.

I would like to thank the other faculty members of the Norbert Wiener Center: Dr. Kasso Okoudjou, Dr. Wojciech Czaja, and Dr. Radu Balan. All three have agreed to take time out of their busy schedules to read my thesis and serve on my committee. They are also every bit essential to the success of the research program at the Norbert Wiener Center. I was fortunate in my studies to be able to take a class with each of them, and benefit from their immense knowledge and expertise. I especially would like to thank Dr. Okoudjou whose instruction in the introductory real analysis class was instrumental in being able to pass the qualification stage of the program.

I would also like to thank the Dean's representative, Dr. Ramani Duraiswami. I am grateful that he is willing to take time to also read my thesis and serve on my committee, especially because he is on sabbatical.

I am eternally grateful to my parents, who have given me so much support both financially and emotionally. To be able to go to a Ph.D. program debt-free and still receieve support from my parents is a privilege I am extremely grateful for.

More than that, my parents have encouraged me every step of the way, and fully supported my decision to pursue a Ph.D. directly out of undergraduate studies. I could never thank them enough.

I thank my younger brother Kyle Magsino, who as a constant companion in childhood and even in college. We have mostly gotten along over the years, and is someone I have shared many of my hobbies and interests with over the years. Although we no longer see each other much, he is and always has been, an integral part of my life.

I also would like to thank two very close childhood friends, Carl Aquino and Michael Qua. I have known both for over twenty (!) years now and are friends who I always know will be part of my life even if at times we do not hear from each other. Both have supported and encouraged me greatly throughout my graduate studies and have taken time to visit me during my time at Maryland. Both have been essentially family to me, and I could not ask for better friends.

I want to thank my many fellow gradute students at the University of Maryland math department. The feeling of camraderie developed among my batch in the first year led to many great friendships and fruitful math discussions in my time at the University of Maryland. Among that batch I would like to thank Ryan Kirk, who has been my officemate all six years of my study, as well as Jean-Philippe Burelle, Danul Gunatilleka, Jacky Chong, and Ian Johnson, with whom I have had many social interactions with. I would also like to thank my fellow Norbert Wiener Center students both former and current who have also been invaluable companions on this journey.

I would also like to thank my many non-math department friends as well, who are too numerous to even begin listing. While many graduate students tend to avoid undergraduate friends, I instead welcomed them during my time at University of Maryland, and several of them have become lasting friends who I know I will continue to be friends with even as we pursue careers in many different places. I particularly enjoyed my time with the Terrapin Anime Society, which I helped re-create in my earlier graduate student years, which has also led to many of the lasting friendships I have today.

Finally, I would like to thank my girlfriend, Kaitlyn Peltzer who I met early in my first year at University of Maryland. She has been by my side supporting me for over five years throughout nearly the entire graduate studies process. Her love and support has been invaluable, and I am excited to see what the future holds in store for us.

Table of Contents

List of Abbreviations

CAZAC	Constant Amplitude Zero Autocorrelation
DFT	Discrete Fourier Transform
GHA	Generalized Harmonic Analysis
NWC	Norbert Wiener Center
STFT	Short-time Fourier Transform

Chapter 1: Introduction

1.1 Background and Motivation

The primary object of study in this thesis is the constant amplitude zero autocorrelation (CAZAC) property. The study of this property originates in radar and communication theory. The constant amplitude part of the proeprty 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. Classic radar theory considers sequences with these two properties for signals where they encode information into the phase of the outgoing signal [1]. It is also used in 4G LTE technology [2], and more recently, in the development of 5G wireless communication technology [3, 4].

In addition to its uses in radar and communcation theory, the CAZAC property leads to fascinating mathematical problems and ideas. In particular, CAZAC sequences are connected to cyclic N-roots and circulant Hadamard matrices. Cyclic N-roots are algebraic varieties, giving CAZAC sequences have a surprising connection to algebraic geometry. Chapter 2 examines these connections, expands upon them, and gives a detailed exposition of the theory of CAZAC sequences.

Another way of viewing the zero autocorrelation property is that it implies that all translations of the sequence are orthogonal to the original sequence. One might hope that this property extends if we look at both time and frequency shifts. To take it one step further, this leads to the idea that these sequences might be suitable for constructing Gabor frames. Gabor frames are representation of vectors in terms of a base vector and time-frequency shifts of the base vector. This motivates the material of Chapter 3, where we examine when it is viable to obtain Gabor frames from CAZAC sequences.

The theory surrounding the CAZAC property, both in engineering and in mathematics, only concerns itself with finite sequences. In particular, these settings only allow for discrete interpretations of the CAZAC property. However, radar signals are continuous waves. It is natural then to consider extending the CAZAC property to continuous domains such as $\mathbb{T} = \mathbb{R}/2\pi$ or $\mathbb{R}$. However, there are a lot of technical problems with this approach. For a start, the usual inner product on functions requires the functions be in $L^2(\mathbb{R})$ but any constant amplitude function on $\mathbb{R}$ will not be in $L^2(\mathbb{R})$. Alternatives include distribution theory and Wiener's generalized harmonic analysis [5]. This is the subject of Chapter 4.

In the final chapter, Chapter 5 we diverge from the theme of the CAZAC property and look at the single pixel camera system. Standard color cameras for consumer have a visible light sensor corresponding to each individual pixel that a camera image will have. In the modern era of megapixel cameras, this corresponds to millions of small sensors crammed into camera devices. For general visible light images, this is viable in large part due to the ability to manufacture chips that can contain millions of sensors for a small cost. However, for other light spectra sensors used in research, the sensors can become prohibitively expensive. To get around this, the idea is to use a pixel mask that lets light through some pixels but not others. Iterating this process enough times (but less times than the number of pixels) allows for reconstruction of the image with only a single sensor. This is made possible by compressed sensing. We only briefly outline the direction of this research in this thesis, as this work is currently still ongoing. Some modern applications of this single pixel camera framework include tomography [6] and imaging in the terahertz frequency range [7].

1.2 Outline and Original Contributions

This section simultaneously serves as an outline and a highlight of the original contributions contained in this body of work. Furthermore, we expand on how the ideas contained in the previous section will be covered in detail in each section within the chapters. The rest of the first chapter serves as a brief review of Fourier analysis as well as a way to establish notation and convention to be used throughout in the later chapters.

Chapter 2 is dedicated to a thorough exposition on Constant Amplitude Zero Autocorrelation (CAZAC) sequences. While this chapter is largely a presentation of the previously known results on CAZAC sequences, some original work is contained within as well. The bulk of this chapter is contained in a joint book chapter with Katherine Cordwell and John Benedetto [8]. The Section 2.1 contains the bulk of introductory theory for CAZAC sequences as well as the deep mathematical problems relating to it. Other refrences include [9,10]. The main original work here is collecting and organizing the known results on CAZACs into a single exposition as well as adding a few minor details to proofs.

Section 2.2 has three pieces which are original contributions, all of which are focused on generating CAZAC sequences comprised of roots of unity. The first contribution is a method which generates all CAZAC sequences of length 3 by parameterizing Hadamard matrices and solving systems of equations to enforce the circulant condition. This contribution is made from one of the other authors in [8], Katherine Cordwell. The second contribution again focuses on length 3 CAZAC sequences, but is a second approach which solves for all cyclic 3-roots. This computation is both elementary and easily performed, but worthwhile for giving insight into the link between cyclic N-roots and CAZAC sequences. The final contribution is a more general and is a way to analyze roots of unity CAZAC sequences of any prime length p. This approach examines the orbits of CAZAC sequences under the group action generated by the CAZAC sequence equivalency generated in [10]. A complete description of the equilvalency classes under the 5-operation equivalence from [10] is given.

Section 2.3 is purely expositional, and focuses on CAZAC sequences which are not generated by roots of unity. The main focuses are the general class of CAZAC sequences generated by Göran Björck and specific examples in the length 7 case which are due to Uffe Haagerup. The final section of Chapter 2, Section 2.4, is an exposition of Haagerup's proof that the number of CAZAC sequences of prime length which begin with 1 is finite.

Chapter 3 is original work submitted to the Sampling Theory in Signal and Image Processing Journal [11]. In Section 3.1, we give a brief exposition on frame theory and Gabor frame theory in order to set up the necessary tools to prove the main theorem, Theorem 3.2.7. Section 3.2 deals with general finite Gabor frames and presents a necessary and sufficient condition for determining if a finite Gabor frame is tight. Section 3.3 applies Theorem 3.2.7 from Section 3.2 to Gabor frames generated by CAZAC sequences. The major contribution in Section 3.3 is a collection of detailed examples which illustrate Theorem 3.2.7. All of these examples are important for giving insight into the suitability of CAZAC sequences for the construction of tight Gabor frames. We shall see that some CAZACs are suitable for the generation of tight Gabor frames while others are very poor for generating tight Gabor frames. Finally, Section 3.4 presents a novel alternate approach to determining if a finite Gabor frames are tight. This approach examines the structure of the Gram matrix generated by a CAZAC sequence Gabor frame and uses that structure to prove tightness.

Chapter 4 is also original work which focuses on generalizing the CAZAC property. In Section 4.1, we give a brief motivation and justification for the study of generalized CAZAC property. Section 4.2 relates the discrete periodic ambiguity function to the ambiguity function on the torus. We also give an explicit example of computing the ambiguity function on the torus using discrete approximations of an $L^2(\mathbb{T})$ function. Section 4.3is focused on distribution theory as a way to extend the CAZAC property to the real line. In this section, we give a brief introduction to the theory of tempered distributions but one of many places to find a more detailed exposition is [12]. The major result here, Theorem 4.3.9, is easy to prove from basic distribution theory but gives a simple and natural analogue of the theorem in the discrete case where a sequence $\varphi \in \mathbb{C}^N$ is CAZAC if and only if $\widehat{\varphi} \in \mathbb{C}^N$ is also CAZAC. Section 4.4 is focused on Wiener's generalized harmonic analysis as another way to extend the CAZAC property to sequences on the real line. This section opens up with an exposition of Wiener's generalized harmonic analysis and is one of the building blocks to spectral synthesis [13]. We explore possible formulations of both mean constant amplitude and zero mean autocorrelation.

Chapter 5 is a mixture of exposition and collaborative work alongside Alfredo

Nava-Tudela and John Benedetto, as well as David Bowen from the University of Maryland Labratory for Physical Sciences. All of it is a work still in progress and this chapter serves as a highlight of our current agenda. Section 5.1 is a short introduction and explanation of the single pixel camera setup. Section 5.2 is a quick overview of the basic theory of compressed sensing, the bulk of which is taken from the exposition of Bruckstein, Donoho, and Elad [14]. It also explains how the compressed sensing theory can be used in the single pixel camera setup. Finally, Section 5.3 highlights possible applications of compressed sensing theory to the topics of super-resolution and de-mosaicing.

1.3 Fourier Analysis

The purpose of this section is to simultaneously give a quick referesher of the basics of Fourier analysis and to establish the related conventions that will be used throughout. Again, there are numerous fantastic references for Fourier analysis, but the bulk of this brief exposition is taken from [12]. First, we will write $\mathbb{R}$ for the real line when we talk about the time domain, and $\widehat{\mathbb{R}}$ for the real line when we talk about the Fourier (frequency) domain. The reasoning for this is when dealing with Fourier analysis for a locally compact Abelian group, G, the Fourier domain consists of characters from the dual group of G, typically denoted Γ. In the case of $G = \mathbb{R}$, the character group can be identified with the real line itself, that is $\Gamma \cong \mathbb{R}$. We thus choose the notation $\widehat{\mathbb{R}}$ to emphasize this relation and choose the hat notation to match the Fourier transform notation. We begin by defining the Fourier transform.

Definition 1.3.1. Let $f \in L^1(\mathbb{R})$. We define the *Fourier transform*, $\widehat{f} : \widehat{\mathbb{R}} \to \mathbb{C}$ as

$$\widehat{f}(\gamma) = \int_{\mathbb{R}} f(t)e^{-2\pi it\gamma}\, dt. \tag{1.3.1}$$

We denote the space of all functions which are the Fourier transform of some function in $L^1(\mathbb{R})$ as $A(\widehat{\mathbb{R}})$. That is,

$$A(\widehat{\mathbb{R}}) = \{\widehat{f} : f \in L^1(\mathbb{R})\}. \tag{1.3.2}$$

Definition 1.3.2. The inversion formula is given by the *inverse Fourier transform* and is computed by

$$f(t) = \int_{\widehat{\mathbb{R}}} \widehat{f}(\gamma)e^{2\pi it\gamma}\, d\gamma. \tag{1.3.3}$$

Although a complete general characterization of $A(\widehat{\mathbb{R}})$ is still not known, there are a few things one can say about $A(\widehat{\mathbb{R}})$. In fact, $A(\widehat{\mathbb{R}}) \subseteq C_0(\widehat{\mathbb{R}})$. Continuity comes easily from the Lebesgue dominated convergence theorem, and the decay at infinity is the result of the Riemann-Lebesgue lemma. We now define the operators of translation, modulation, and dilation, and describe how they interact with the Fourier transform.

Definition 1.3.3.

(a) The translation operator, τ_x, is given by

$$\tau_x f(t) = f(t - x). \tag{1.3.4}$$

(b) The modulation operator, e_ω, is given by

$$e_\omega f(t) = e^{2\pi i \omega t} f(t). \tag{1.3.5}$$

(c) The dilation operator, d_λ, ($\lambda \neq 0$) is given by

$$d_\lambda f(t) = \lambda f(\lambda(t)). \tag{1.3.6}$$

Theorem 1.3.4. *Let $f \in L^1(\mathbb{R})$, and let $\mathcal{F} : L^1(\mathbb{R}) \to A(\widehat{\mathbb{R}})$ denote the Fourier transform operator. Then,*

(a) $\mathcal{F}(\tau_x f) = e_{-x}\widehat{f}$,

(b) $\mathcal{F}(e_\omega f) = \tau_\omega \widehat{f}$,

(c) $\mathcal{F}(d_\lambda f) = |\lambda| d_{1/\lambda}\widehat{f}$.

Another important formula of Fourier transforms is known as the *exchange formula*, which states the following,

Proposition 1.3.5. *Let $f, g \in L^1(\mathbb{R})$, and let $\mathcal{F} : L^1(\mathbb{R}) \to A(\widehat{\mathbb{R}})$ be the Fourier transform operator. Then,*

$$\mathcal{F}(f * g) = \widehat{f}\widehat{g}. \tag{1.3.7}$$

Last, we briefly cover the Fourier theory of $L^2(\mathbb{R})$. This setting is important for practical considerations as $L^2(\mathbb{R})$ can be seen as the space of signal which have finite energy. Moreover, the following theorem shows that the $L^2(\mathbb{R})$ Fourier transform has several useful properties. The proof only uses basic Lebesuge integral theory, but is long and involved and is omitted here.

Theorem 1.3.6 (Plancherel)**.** *There is a unique linear bijection $\mathcal{F} : L^2(\mathbb{R}) \to L^2(\widehat{\mathbb{R}})$ with the properties:*

(a) $\forall f \in L^2(\mathbb{R}), \|f\|_2 = \|\mathcal{F}f\|_2$,

(b) $\forall f \in L^1(\mathbb{R}) \cap L^2(\mathbb{R}), \widehat{f} = \mathcal{F}f$,

(c) $\forall f \in L^2(\mathbb{R})$, *there exists* $\{f_n\}_{n=1}^{\infty}$ *such that*

$$\lim_{n\to\infty} \|f_n - f\|_2 = 0 \text{ and } \lim_{n\to\infty} \|\widehat{f}_n - \mathcal{F}f\|_2 = 0. \tag{1.3.8}$$

From Theorem 1.3.6, we derive one more formula using the inner products of the spaces $L^2(\mathbb{R})$ and $L^2(\widehat{\mathbb{R}})$.

Theorem 1.3.7 (Parseval)**.** *Let $f, g \in L^2(\mathbb{R})$, and $\widehat{f}, \widehat{g} \in L^2(\mathbb{R})$ be their $L^2(\mathbb{R})$ Fourier transforms. Then,*

$$\langle f, g\rangle = \langle \widehat{f}, \widehat{g}\rangle. \tag{1.3.9}$$

Chapter 2: CAZAC: Constant Amplitude Zero Autocorrelation

2.1 CAZAC Sequences

This chapter is dedicated to an exposition on CAZAC sequences. Much of this chapter is based on [8], but also includes some work from [11] and concludes with the fascinating unpublished theorem of Uffe Haagerup [15] which proves that the number of finite CAZAC sequences which begin with 1 is finite. To begin the exposition, we define the discrete Fourier transform to establish convention.

Definition 2.1.1. Let $\varphi \in \mathbb{C}^N$.

(a) The *discrete Fourier transform* of φ, $\widehat{\varphi} \in \mathbb{C}^N$, is defined by

$$\widehat{\varphi}[\ell] = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \varphi[k] e^{-2\pi i k\ell/N}. \tag{2.1.1}$$

(b) The *inverse discrete Fourier transform* is defined by

$$\varphi[k] = \frac{1}{\sqrt{N}} \sum_{\ell=0}^{N-1} \widehat{\varphi}[\ell] e^{2\pi i k\ell/N} \tag{2.1.2}$$

Definition 2.1.2. A sequence $\varphi \in \mathbb{C}^N$ is called a *constant amplitude zero autocorrelation* (CAZAC) sequence if it satisfies the two properties:

$$|\varphi[k]| = 1, \quad \forall k \in (\mathbb{Z}/N\mathbb{Z}). \tag{CA}$$

and

$$\sum_{k=0}^{N-1} \varphi[k+m]\overline{\varphi[k]} = 0, \quad \forall m \in (\mathbb{Z}/N\mathbb{Z})\backslash\{0\} \tag{ZAC}$$

An equivalent definition of CAZAC sequences are sequences where both φ and $\widehat{\varphi}$ satisfy (CA). As such, CAZAC sequences are sometimes refered to *biunimodular sequences*. threfcazacprop highlights this property along with other facts about CAZAC sequences and its relation to the Fourier transform. Before proving Proposition 2.1.5, we list a few examples of known CAZAC seqeuences.

Definition 2.1.3. Let $\varphi \in \mathbb{C}^N$ be of the form

$$\varphi[k] = e^{\pi i p[k]/N}, \tag{2.1.3}$$

where $p[k]$ is a polynomial. We define the Chu, P4, and Wiener sequences with,

- Chu: $p[k] = k(k-1)$ if N is odd.
- P4: $p[k] = k(k-N)$ for any N.
- Wiener (odd length): $p[k] = sk^2$, if N is odd and $\gcd(s, N) = 1$.
- Wiener (even length): $p[k] = sk^2/2$, if N is even and $\gcd(s, 2N) = 1$.

It is elementary to verify that all three classes of sequences are indeed CAZAC. They belong to a class of sequences known as chirp sequences. Chirp sequences are sequences whose frequency change linearly in time and are also known as quadratic phase sequences. Additional exposition on chirp sequences can be found in [9].

Definition 2.1.4. Let $c \in \mathbb{C}^N$ be CA, $v \in \mathbb{C}^M$ be CAZAC, and σ be any permutation of $(\mathbb{Z}/N\mathbb{Z})$. Then,

(i) The *square length Björck-Saffari sequence*, $\varphi \in \mathbb{C}^{N^2}$, is defined by,

$$\forall r \in (\mathbb{Z}/N\mathbb{Z}), h \in (\mathbb{Z}/N\mathbb{Z}), \varphi[rN + h] = c[h]e^{2\pi i r\sigma(h)/N}. \tag{2.1.4}$$

(ii) The *Milewski sequence*, $\varphi \in \mathbb{C}^{MN^2}$ is defined by,

$$\forall a \in (\mathbb{Z}/MN\mathbb{Z}), b \in (\mathbb{Z}/N\mathbb{Z}), \varphi[aN + b] = v[a]e^{2\pi i ab/MN}. \tag{2.1.5}$$

The square-length Björck-Saffari sequences were defined by Björck and Saffari as a building block to a more general class of CAZAC sequences whose lengths are not necessarily a perfect square [16]. The Milewski sequence was first defined by Milewski in [17] as a way to construct more CAZAC sequences out of already existing ones.

Proposition 2.1.5. *Let $\varphi \in \mathbb{C}^N$ and let $c \in \mathbb{C}$ be such that $|c| = 1$. Then,*

(i) If φ is CA, then $\widehat{\varphi}$ is ZAC.

(ii) If φ is CAZAC, then $\widehat{\varphi}$ is also CAZAC.

(iii) If φ is CAZAC, then $c\varphi$ is also CAZAC.

Proof. Parts *(ii)* is an immediate consequences of part *(i)*. To prove part *(i)* we proceed as follows. Suppose $\varphi \in \mathbb{C}^N$ is CA and let $n \neq 0$. Then, using the Parseval formula for the third equality, we have

$$\sum_{k=0}^{N-1} \widehat{\varphi}[n+k]\overline{\widehat{\varphi}[k]} = \langle \tau_{-n}\widehat{\varphi}, \widehat{\varphi}\rangle = \langle e_n\varphi, \varphi\rangle \tag{2.1.6}$$

$$= \sum_{k=0}^{N-1} |\varphi[k]|^2 e^{2\pi i kn/N} = \sum_{k=0}^{N-1} e^{2\pi i kn/N} = 0. \tag{2.1.7}$$

and so $\widehat{\varphi}$ is ZAC.

Next, suppose that $\varphi \in \mathbb{C}^N \backslash \{0\}$ is ZAC and let $m \neq 0$. Then,

$$0 = \sum_{k=0}^{N-1} \varphi[m+k]\overline{\varphi[k]} = \langle \tau_{-m}\varphi, \varphi \rangle = \sum_{k=0}^{N-1} |\widehat{\varphi}[k]|^2 \, e^{2\pi imk/N}, \tag{2.1.8}$$

where the last step follows from the Parseval formula. Let $\widehat{\psi} = |\widehat{\varphi}|^2$, so that by the inversion theorem, we have

$$\forall m \in \mathbb{Z}/N\mathbb{Z}, \quad \psi[m] = \frac{1}{N^{1/2}} \sum_{k=0}^{N-1} \widehat{\psi}[k] \, e^{2\pi imk/N}. \tag{2.1.9}$$

Thus, because of (2.1.8), we know that $\psi[m] = 0$ for $m \in \mathbb{Z}/N\mathbb{Z}\backslash\{0\}$, and so

$$\forall n \in \mathbb{Z}/N\mathbb{Z}, \quad \widehat{\psi}[n] = \frac{1}{N^{1/2}} \, \psi[0] \tag{2.1.10}$$

by the definition of the DFT. Hence, by the definition of $\widehat{\psi}$, $\widehat{\varphi}$ is constant on $\mathbb{Z}/N\mathbb{Z}$, although not necessarily taking the value 1. The converse directions in each case are proved by replacing φ with $\widehat{\varphi}$. □

Property (iii) allows us to say two CAZAC sequences are equivalent if they are complex rotations of each other. We assume that the representative CAZAC sequence in each equivalence class is the sequence whose first entry is 1. Given this, a natural question follows: For each N, how many CAZAC sequences of length N are there? If N is prime, then there are only finitely many classes [15]. We present Haagerup's brilliant proof of this in Section 2.4. On the other hand, if N is composite and is not square-free, then there are infinitely many classes [16], see Theorem 2.1.8. This result is due to Björck and Saffari and we present their proof of it here as well. If N is composite and square-free, it is unknown whether the number

Table 2.1: $r(N)$ and $r_u(N)$ for $N = 2, \dots, 9$

N	2	3	4	5	6	7	8	9
$r(N)$	2	6	∞	70	156	924	∞	∞
$r_u(N)$	2	6	∞	20	48	532	∞	∞

of equivalence classes is finite or infinite. Another question is, what other CAZAC sequences can we construct besides the Chu, P4, etc.? The problem of discovering other CAZAC sequences can be transformed into two different problems in very different areas of mathematics. In particular, the problem of discovering CAZAC sequences is equivalent to two other problems: The first is finding all circulant Hadamard matrices and the second is finding all cyclic n-roots. We present these alternate formulations in this section as well.

Theorem 2.1.6. *Let $c \in \mathbb{C}^N$ be any constant amplitude sequence of length $N \geqslant 2$, and let σ be any permutation of $(\mathbb{Z}/N\mathbb{Z})$. Define a new sequence, $\varphi \in \mathbb{C}^{N^2}$, by the formula,*

$$\forall a, b \in (\mathbb{Z}/N\mathbb{Z}), \quad \varphi[aN + b] = c[b]e^{2\pi i a\sigma(b)/N}. \tag{2.1.11}$$

Then, φ is a CAZAC sequence of length N^2.

Proof. Without loss of generality, assume $|c[i]| = 1$ for all $i = 0, 1, \dots, N-1$. The sequence, φ, is CA by its definition. We shall prove that φ is also ZAC by verifying that $\widehat{\varphi}$ is CA. Let $W_{N^2} = e^{2\pi i/N^2}$. Then,

$$|\widehat{\varphi}[j]| = \left|\sum_{k=0}^{N^2-1} \varphi[k] W_{N^2}^{-kj}\right| = \left|\sum_{a=0}^{N-1}\sum_{b=0}^{N-1} \varphi[aN+b] W_{N^2}^{-(aN+b)j}\right| \tag{2.1.12}$$

$$= \left| \sum_{a=0}^{N-1} \sum_{b=0}^{N-1} c[b] W_{N^2}^{Na\sigma(b)} W_{N^2}^{-aNj} W_{N^2}^{-bj} \right| \tag{2.1.13}$$

$$= \left| \sum_{b=0}^{N-1} c[b] W_{N^2}^{-bj} \sum_{a=0}^{N-1} W_{N^2}^{Na\sigma(b)} W_{N^2}^{-aNj} \right| \tag{2.1.14}$$

$$= \left| \sum_{b=0}^{N-1} c[b] W_{N^2}^{-bj} \sum_{a=0}^{N-1} W_{N^2}^{N(\sigma(b)-j)a} \right|. \tag{2.1.15}$$

Note that the inner sum of (2.1.15) is 0 unless $\sigma(b) \equiv j \bmod N$, in which case the inner sum is N. Thus, we can rewrite (2.1.15), taking j modulo N if necessary, as

$$|\hat{\varphi}[j]| = \left| \sum_{b=0}^{N-1} c[b] W_{N^2}^{-bj} \sum_{a=0}^{N-1} W_{N^2}^{N(\sigma(b)-j)a} \right| = |Nc[\sigma^{-1}(j) W_{N^2}^{-\sigma^{-1}(j)j}| = N. \tag{2.1.16}$$

□

Corollary 2.1.7. *Given an integer $N \geqslant 2$. There are infinitely many non-equivalent CAZAC sequences of length N^2 whose first term is 1.*

The corollary immediately follows from taking any $c \in \mathbb{C}^N$ where $c[0] = 1$. The next theorem extends Theorem 2.1.6 to arbitrary sequences whose length is not square free.

Theorem 2.1.8. *Let $Q \geqslant 2$ be an integer, let N^2 be the largest square dividing Q, let σ be any permutation of $(\mathbb{Z}/N\mathbb{Z})$, and consider the primitive M-root W_M, where $M = Q/N$. Let $W_M = e^{2\pi i/M}$. If $c \in \mathbb{C}^N$ is a constant amplitude sequence of length N, then define a new sequence, $\varphi \in \mathbb{C}^Q$, by the formula,*

$$\forall a \in (\mathbb{Z}/M\mathbb{Z}) \text{ and } \forall b \in (\mathbb{Z}/N\mathbb{Z}), \quad \varphi[aN+b] = c[b] W_M^{a\sigma(b)+Na(a-1)/2}. \tag{2.1.17}$$

If at least one of N and $M-1$ is even, then x is a CAZAC sequence of length Q.

Proof. Without loss of generality, assume $|c[i]| = 1$ for every $i \in (\mathbb{Z}/N\mathbb{Z})$. First, we note that x can be extended to an Q-periodic function on all of $\mathbb{Z}$. Indeed, if we let $k \in \mathbb{Z}$ be written as $k = aN + b$, then

$$\frac{\varphi[Q+k]}{\varphi[k]} = \frac{\varphi[(M+a)N+b]}{\varphi[aN+b]} = \frac{c[b]W_M^{(M+a)\sigma(b)+N(M+a)(M+a-1)/2}}{c[b]W_M^{a\sigma(b)+Na(a-1)/2}} \tag{2.1.18}$$

$$= \frac{W_M^{M\sigma(b)}W_M^{a\sigma(b)}W_M^{N(M^2+2Ma-M)}W_M^{Na(a-1)/2}}{W_M^{a\sigma(b)}W_M^{Na(a-1)/2}} \tag{2.1.19}$$

$$= W_M^{M\sigma(b)}W_M^{NM(2a+(M-1))/2} = 1, \tag{2.1.20}$$

since both terms are an M-th root of unity raised to a power which is an integer multiple of M.

Using this, we can directly compute the auto-correlation of φ at $u = rN + s$, where $r \in (\mathbb{Z}/M\mathbb{Z})$ and $s \in (\mathbb{Z}/N\mathbb{Z})$ and at least one of r and s is nonzero, i.e., $u \neq 0$. Let $k = aN + b$ and $\theta = \lfloor \frac{b+s}{N} \rfloor$. Then,

$$\sum_{k=0}^{Q-1} \varphi[k+u]\overline{\varphi[k]} = \sum_{a=0}^{M-1}\sum_{b=0}^{N-1} \varphi[(a+r+\theta)N + (b+s)]\overline{\varphi[aN+b]} \tag{2.1.21}$$

$$= \sum_{a=0}^{M-1}\sum_{b=0}^{N-1} c[b+s]W_M^{(a+r+\theta)\sigma(b+s)+N(a+r+\theta)(a+r+\theta-1)/2}\overline{c[b]}W_M^{-a\sigma(b)-Na(a-1)/2} \tag{2.1.22}$$

$$= C_r \sum_{b=0}^{N-1} c[b+s]\overline{c[b]}W_M^{\frac{N\theta(2r+\theta-1)}{2}+(r+\theta)\sigma(b+s)} \sum_{a=0}^{M-1} W_M^{a(\sigma(b+s)-\sigma(b)+N(r+\theta))}, \tag{2.1.23}$$

where $C_r = W_M^{N(r^2-r)/2}$. If $s = 0$, then $\theta = 0$ for every $b \in (\mathbb{Z}/N\mathbb{Z})$, and we can write (2.1.23) as

$$C_r \sum_{b=0}^{N-1} |c[b]|^2 W_M^{r\sigma(b)} \sum_{a=0}^{M-1} W_M^{aNr} = C_r \sum_{a=0}^{M-1}\sum_{b=0}^{N-1} W_M^{r(\sigma(b)+aN)}. \tag{2.1.24}$$

Since σ is a permutation of $(\mathbb{Z}/N\mathbb{Z})$, we can make a substitution $q = \sigma(b)$ and reorder as necessary to rewrite (2.1.24) as

$$C_r \sum_{a=0}^{M-1} \sum_{q=0}^{N-1} W_M^{r(aN+q)} = C_r \sum_{k=0}^{Q-1} W_M^{rk} = 0, \tag{2.1.25}$$

since $r \neq 0 \bmod N$. If $s \neq 0$, then in the inner sum of (2.1.23) we observe that $0 < |\sigma(b+s) - \sigma(b)| < N$, and thus N does not divide $(\sigma(b+s) - \sigma(b) + N(r+\theta))$ for any fixed b. It then follows that M does not divide $(\sigma(b+s) - \sigma(b) + N(r+\theta))$ for any fixed b and the inner sum is 0 for every b. Thus, if $s \neq 0$ then (2.1.23) is 0 as well. □

Corollary 2.1.9. *Given an integer $Q \geqslant 2$, that is not square-free. There are infinitely many non-equivalent CAZAC sequences of length Q whose first term is 1.*

Proof. Take $c[0] = 1$. Let N^2 be the largest square dividing Q and $M = Q/N$. If either N is even or M is odd, then Theorem Theorem 2.1.8 applies immediately and the sequence given in Theorem Theorem 2.1.8 gives us infinitely many CAZAC sequences. If N is odd and M is even, then Q has exactly one factor of 2. Thus, we can write $M = 2M'$ with M' odd. In Theorem Theorem 2.1.8, replace Q by $Q/2$ and M with M', and let y be the resulting CAZAC sequence of length $Q/2$. We can then construct a CAZAC sequence of length Q by taking the Kronecker product $z \otimes y$ of $z = (1, i) \in \mathbb{C}^2$ by $y \in \mathbb{C}^{Q/2}$, so that

$$z \otimes y = \left(y[0], y[1], \ldots, y\left[\frac{Q}{2} - 1\right], i\,y[0], i\,y[1], \ldots, i\,y\left[\frac{Q}{2} - 1\right] \right). \tag{2.1.26}$$

□

We now proceed to connecting CAZAC sequences to Hadamard matrices and cyclic N-roots. In the next section we will explore these connections to generate all CAZAC sequences of length 3 and 5.

Definition 2.1.10. Let $H \in \mathbb{C}^{N \times N}$.

(i) H is a *Hadamard matrix* if for every (i, j), $|H_{i,j}| = 1$ and $HH^* = NId$.

(ii) H is a *circulant matrix* if for each i, the i-th row is a circular shift of the first row by $i - 1$ entries to the right.

One can construct a circulant Hadamard matrix by making the first row a CAZAC sequence and each row after a shift of the previous row to the right. It is clear that this construction leads to a circulant matrix, and the ZAC property will guarantee that $HH^* = NId$. The converse direction also holds true as well. We prove this with Theorem 2.1.11 below [9].

Theorem 2.1.11. *$\varphi \in \mathbb{C}^{N \times N}$ is a CAZAC sequence if and only if the circulant matrix generated by φ is a Hadamard matrix.*

Proof. First, we show that if $\varphi = (\varphi_0, \cdots, \varphi_{N-1})$ is the first row of a complex $N \times N$ circulant Hadamard matrix H, then φ is a CAZAC sequence, $\{\varphi[0], \ldots, \varphi[N-1]\}$, where each $\varphi[m] = \varphi_m$. Because H is a Hadamard matrix, each entry has norm 1, so φ satisfies the CA condition defining CAZAC sequences. Next, because H is circulant, H has the form

$$\begin{bmatrix} \varphi_0 & \varphi_1 & \cdots & \varphi_{N-1} \\ \varphi_1 & \varphi_2 & \cdots & \varphi_0 \\ & & \ddots & \\ \varphi_{N-1} & \varphi_0 & \cdots & \varphi_{N-2} \end{bmatrix}.$$

Now, as noted in Definition 2.1.10, the orthogonality property of Hadamard matrices implies that $HH^* = NId$. In particular, this means that the inner product of x with column i of H is zero, where $2 \leqslant i \leqslant n$. Note that column i is of the form $\varphi_i, \varphi_{i+1}, \cdots, \varphi_{i+(N-1)}$ where subscripts are taken modulo N. So the ith column is a rotation of φ, and, taken together, columns $2, \ldots, N$ comprise all the nonidentity rotations of φ. So, the inner product of φ with any nonidentity rotation of φ is 0, and thus φ satisfies the zero auto-correlation property of CAZAC sequences. Hence, $\varphi = \{\varphi[0], \ldots, \varphi[N-1]\}$ is a CAZAC sequence.

Conversely, we show that if $\varphi = \{\varphi[0], \ldots, \varphi[N-1]\}$ is a CAZAC sequence, then $\varphi = (\varphi[0], \cdots, \varphi[N-1])$ is the first row of a complex circulant Hadamard matrix $H = C_N$, of the form

$$\begin{bmatrix} \varphi_0 & \varphi_1 & \cdots & \varphi_{N-1} \\ \varphi_1 & \varphi_2 & \cdots & \varphi_0 \\ & & \ddots & \\ \varphi_{N-1} & \varphi_0 & \cdots & \varphi_{n-2} \end{bmatrix}.$$

Now, because φ is a CAZAC sequence, the absolute value of each φ_i is 1. Thus, H satisfies the unimodular condition of complex Hadamard matrices.

Next, choose any row $(\varphi_i, \varphi_{i+1}, \cdots, \varphi_{i+(N-1)})$ of H, where we consider subscripts mod N. Then, when we take the inner product of $(\varphi_i, \varphi_{i+1}, \cdots, \varphi_{i+(N-1)})$ with itself, we obtain $\varphi_i\overline{\varphi_i}+\varphi_{i+1}\overline{\varphi_{i+1}}+\cdots+\varphi_{N-1}\overline{\varphi_{N-1}} = 1+1+\cdots+1 = N$, since the absolute value of each φ_i is 1. If we take any other row, $(\varphi_j, \varphi_{j+1}, \ldots, \varphi_{j+(N-1)})$, of H, where $i \neq j$, then the inner product $\langle(\varphi_i, \varphi_{i+1}, \ldots, \varphi_{i+(N-1)}), (\varphi_j, \varphi_{j+1}, \ldots, \varphi_{j+(N-1)})\rangle$ is zero because φ has zero auto-correlation. This implies that

$$HH^* = \begin{bmatrix} \varphi_0 & \varphi_1 & \cdots & \varphi_{N-1} \\ \varphi_1 & \varphi_2 & \cdots & \varphi_0 \\ & & \ddots & \\ \varphi_{N-1} & \varphi_0 & \cdots & \varphi_{N-2} \end{bmatrix} \begin{bmatrix} \overline{\varphi_0} & \overline{\varphi_1} & \cdots & \overline{\varphi_{N-1}} \\ \overline{\varphi_1} & \overline{\varphi_2} & \cdots & \overline{\varphi_0} \\ & & \ddots & \\ \overline{\varphi_{N-1}} & \overline{\varphi_0} & \cdots & \overline{\varphi_{N-2}} \end{bmatrix} = NId,$$

where Id is the identity matrix. Thus, H satisfies the orthogonality property of complex Hadamard matrices, and hence $H = C_N$ is a complex circulant Hadamard matrix. □

From Theorem 2.1.11 we conclude that there is a one-to-one correspondence between circulant $N \times N$ Hadamard matrices whose diagonal consists of 1s and of CAZAC sequences of length N whose first entry is 1. Therefore, computing circulant Hadamard matrices is equivalent to the discovery of CAZAC sequences. There is a significant amount of research and interest in Hadamard matrices, even outside of the context of CAZACs. A catalogue of complex Hadamard matrices with relevant citations can be found online at [18]. Moreover, we can get at another notion of equivalence between CAZAC sequences by defining them to be equivalent if they satisfy Hadamard matrix equivalency defined by Definition 2.1.12 below.

Definition 2.1.12. Let H_1, H_2 be two Hadamard matrices. As matrices they are equivalent if they can be transformed one into the other by elementary row and column operations. In the case of Hadamard matrices, this is the same as saying that H_1 and H_2 are *equivalent* if there exist diagonal unitary matrices D_1, D_2 and permutation matrices P_1, P_2 such that

$$H_2 = D_1 P_1 H_1 P_2 D_2. \tag{2.1.27}$$

Definition 2.1.13. $(z_0, z_1, \cdots, z_{N-1}) \in \mathbb{C}^N$ is a *cyclic N-root* if it satisfies the following system of equations,

$$\begin{cases} z_0 + z_1 + \cdots + z_{N-1} = 0 \\ z_0 z_1 + z_1 z_2 + \cdots + z_{N-1} z_0 = 0 \\ z_0 z_1 z_2 + z_1 z_2 z_3 + \cdots + z_{N-1} z_0 z_1 = 0 \\ \cdots\cdots \\ z_0 z_1 z_2 \cdots z_{N-1} = 1 \end{cases} . \tag{2.1.28}$$

Let $\varphi \in \mathbb{C}^N$ be CAZAC with $\varphi[0] = 1$. Let us emphasize the sequence nature of $\varphi \in \mathbb{C}^N$ and write $\varphi[k] = \varphi_k$. Then,

$$(z_0, z_1, \cdots, z_{N-1}) := \left(\frac{\varphi_1}{\varphi_0}, \frac{\varphi_2}{\varphi_1}, \cdots, \frac{\varphi_0}{\varphi_{N-1}} \right) \tag{2.1.29}$$

is a cyclic N-root. In fact, there is a one-to-one correspondence between cyclic N-roots and CAZAC sequences whose first entry is one [15]. Like with circulant Hadamard matrices, finding cyclic N-roots is equivalent to finding CAZAC sequences of length N. In particular, using (2.1.29) we can see that we can construct CAZAC sequences by the following (recursive) formula:

$$\forall k \in (\mathbb{Z}/N\mathbb{Z}),\ \varphi_0 = 1,\ \varphi_k = \varphi_{k-1} z_{k-1}. \tag{2.1.30}$$

Cyclic N-roots can be used to show that the number of prime length CAZACs is finite. This was proved by Haagerup [15], but we provide the part of the proof which shows the number of cyclic p-roots is finite in Section 2.4. This proof summary can also be found in [8].

Theorem 2.1.14. *For every prime number p, the set of cyclic p-roots in $\mathbb{C}^p$ is finite. Moreover the number of cyclic p-roots counted with multiplicity is equal to*

$$\binom{2p-2}{p-1} = \frac{(2p-2)!}{(p-1)!^2}. \tag{2.1.31}$$

In particular, the number of complex $p \times p$ circulant Hadamard matrices with diagonal entries equal to 1 is less than or equal to $(2p-2)!/(p-1)!^2$.

Another definition of equivalence, that was developed in [10], is the following. Two CAZAC sequences, φ and ψ, on $\mathbb{Z}/N\mathbb{Z}$, are defined to be *5-operation equivalent* if they can be obtained from one another by means of compositions of the five operations: rotation, translation, decimation, linear frequency modulation, and conjugation. These *5-equivalence operations* for CAZAC sequences are defined as follows for all $k \in \mathbb{Z}/N\mathbb{Z}$:

1. (Rotation) $\psi[k] = c\varphi[k]$, for some $|c| = 1$.

2. (Translation) $\psi[k] = \varphi[k-m]$, for some $m \in \mathbb{Z}/N\mathbb{Z}$.

3. (Decimation) $\psi[k] = \varphi[mk]$, for some $m \in \mathbb{Z}/N\mathbb{Z}$ for which $\gcd(m, N) = 1$.

4. (Linear Frequency Modulation) $\psi[k] = e^{2\pi i k\ell/N}\varphi[k]$, for some $\ell \in \mathbb{Z}/N\mathbb{Z}$.

5. (Conjugation) $\psi[k] = \overline{\varphi[k]}$.

Suppose two CAZAC sequences, x and y, defined on $\mathbb{Z}/N\mathbb{Z}$ have associated cyclic N-roots $\{z_k\}$ and $\{w_k\}$. It is straightforward to verify the following relations (stated for all $k \in \mathbb{Z}/N\mathbb{Z}$) between the 5-equivalence operations for CAZAC sequences, and how they become relations between cyclic N-roots.

1. $y[k] = cx[k] \Longrightarrow w_k = z_k$.

2. $y[k] = x[k-m] \Longrightarrow w_k = z_{k-m}$.

3. $y[k] = x[mk] \Longrightarrow w_k = \prod_{j=mk+1}^{mk+m} z_j$.

4. $y[k] = W_N^k x[k] \Longrightarrow w_k = W_N z_k$.

5. $y[k] = \overline{x[k]} \Longrightarrow w_k = \overline{z_k}$.

In particular, the 5-equivalence operations for CAZAC sequences give rise to operations under which cyclic N-roots are closed.

CAZAC sequences that are equivalent are also 5-operation equivalent. However, CAZAC sequences that are 5-operation equivalent may not be equivalent. The numbers in Table 2.1 and in Theorem 2.1.14 refer to the number of equivalent CAZAC sequences.

In practice, two CAZAC sequences, x and y, are not equivalent if $x[0] = y[0] = 1$, but $x[k] \neq y[k]$ for some $k > 0$. It is clearly more difficult to check if two CAZAC sequences are 5-operation equivalent than if they are equivalent. However, we will show in 2.2 that the 5-operation equivalence operations, written in the correct order, form a group action on the space of CAZAC sequences and we can simplify checking for 5-operation equivalence somewhat.

Additionally, there are questions about how these two notions of equivalence among CAZAC sequences relate to equivalence classes of the corresponding Hadamard matrices. It is not true that CAZAC sequences from two equivalent Hadamard matrices will be equivalent in the sense of the 5-equivalence operations.

2.2 CAZAC Sequences Generated by Roots of Unity

In this section we focus on CAZAC sequences which are generated by roots of unity. This first result leads to a lower bound for the number of cyclic p-roots which come from roots of unity.

Proposition 2.2.1. *Let p be an odd prime, and let $W_p = e^{2\pi i/p}$. If $s \in \{1, \cdots, p-1\}$ and $r \in \{1, \cdots, p\}$, then $(W_p^r, W_p^{r+s}, W_p^{r+2s}, \cdots, W_p^{r+(p-1)s})$ is a cyclic p-root.*

Proof. Given any cyclic p-root we can obtain another cyclic p-root by multiplying by W_p^r. In particular, we can assume without loss of generality that $r = 0$. Fix $s \in \{0, \cdots, p-1\}$. The t-th equation ($0 \leqslant t < p$) in the cyclic p-root system can be written as

$$\sum_{k=0}^{p-1} \prod_{\ell=0}^{t-1} z_{k+\ell} = 0 \tag{2.2.1}$$

so we would like to verify that

$$\sum_{k=0}^{p-1} \prod_{\ell=0}^{t-1} W_p^{s(k+\ell)} = 0. \tag{2.2.2}$$

To this end, we compute directly and obtain

$$\sum_{k=0}^{p-1} \prod_{\ell=0}^{t-1} W_p^{s(k+\ell)} = \sum_{k=0}^{p-1} W_p^{skt} \prod_{\ell=0}^{t-1} W_p^{s\ell} = \sum_{k=1}^{p-1} W_p^{skt} W_p^{s \sum_{\ell=0}^{t-1} \ell} = \sum_{k=1}^{p-1} W_p^{skt} W_p^{st(t-1)/2} \tag{2.2.3}$$

$$= W_p^{st(t-1)/2} \sum_{k=1}^{p-1} W_p^{skt} = 0, \tag{2.2.4}$$

since W_p^{st} is a primitive p-root of unity. For the last (p-th) equation we want to show

$$\prod_{k=0}^{p-1} W_p^{sk} = 1. \tag{2.2.5}$$

To verify this, we once again compute directly, and obtain

$$\prod_{k=0}^{p-1} W_p^{sk} = W_p^{s\sum_{k=0}^{p-1} k} = W_p^{sp(p-1)/2} = e^{s(p-1)\pi i} = 1, \tag{2.2.6}$$

since p is odd. Combining Equations (2.2.2) and (2.2.5) gives us that $(1, W_p^s, \cdots, W_p^{(p-1)s})$ is a cyclic p-root. □

Corollary 2.2.2. *The number of cyclic p-roots that are comprised of p-roots of unity is bounded below by $p(p-1)$.*

Proof. Each cylcic p-root in Proposition 2.2.1 is comprised of roots of unity. There are two parameters: s and r. Note that s can take up to $p-1$ different values, and r can take up to p different values. Thus, the number of possible cyclic p-roots that can be formed by Proposition 2.2.1 is $p(p-1)$. This gives us the desired lower bound. □

In particular, as a consequence of Corollary 2.2.2, all 20 cyclic 5-roots with modulus 1 are generated by Proposition 2.2.1. It is natural to speculate that all cyclic p-roots are given by Proposition 2.2.1, and that the lower bound $p(p-1)$ of Corollary 2.2.2 is the exact number of cyclic p-roots that are comprised of p-roots of unity.

We first would like to look at the specific case of cyclic 3-roots, which correspond to CAZAC sequences of length 3. In this case we are looking for solutions

$(x, y, z) \in \mathbb{C}^3$ to the system of equations,

$$\begin{cases} x + y + z = 0 \\ xy + yz + zx = 0 \\ xyz = 1. \end{cases} \tag{2.2.7}$$

This system is easily solvable in the following way. First, multiply the second equation in (2.2.7) by z. This yields

$$xyz + yz^2 + xz^2 = 0. \tag{2.2.8}$$

By factoring z in the last two terms on the left hand side and using the third equation in (2.2.7) we have

$$1 + z^2(x + y) = 0. \tag{2.2.9}$$

Rearranging the first equation in (2.2.7) gives us that $x + y = -z$. Substituting this into the above, we obtain

$$1 - z^3 = 0, \tag{2.2.10}$$

or, in other words, z must be a 3rd root of unity. Note that the same computations can also be applied to x and y, and thus x and y must also be 3rd roots of unity.

This leads to the conjecture that the 6 permutations of the 3rd roots of unity $(1, e^{2\pi i/3}, e^{4\pi i/3})$ indeed generate all 6 CAZAC sequences of length 3. Indeed if you write the sequence in $\mathbb{C}^N$ which corresponds to each root of unity, one can observe that it is indeed either one of the known roots of unity CAZAC sequence (e.g. Chu, P4, Wiener) or a 5-operation equivalence of one. To illustrate this we compute that the 6 permutations of the 3rd roots of unity are

1. $(1, e^{2\pi i/3}, e^{4\pi i/3})$

2. $(1, e^{4\pi i/3}, e^{2\pi i/3})$

3. $(e^{2\pi i/3}, 1, e^{4\pi i/3})$

4. $(e^{2\pi i/3}, e^{4\pi i/3}, 1)$

5. $(e^{4\pi i/3}, 1, e^{2\pi i/3})$

6. $(e^{4\pi i/3}, e^{2\pi i/3}, 1)$.

Using this, we can construct Table 2.2, listing all 6 CAZACs of length 3, see Figure 2.1.

Table 2.2: Cyclic 3-roots and CAZAC sequences of length 3

Cyclic 3-root	CAZAC sequence
$(1, e^{2\pi i/3}, e^{4\pi i/3})$	$(1, 1, e^{2\pi i/3})$
$(1, e^{4\pi i/3}, e^{2\pi i/3})$	$(1, 1, e^{4\pi i/3})$
$(e^{2\pi i/3}, 1, e^{4\pi i/3})$	$(1, e^{2\pi i/3}, e^{2\pi i/3})$
$(e^{2\pi i/3}, e^{4\pi i/3}, 1)$	$(1, e^{2\pi i/3}, 1)$
$(e^{4\pi i/3}, 1, e^{2\pi i/3})$	$(1, e^{4\pi i/3}, e^{4\pi i/3})$
$(e^{4\pi i/3}, e^{2\pi i/3}, 1)$	$(1, e^{4\pi i/3}, 1)$

In [19], [18], it is stated that all 3 × 3 Hadamard matrices are equivalent to the Fourier matrix. We shall use this result to compute all CAZAC sequences by finding their corresponding circulant Hadamard matrix. The website [18] further characterizes the set of 3×3 Hadamard matrices into two types:

$$\left\{ \begin{bmatrix} e^{ia} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{ic} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & W_3 & W_3^2 \\ 1 & W_3^2 & W_3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{ix} & 0 \\ 0 & 0 & e^{iy} \end{bmatrix} \right\} \bigcup$$

$$\left\{ \begin{bmatrix} e^{ia} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{ic} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & W_3^2 & W_3 \\ 1 & W_3 & W_3^2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{ix} & 0 \\ 0 & 0 & e^{iy} \end{bmatrix} \right\},$$

where $a, b, c, x, y \in [0, 2\pi)$ and $W_3 = e^{2\pi i/3}$. We shall use these two forms to find all 3×3 circulant Hadamard matrices.

First, we consider the first form and compute the matrix product:

$$\begin{bmatrix} e^{ia} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{ic} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & W_3 & W_3^2 \\ 1 & W_3^2 & W_3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{ix} & 0 \\ 0 & 0 & e^{iy} \end{bmatrix} = \begin{bmatrix} e^{ia} & e^{i(a+x)} & e^{i(a+y)} \\ e^{ib} & e^{i(b+x+\frac{2}{3}\pi)} & e^{i(b+y-\frac{2}{3}\pi)} \\ e^{ic} & e^{i(c+x-\frac{2}{3}\pi)} & e^{i(c+y+\frac{2}{3}\pi)} \end{bmatrix}. \tag{2.2.11}$$

In order for this matrix to be circulant, the following system of equations must hold mod 2π:

$$\begin{cases} a = b + x + \frac{2\pi}{3} = c + y + \frac{2\pi}{3} \\ c = a + x = b + y + \frac{4\pi}{3} \\ a + y = b = c + x + \frac{4\pi}{3}. \end{cases} \tag{2.2.12}$$

From the first equation in (2.2.12) we have

$$a = b + x + \frac{2}{3}\pi. \tag{2.2.13}$$

Using (2.2.13) in the second equation of (2.2.12), we calculate that

$$c = a + x = \left(b + x + \frac{2}{3}\pi\right) + x = b + 2x + \frac{2}{3}\pi. \tag{2.2.14}$$

From (2.2.13), (2.2.14), and the third equation of (2.2.12) we obtain,

$$y = c + x + \frac{4}{3}\pi - a = \left(b + 2x + \frac{2}{3}\pi\right) + x + \frac{4}{3}\pi - \left(b + x + \frac{2}{3}\pi\right) = 2x + \frac{4}{3}\pi. \tag{2.2.15}$$

Finally, returning to the first equation of (2.2.12) and using (2.2.14) and (2.2.15), we have

$$b = c + y - x = \left(b + 2x + \frac{2}{3}\pi\right) + \left(2x + \frac{4}{3}\pi\right) - x = b + 3x + 2\pi. \tag{2.2.16}$$

In particular, (2.2.16) implies that $3x \equiv 0 \bmod 2\pi$, i.e., x is $\frac{2}{3}\pi, 0$, or $-\frac{2}{3}\pi$. Letting $x = \frac{2}{3}\pi$, we obtain as one solution: $x = \frac{2}{3}\pi$, $a = \frac{4}{3}\pi + b$, $c = b$, and $y = \frac{2}{3}\pi$, where b is left indeterminate.

As such, we return to (2.2.11) and use this solution to compute

$$\begin{bmatrix} e^{i(\frac{4}{3}\pi+b)} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{ib} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & W_3 & W_3^2 \\ 1 & W_3^2 & W_3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{\frac{2}{3}\pi i} & 0 \\ 0 & 0 & e^{\frac{2}{3}\pi i} \end{bmatrix} = e^{ib} \begin{bmatrix} e^{-\frac{2}{3}\pi i} & 1 & 1 \\ 1 & e^{-\frac{2}{3}\pi i} & 1 \\ 1 & 1 & e^{-\frac{2}{3}\pi i} \end{bmatrix}.$$

The first row of the resulting circulant Hadamard matrix is $e^{ib}(e^{\frac{-2}{3}\pi i}, 1, 1)$. We let $b = \frac{2}{3}\pi$ and choose $(1, e^{\frac{2}{3}\pi i}, e^{\frac{2}{3}\pi i})$ as the representative for this class of CAZAC sequences and find our first CAZAC sequence.

As a second solution, we choose $x = 0$, which gives $a = \frac{2}{3}\pi + b$, $c = \frac{2}{3}\pi + b$, and $y = \frac{4}{3}\pi$, where b is again indeterminate. We return to (2.2.11) and compute,

$$\begin{bmatrix} e^{i(\frac{2}{3}\pi+b)} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{i(\frac{2}{3}\pi+b)} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & W_3 & W_3^2 \\ 1 & W_3^2 & W_3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & e^{\frac{4}{3}\pi i} \end{bmatrix} = e^{ib} \begin{bmatrix} e^{\frac{2}{3}\pi i} & e^{\frac{2}{3}\pi i} & 1 \\ 1 & e^{\frac{2}{3}\pi i} & e^{\frac{2}{3}\pi i} \\ e^{\frac{2}{3}\pi i} & 1 & e^{\frac{2}{3}\pi i} \end{bmatrix}.$$

The first row of this circulant Hadamard matrix is $e^{ib}(e^{\frac{2}{3}\pi i}, e^{\frac{2}{3}\pi i}, 1)$. Letting $b = -\frac{2}{3}\pi$, we have $(1, 1, e^{\frac{4}{3}\pi i})$ as our second CAZAC sequence.

The final solution is $x = -\frac{2}{3}\pi$, $a = b$, $c = b - \frac{2}{3}\pi$, and $y = 0$, where b is indeterminate. Returning to (2.2.11), we take

$$\begin{bmatrix} e^{ib} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{i(b-\frac{2}{3}\pi)} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & W_3 & W_3^2 \\ 1 & W_3^2 & W_3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{-\frac{2}{3}\pi i} & 0 \\ 0 & 0 & 1 \end{bmatrix} = e^{ib} \begin{bmatrix} 1 & e^{-\frac{2}{3}\pi i} & 1 \\ 1 & 1 & e^{-\frac{2}{3}\pi i} \\ e^{-\frac{2}{3}\pi i} & 1 & 1 \end{bmatrix}.$$

The first row of this circulant Hadamard matrix is $e^{ib}(1, e^{-\frac{2}{3}\pi i}, 1)$, and so letting $b = 0$, we have $(1, e^{\frac{4}{3}\pi i}, 1)$ as our third CAZAC sequence.

Now, we consider the second form of 3×3 Hadamard matrices in the union written at the beginning of this subsection, and take the product,

$$\begin{bmatrix} e^{ia} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{ic} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & W_3^2 & W_3 \\ 1 & W_3 & W_3^2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{ix} & 0 \\ 0 & 0 & e^{iy} \end{bmatrix} = \begin{bmatrix} e^{ia} & e^{i(a+x)} & e^{i(a+y)} \\ e^{ib} & e^{i(b+x-\frac{2}{3}\pi)} & e^{i(b+y+\frac{2}{3}\pi)} \\ e^{ic} & e^{i(c+x+\frac{2}{3}\pi)} & e^{i(c+y-\frac{2}{3}\pi)} \end{bmatrix}. \tag{2.2.17}$$

In order for the right hand side matrix to be circulant, the following equations must hold mod 2π:

$$\begin{cases} a = b + x + \frac{4\pi}{3} = c + y + \frac{4\pi}{3} \\ c = a + x = b + y + \frac{2\pi}{3} \\ a + y = b = c + x + \frac{2\pi}{3}. \end{cases} \tag{2.2.18}$$

Using the first equation in (2.2.18) we have

$$a = b + x + \frac{4}{3}\pi. \tag{2.2.19}$$

Next, using the second equation in (2.2.18) and as well as (2.2.19), we calculate that

$$c = a + x = \left(b + x + \frac{4}{3}\pi\right) + x = b + 2x + \frac{4}{3}\pi. \tag{2.2.20}$$

We now use the third equation in (2.2.18) along with (2.2.19) and (2.2.20), and obtain

$$y = c + x + \frac{2}{3}\pi - a = \left(b + 2x + \frac{4}{3}\pi\right) + x + \frac{2}{3}\pi - \left(b + x + \frac{4}{3}\pi\right) = 2x + \frac{2}{3}\pi \tag{2.2.21}$$

Finally, we return to the first equation of (2.2.18) and use (2.2.20) and (2.2.21) to compute

$$b = c + y - x = \left(b + 2x + \frac{4}{3}\pi\right) + \left(2x + \frac{2}{3}\pi\right) - x = b + 3x + 2\pi. \tag{2.2.22}$$

Similar to the previous calculations, (2.2.22) gives $3x \equiv 0 \bmod 2\pi$, or $x = \frac{2}{3}\pi$, $x = 0$, i.e., x is $0, \frac{2}{3}\pi$ or $-\frac{2}{3}\pi$.

Our first solution is $x = \frac{2}{3}\pi$, $a = b$, $c = b + \frac{2}{3}\pi$, and $y = 0$, where b is arbitrary. As such, we return to (2.2.17) and compute

$$\begin{bmatrix} e^{ib} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{i(b+\frac{2}{3}\pi)} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & W_3 & W_3^2 \\ 1 & W_3^2 & W_3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{\frac{2}{3}\pi} & 0 \\ 0 & 0 & 1 \end{bmatrix} = e^{ib} \begin{bmatrix} 1 & e^{\frac{2}{3}\pi i} & 1 \\ 1 & 1 & e^{\frac{2}{3}\pi i} \\ e^{\frac{2}{3}\pi i} & 1 & 1 \end{bmatrix}.$$

The first row of the resulting circulant Hadamard matrix is $e^{ib}(1, e^{\frac{2}{3}\pi i}, 1)$, and so letting $b = 0$ we obtain $(1, e^{\frac{2}{3}\pi i}, 1)$ as the fourth CAZAC sequence.

Our second solution is $x = 0$, $y = \frac{2}{3}\pi$, $a = b + \frac{4}{3}\pi$, and $c = b + \frac{4}{3}\pi$ where b is arbitrary. In this case, we take

$$\begin{bmatrix} e^{i(b+\frac{4}{3}\pi)} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{i(b+\frac{4}{3}\pi)} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & W_3 & W_3^2 \\ 1 & W_3^2 & W_3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & e^{\frac{2}{3}\pi} \end{bmatrix} = e^{ib} \begin{bmatrix} e^{-\frac{2}{3}\pi i} & e^{-\frac{2}{3}\pi i} & 1 \\ 1 & e^{-\frac{2}{3}\pi i} & e^{-\frac{2}{3}\pi i} \\ e^{-\frac{2}{3}\pi i} & 1 & e^{-\frac{2}{3}\pi i} \end{bmatrix}.$$

The first row of this circulant Hadamard matrix is $e^{ib}(e^{-\frac{2}{3}\pi i}, e^{-\frac{2}{3}\pi i}, 1)$, and so letting $b = \frac{2}{3}\pi$ we obtain $(1, 1, e^{\frac{2}{3}\pi i})$ as the fifth CAZAC sequence.

A third solution is $x = -\frac{2}{3}\pi$, $y = -\frac{2}{3}\pi$, $a = b + \frac{2}{3}\pi$, and $c = b$. We take

$$\begin{bmatrix} e^{i(b+\frac{2}{3}\pi)} & 0 & 0 \\ 0 & e^{ib} & 0 \\ 0 & 0 & e^{ib} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & W_3 & W_3^2 \\ 1 & W_3^2 & W_3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{-\frac{2}{3}\pi} & 0 \\ 0 & 0 & e^{-\frac{2}{3}\pi} \end{bmatrix} = e^{ib} \begin{bmatrix} e^{\frac{2}{3}\pi i} & 1 & 1 \\ 1 & e^{\frac{2}{3}\pi i} & 1 \\ 1 & 1 & e^{\frac{2}{3}\pi i} \end{bmatrix}.$$

The first row of this Hadamard matrix is $e^{ib}(e^{\frac{2}{3}\pi i}, 1, 1)$, and so letting $b = -\frac{2}{3}\pi$ we obtain $(1, e^{\frac{4}{3}\pi i}, e^{\frac{4}{3}\pi i})$ as the sixth and final CAZAC sequence.

To summarize, the six CAZAC sequences that we have obtained are:

$$(1, e^{2\pi i/3}, e^{2\pi i/3})$$

$$(1, 1, e^{4\pi i/3})$$

$$(1, e^{4\pi i/3}, 1)$$

$$(1, e^{2\pi i/3}, 1)$$

$$(1, 1, e^{2\pi i/3})$$

$$(1, e^{4\pi i/3}, e^{4\pi i/3});$$

and they are associated with the following circulant Hadamard matrices:

$$\begin{bmatrix} 1 & e^{2\pi i/3} & e^{2\pi i/3} \\ e^{2\pi i/3} & 1 & e^{2\pi i/3} \\ e^{2\pi i/3} & e^{2\pi i/3} & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & e^{4\pi i/3} \\ e^{4\pi i/3} & 1 & 1 \\ 1 & e^{4\pi i/3} & 1 \end{bmatrix}, \begin{bmatrix} 1 & e^{4\pi i/3} & 1 \\ 1 & 1 & e^{4\pi i/3} \\ e^{4\pi i/3} & 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & e^{2\pi i/3} & 1 \\ 1 & 1 & e^{2\pi i/3} \\ e^{2\pi i/3} & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & e^{2\pi i/3} \\ e^{2\pi i/3} & 1 & 1 \\ 1 & e^{2\pi i/3} & 1 \end{bmatrix}, \begin{bmatrix} 1 & e^{4\pi i/3} & e^{4\pi i/3} \\ e^{4\pi i/3} & 1 & e^{4\pi i/3} \\ e^{4\pi i/3} & e^{4\pi i/3} & 1 \end{bmatrix}.$$

Let p be prime. In this section we show that the 5-operation equivalence relation is an equivalence relation which is generated by a group G acting on $U_p^p \subseteq \mathbb{C}^p$, where U_p^p is the group of ordered p-tuples of p roots of unity. We now write the five operations again in the follwing way,

1. $c_1\varphi[n] = \overline{\varphi[n]}$ and $c_0\varphi[n] = \varphi[n]$.

2. $\tau_b\varphi[n] = \varphi[n-b]$, $b \in \mathbb{Z}/p\mathbb{Z}$.

3. $\pi_c\varphi[n] = \varphi[cn]$, $c \in \mathbb{Z}/p\mathbb{Z}$, $c \neq 0$.

4. $e_d\varphi[n] = e^{2\pi i dn/p}\varphi[n]$, $d \in \mathbb{Z}/p\mathbb{Z}$.

5. $\omega_f\varphi[n] = e^{2\pi i f/p}\varphi[n]$, $f \in \mathbb{Z}/p\mathbb{Z}$.

With this we can define the set G by

$$G = \{(a,b,c,d,f) : a \in \{0,1\},\ b,c,d,f \in \mathbb{Z}/p\mathbb{Z},\ c \neq 0\} \tag{2.2.23}$$

which has size $|G| = 2p^3(p{-}1)$. To each element $(a, b, c, d, f) \in G$ we associate the operator $\omega_f e_d \pi_c \tau_b c_a$. To motivate the group operation we take $(a, b, c, d, f), (h, j, k, \ell, m) \in G$. One can show that the composition of the associated operators is

$$(\omega_m e_\ell \pi_k \tau_j c_h) \circ (\omega_f e_d \pi_c \tau_b c_a) = \omega_{m+(-1)^h(f-jc)} e_{\ell+(-1)^h kd} \pi_{ck} \tau_{cj+b} c_{a+h} \tag{2.2.24}$$

As such we write define the operation $\cdot : G \times G \to G$ by

$$(a, b, c, d, f)\cdot(h, j, k, \ell, m) = (a{+}h, cj{+}b, ck, \ell{+}(-1)^h kd, m{+}(-1)^h(f{-}jc)). \tag{2.2.25}$$

Theorem 2.2.3. *The operation $\cdot$ defines a group operation for G. In particular, $(G, \cdot)$ is a group.*

Proof. We need to show that the operation is associative, has an identity element, and that each element has an inverse. It is easily verified that the identity element is $(0, 0, 1, 0, 0)$. Given an element $(a, b, c, d, f) \in G$, it is elementary to verify that

$$(a, b, c, d, f)^{-1} = (-a, -bc^{-1}, c^{-1}, (-1)^{-a+1}c^{-1}d, (-1)^{-a+1}(f + bc^{-1}d)) \tag{2.2.26}$$

Finally, for associativity we first compute

$$(v, w, x, y, z) \cdot ((a, b, c, d, f) \cdot (h, j, k, \ell, m)) \tag{2.2.27}$$

$$= (v, w, x, y, z) \cdot (a + h, cj + b, ck, \ell + (-1)^h kd, m + (-1)^h(f - jc)) \tag{2.2.28}$$

$$= (a + h + v, cjx + bx + w, ckx, \ell + (-1)^h kd + (-1)^{a+h}cky, \tag{2.2.29}$$

$$m + (-1)^h(f - jc) + (-1)^{a+h}(z - cjx - bx)) \tag{2.2.30}$$

On the other hand if we compute

$$((v, w, x, y, z) \cdot (a, b, c, d, f)) \cdot (h, j, k, \ell, m) \tag{2.2.31}$$

$$= (a + v, bx + w, cx, d + (-1)^a cy, f + (-1)^a (z - bx)) \cdot (h, j, k, \ell, m) \tag{2.2.32}$$

$$= (a + h + v, cxj + bx + w, ckx, \ell + (-1)^h kd + (-1)^{a+h} kcy, \tag{2.2.33}$$

$$m + (-1)^h (f - jc) + (-1)^{a+h} (z - cjx - bx)) \tag{2.2.34}$$

and we see that $\cdot$ is an associative operation. □

Since $(G, \cdot)$ is a group, it defines a proper group action on U_p^p. There are $p(p-1)$ many CAZAC sequences which start with 1 in U_p^p. Adding in direct scalars by elements in U_p^p, there are $p^2(p-1)$ CAZACs in U_p^p.

Theorem 2.2.4. *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 has size $p^2(p-1)$ if $p \equiv 3 \mod 4$.*

Proof. First, let $(a, b, c, d, f) \in G$, $\omega = e^{2\pi i/p}$ and note that

$$(\omega_f e_d \pi_c \tau_b c_a)(\varphi)[n] = \omega^{f+dn} c_a \varphi[cn - b] = \omega^{f+dn+(-1)^a s(cn-b)^2}. \tag{2.2.35}$$

Setting $n = 0$ gives the condition that for $(a, b, c, d, f) \in G$,

$$f + (-1)^a sb^2 \equiv 0 \mod p \tag{2.2.36}$$

from which we conclude that

$$f \equiv -(-1)^a sb^2 \mod p. \tag{2.2.37}$$

Setting $n = 1$ and subtituting (2.2.37) for f gives us another condition

$$(-1)^a s(c - b)^2 + d - (-1)^a sb^2 \equiv s \mod p. \tag{2.2.38}$$

From (2.2.38) we can solve for d to obtain

$$d \equiv s + (-1)^a s(2bc - c^2) \mod p. \tag{2.2.39}$$

Now, note for any other $n > 1$, we can substitute (2.2.37) and (2.2.39) in and obtain the equation

$$(-1)^a s(nc - b)^2 + n + (-1)^a s(2bc - c^2)n - (-1)^a sb^2 \equiv sn^2 \mod p. \tag{2.2.40}$$

After expanding and cancelling terms, we can reduce (2.2.40) to

$$c^2 \equiv (-1)^a \mod p. \tag{2.2.41}$$

If $a = 0$, then (2.2.41) has two solutions, which we will denote c_0^+ and c_0^-. If $a = 1$, then by the law of quadratic reciprocity, (2.2.41) has two solutions, c_1^+ and c_1^-, if $p \equiv 1 \mod 4$, but no solutions if $p \equiv 3 \mod 4$. Thus, if $p \equiv 3 \mod 4$, we get as stabilizers of φ,

1. $(0, b, c_0^+, 1 + 2bc_0^+ - (c_0^+)^2, -b^2)$

2. $(0, b, c_0^-, 1 + 2bc_0^- - (c_0^-)^2, -b^2)$

where the above holds for any $b \in \mathbb{Z}/p\mathbb{Z}$. If $p \equiv 1 \mod 4$, then the first two sets of stabilizers also hold in addition to

1. $(0, b, c_1^+, 1 + 2bc_1^+ - (c_1^+)^2, -b^2)$

2. $(0, b, c_1^-, 1 + 2bc_1^- - (c_1^-)^2, -b^2)$

where again any $b \in \mathbb{Z}/p\mathbb{Z}$ is valid. Thus, if $p \equiv 1 \mod 4$ there are $4p$ stabilizers for φ, and if $p \equiv 3 \mod 4$ there are $2p$ stabilizers for φ. □

Corollary 2.2.5. *If $p \equiv 3 \mod 4$, there is only one equivalence class of CAZACs in U_p^p.*

Theorem 2.2.6. *Let $p \equiv 1 \mod 4$, and $\varphi, \psi \in \mathbb{C}^N$. Let $\varphi = e^{2\pi i n^2/p}$ and $\psi = e^{2\pi i s n^2/p}$ where s is not a quadratic residue modulo p. Then φ and ψ belong to different 5-operation equivalence classes.*

Proof. Let $s = 1$ in the proof of Theorem 2.2.4 and for $(a, b, c, d, f) \in G$ and $\omega = e^{2\pi i/p}$ we have

$$(\omega_f e_d \pi_c \tau_b c_a)(\varphi)[n] = \omega^{f+dn} c_a \varphi[cn - b] = \omega^{f+dn+(-1)^a(cn-b)^2}. \tag{2.2.42}$$

Emulating the proof of Theorem 2.2.4, we let $n = 0$ and get the condition

$$f \equiv -(-1)^a b^2 \mod p. \tag{2.2.43}$$

Now letting $n = 1$ we get the condition

$$d \equiv s + (-1)^a(2bc - c^2) \mod p \tag{2.2.44}$$

Now for a general $n > 1$, we have

$$(-1)^a(nc - b)^2 + sn + (-1)^a(2bc - c^2)n - (-1)^a b^2 \equiv sn^2 \mod p \tag{2.2.45}$$

After expanding and cancelling terms we obtain

$$c^2 \equiv (-1)^a s \mod p. \tag{2.2.46}$$

Since $p \equiv 1 \mod 4$ and s is not a residue modulo p, (2.2) cannot be solved for either value of a. Thus, φ and ψ must belong to different equivalence classes. □

Corollary 2.2.7. *If $p \equiv 1 \mod 5$, then there are exactly two equivalence classes of CAZACs in U_p^p both of which have size $p^2(p-1)/2$.*

We now apply these results to the $p = 3$ and $p = 5$ cases to illustrate these results with a concrete exmaple. We first show explicitly there is only one 5-operation equivalence class for length 3 CAZAC sequences. Indeed, suppose that $\varphi = (1, 1, e^{2\pi i/3})$, i.e. the Chu sequence. Then, the other five CAZAC sequences can be obtained from 5-operation equivalency as follows:

1. $c_1\varphi = (1, 1, e^{4\pi i/3})$

2. $e_1c_1\varphi = (1, e^{2\pi i/3}, e^{2\pi i/3})$

3. $e_1\varphi = (1, e^{2\pi i/3}, 1)$

4. $e_2\varphi = (1, e^{4\pi i/3}, e^{4\pi i/3})$

5. $e_2c_1\varphi = (1, e^{4\pi i/3}, 1)$

Corollary 2.2.7 tells us that there are two 5-operation equivalence classes in the case $p = 5$. To explicitly write them, first we start with the Wiener sequence, $\varphi = (1, e^{2\pi i/5}, e^{8\pi i/5}, e^{8\pi i/5}, e^{2\pi i/5})$,. We then show that we can get 10 CAZAC sequences by applying 5-operation equivalencies to φ:

1. $\varphi = (1, e^{2\pi i/5}, e^{8\pi i/5}, e^{8\pi i/5}, e^{2\pi i/5})$

2. $c_1\varphi = (1, e^{8\pi i/5}, e^{2\pi i/5}, e^{2\pi i/5}, e^{8\pi i/5})$

3. $\omega_1\tau_1c_1\varphi = (1, e^{2\pi i/5}, 1, e^{4\pi i/5}, e^{4\pi i/5})$

4. $\omega_4 \tau_1 \varphi = (1, e^{8\pi i/5}, 1, e^{6\pi i/5}, e^{6\pi i/5})$

5. $\omega_4 \tau_2 c_1 \varphi = (1, e^{6\pi i/5}, e^{8\pi i/5}, e^{6\pi i/5}, 1)$

6. $\omega_1 \tau_2 \varphi = (1, e^{4\pi i/5}, e^{2\pi i/5}, e^{4\pi i/5}, 1)$

7. $\omega_4 \tau_3 c_1 \varphi = (1, 1, e^{6\pi i/5}, e^{8\pi i/5}, e^{6\pi i/5})$

8. $\omega_1 \tau_3 \varphi = (1, 1, e^{4\pi i/5}, e^{2\pi i/5}, e^{4\pi i/5})$

9. $\omega_1 \tau_4 c_1 \varphi = (1, e^{4\pi i/5}, e^{4\pi i/5}, 1, e^{2\pi i/5})$

10. $\omega_4 \tau_4 \varphi = (1, e^{6\pi i/5}, e^{6\pi i/5}, 1, e^{8\pi i/5})$

To get the other orbit, we use the fact that 3 is not a quadratic residue modulo 5 and apply Theorem 2.2.6. We now let φ be the Wiener sequence where $s = 3$, i.e. $\varphi = (1, e^{6\pi i/5}, e^{4\pi i/5}, e^{4\pi i/5}, e^{6\pi i/5})$.

1. $\varphi = (1, e^{6\pi i/5}, e^{4\pi i/5}, e^{4\pi i/5}, e^{6\pi i/5})$

2. $c_1 \varphi = (1, e^{4\pi i/5}, e^{6\pi i/5}, e^{6\pi i/5}, e^{4\pi i/5})$

3. $\omega_3 \tau_1 c_1 \varphi = (1, e^{6\pi i/5}, 1, e^{2\pi i/5}, e^{2\pi i/5})$

4. $\omega_2 \tau_1 \varphi = (1, e^{4\pi i/5}, 1, e^{8\pi i/5}, e^{8\pi i/5})$

5. $\omega_2 \tau_2 c_1 \varphi = (1, e^{8\pi i/5}, e^{4\pi i/5}, e^{8\pi i/5}, 1)$

6. $\omega_3 \tau_2 \varphi = (1, e^{2\pi i/5}, e^{6\pi i/5}, e^{2\pi i/5}, 1)$

7. $\omega_2 \tau_3 c_1 \varphi = (1, 1, e^{8\pi i/5}, e^{4\pi i/5}, e^{8\pi i/5})$

8. $\omega_3 \tau_3 \varphi = (1, 1, e^{2\pi i/5}, e^{6\pi i/5}, e^{2\pi i/5})$

9. $\omega_3\tau_4\varphi = (1, e^{2\pi i/5}, e^{2\pi i/5}, 1, e^{6\pi i/5})$

10. $\omega_2\tau_4\varphi = (1, e^{8\pi i/5}, e^{8\pi i/5}, 1, e^{4\pi i/5})$

In conclusion, we have explicitly shown that the $p = 3$ case has exactly one orbit and shown which 5-operation transformations generate them starting with the Chu sequence. In the $p = 5$ case we have also explicitly shown that there are two orbits under 5-operation equivalence, generated both orbits entirely using two different base Wiener sequences, and written out which 5-operation transformations generate them.

2.3 CAZAC Sequences Not Generated by Roots of Unity

Here we discuss CAZAC sequences which are not generated by roots of unity. The primary example here is the Björck sequence.

Definition 2.3.1. Let p be prime. The *Legendre symbol* is defined by

$$\left(\frac{k}{p}\right) = \begin{cases} 0, & \text{if } k \equiv 0 \mod p \\ 1, & \text{if } k \equiv n^2 \mod p \text{ for some } n \not\equiv 0 \mod p \\ -1, & \text{otherwise.} \end{cases}$$

Definition 2.3.2. Let p be prime and let $\varphi \in \mathbb{C}^p$ be of the following form,

$$\varphi[k] = e^{i\theta[k]}. \tag{2.3.1}$$

We define the *Björck sequence* by letting $\theta[k]$ in (2.3.1) be as follows,

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

$$\theta[k] = \left(\frac{k}{p}\right) \arccos\left(\frac{1}{1+\sqrt{p}}\right). \tag{2.3.2}$$

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

$$\theta[k] = \begin{cases} \arccos\left(\frac{1-p}{1+p}\right), & \text{if } \left(\frac{k}{p}\right) = -1 \\ 0 & \text{otherwise.} \end{cases} \tag{2.3.3}$$

Figure 2.3.1 shows that for $p = 11$, the Björck sequence is indeed a CAZAC sequence. The Björck sequence is also CAZAC for any other prime length, p [20]. In this particular example, one can see that the discrete periodic ambiguity function of

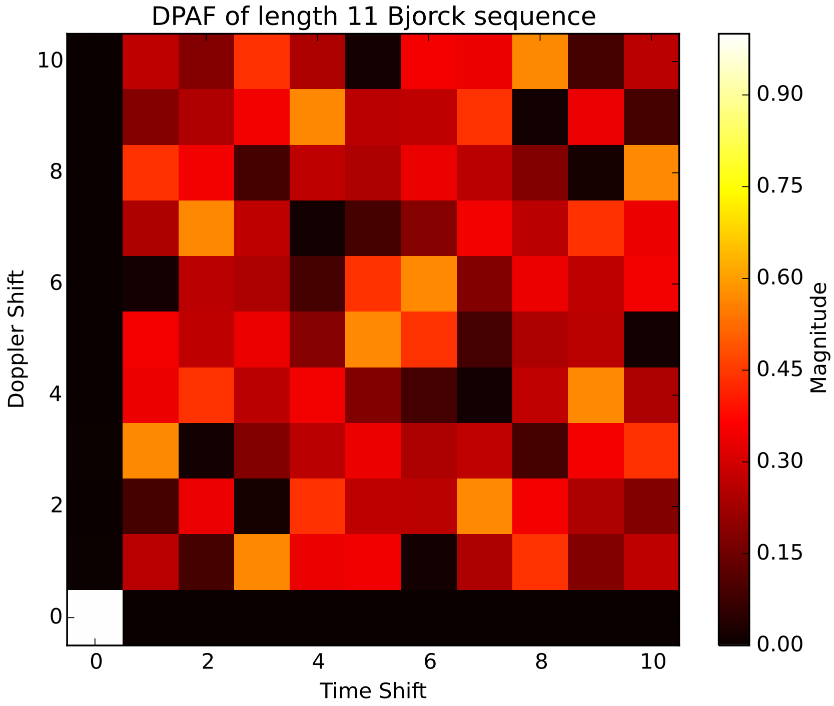

Figure 2.3.1: DPAF of length 11 Björck sequence.

the length 11 Björck sequence is almost always nonzero, except for $A_p(\varphi)[\cdot, 0]$ and $A_p(\varphi)[0, \cdot]$. This holds for any Björck sequence of any prime length, $p \geqslant 7$. More detailed exploration on the behavior of the DPAF of the Björck sequence can be found in [21] and [22]. For completeness, the length 11 Björck sequence is listed out below,

$$\varphi = (1, 1, e^{i\theta_{11}}, 1, 1, 1, e^{i\theta_{11}}, e^{i\theta_{11}}, e^{i\theta_{11}}, 1, e^{i\theta_{11}}), \tag{2.3.4}$$

where $\theta_{11} = \arccos(-10/11)$.

If we consider $p \times p$ Hadamard matrices, where p is prime, we want to know if the Hadamard matrices generated by CAZAC sequences are always equivalent to $\mathcal{D}_p$, the $p \times p$ DFT matrix. If $p = 2, 3, 5$, then we have already noted that all Hadamard matrices are equivalent to $\mathcal{D}_p$, regardless of whether or not they are generated by a CAZAC sequence [18].

If $p = 7$, then Björck's example shows that there are Hadamard matrices not equivalent to $\mathcal{D}_7$ [18]. One such Hadamard matrix H_1 is defined as follows. Let $\theta = \arccos(-3/4)$ and let $d = \exp(i\theta)$, and set

$$H_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & d^{-1} & 1 & d & d^{-1} & d & 1 \\ 1 & d^{-1} & d^{-1} & d & 1 & 1 & d \\ 1 & d^{-2} & d^{-2} & d^{-1} & d^{-1} & 1 & d^{-1} \\ 1 & 1 & d^{-1} & 1 & d^{-1} & d & d \\ 1 & d^{-2} & d^{-1} & d^{-1} & d^{-2} & d^{-1} & 1 \\ 1 & d^{-1} & d^{-2} & 1 & d^{-2} & d^{-1} & d^{-1} \end{bmatrix},$$

[18], [23]. To continue the process, let $P_1 = P_2 = Id_7$ and D_1, D_2 be the following matrices,

$$D_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & d & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & d & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & d \end{bmatrix}, \qquad D_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & d & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & d & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & d & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Then we can define an equivalent circulant Hadamard matrix H_2 by

$$H_2 = D_1 H_1 D_2 = \begin{bmatrix} 1 & d & d & 1 & d & 1 & 1 \\ 1 & 1 & d & d & 1 & d & 1 \\ 1 & 1 & 1 & d & d & 1 & d \\ d & 1 & 1 & 1 & d & d & 1 \\ 1 & d & 1 & 1 & 1 & d & d \\ d & 1 & d & 1 & 1 & 1 & d \\ d & d & 1 & d & 1 & 1 & 1 \end{bmatrix}.$$

In particular, the first column of H_2 is the length 7 Björck sequence and so H_2 is the Hadamard matrix associated with the length 7 Björck sequence.

Another matrix, that is equivalent to neither $\mathcal{D}_7$ nor H_1, is

$$J_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a^{-2} & a^{-1}b^{-1} & a^{-1}c^{-1} & a^{-1} & a^{-1}c & a^{-1}b \\ 1 & a^{-1}b^{-1} & a^{-2}b^{-2} & a^{-1}b^{-2}c^{-1} & a^{-1}b^{-1}c^{-1} & a^{-1}b^{-1}c & a^{-1}c \\ 1 & a^{-1}c^{-1} & a^{-1}b^{-2}c^{-1} & a^{-2}b^{-2}c^{-2} & a^{-1}b^{-2}c^{-2} & a^{-1}b^{-1}c^{-1} & a^{-1} \\ 1 & a^{-1} & a^{-1}b^{-1}c^{-1} & a^{-1}b^{-2}c^{-2} & a^{-2}b^{-2}c^{-2} & a^{-1}b^{-2}c^{-1} & a^{-1}c^{-1} \\ 1 & a^{-1}c & a^{-1}b^{-1}c & a^{-1}b^{-1}c^{-1} & a^{-1}b^{-2}c^{-1} & a^{-2}b^{-2} & a^{-1}b^{-1} \\ 1 & a^{-1}b & a^{-1}c & a^{-1} & a^{-1}c^{-1} & a^{-1}b^{-1} & a^{-2} \end{bmatrix},$$

where $a \approx \exp(4.312839i), b \approx \exp(1.356228i), c \approx \exp(1.900668i)$, see [24], [18], The parameters, a, b, and c, are algebraic numbers whose explicit values can be found in [24]. We can put these two matrices in circulant form by multiplying J_1

on the left and right by the matrix,

$$D = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & ab & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & abc & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & abc & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & ab & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & a \end{bmatrix}.$$

Carrying out the multiplication, the circulant form of J_1, denoted as J_2, can be written as

$$J_2 = DJ_1D = \begin{bmatrix} 1 & a & ab & abc & abc & ab & a \\ a & 1 & a & ab & abc & abc & ab \\ ab & a & 1 & a & ab & abc & abc \\ abc & ab & a & 1 & a & ab & abc \\ abc & abc & ab & a & 1 & a & ab \\ ab & abc & abc & ab & a & 1 & a \\ a & ab & abc & abc & ab & a & 1 \end{bmatrix}.$$

2.4 Haagerup's Theorem

We shall now outline that part Haagerup's proof of his Theorem 2.1.14 [15], in which he proves that there are only finitely many cyclic p-roots. The complete proof in which the precise number of cyclic p-roots is computed requires sophisticated complex analysis that is beyond the scope of our theme.

At the risk of oversimplifying, the proof that there are only finitely many cyclic p-roots is divided in two parts: an ingenious algebraic manipulation using the DFT, coupled with an application of the uncertainty principle for $\mathbb{Z}/p\mathbb{Z}$.

Recall that cyclic N-roots are solutions $z = (z_0, \ldots, z_{N-1}) \in \mathbb{C}^N$, of the system of equations:

$$\begin{cases} z_0 + z_1 + \cdots + z_{N-1} = 0 \\ z_0z_1 + z_1z_2 + \cdots + z_{N-1}z_0 = 0 \\ \qquad\qquad \ldots \\ z_0z_1\cdots z_{N-2} + \cdots + z_{N-1}z_0\cdots z_{N-3} = 0 \\ z_0z_1\cdots z_{N-1} = 1, \end{cases} \tag{2.4.1}$$

see Definition 2.1.13. In particular, because of the last equation of (2.4.1), $z_j \in \mathbb{C}^\times = \mathbb{C}\backslash\{0\}$ for any cyclic N-root $z \in \mathbb{C}^N$. Haagerup makes several substitutions to transform (2.4.1).

First, assume $z \in \mathbb{C}^N$ is a cyclic N-root. Let $x_0 = 1$ and $x_j = z_0z_1\cdots z_{j-1}$ for all $j = 1, \ldots, N-1$, and set $x_0 = 1$. Thus, $x_{j+1}/x_j = z_j$ for $j = 0, \ldots, N-2$, where the last equation of (2.4.1) guarantees that x_{j+1}/x_j is well-defined. Further, for $j = N-1$,

$$\frac{x_0}{x_{N-1}} = \frac{1}{z_0 z_1 \cdots z_{N-2}} = z_{N-1}, \tag{2.4.2}$$

and because $z_0 z_1 \cdots z_{N-1} = 1$ by the last equation of (2.4.1). Substituting these equations, that relate the x_j and z_i, into (2.4.1) we see that $x = (x_0, \ldots, x_{N-1})$ is a solution to the system,

$$\begin{cases} x_0 = 1 \\ \frac{x_1}{x_0} + \frac{x_2}{x_1} + \ldots + \frac{x_0}{x_{N-1}} = 0 \\ \frac{x_2}{x_0} + \frac{x_3}{x_1} + \ldots + \frac{x_1}{x_{N-1}} = 0 \\ \qquad\qquad \cdots \\ \frac{x_{N-1}}{x_0} + \frac{x_0}{x_1} + \ldots + \frac{x_{N-2}}{x_{N-1}} = 0. \end{cases} \tag{2.4.3}$$

Conversely, if $x = (x_0, \ldots, x_{N-1}) \in (\mathbb{C}^\times)^N$ is a solution to the system (2.4.3), then it is easy to check that

$$z = (z_0, \ldots, z_{N-1}) = \left(\frac{x_1}{x_0}, \frac{x_2}{x_1}, \ldots, \frac{x_0}{x_{N-1}} \right) \in (\mathbb{C}^\times)^N \tag{2.4.4}$$

is a solution to (2.4.1). Haagerup says that solutions x to (2.4.3) are *cyclic N-roots on the x-level.*

Second, assume $x = (x_0, \ldots, x_{N-1}) \in (\mathbb{C}^\times)^N$ is a cyclic N-root on the x-level. Let $y_j = 1/x_j$, for $j = 0, \ldots, N-1$. Then,

$$(x, y) = (x_0, \ldots, x_{N-1}, y_0, \ldots, y_{N-1}) \in (\mathbb{C}^\times)^N \times (\mathbb{C}^\times)^N \tag{2.4.5}$$

is a solution to the system,

$$\begin{cases} x_0 = y_0 = 1, \\ x_k y_k = 1, 1 \leqslant k \leqslant N-1, \\ \sum_{m=0}^{N-1} x_{k+m} y_m = 0, 1 \leqslant k \leqslant N-1. \end{cases} \tag{2.4.6}$$

Conversely, if $(x, y) \in \mathbb{C}^N \times \mathbb{C}^N$ is solution to (2.4.6), then, noting the condition, $x_k y_k = 1$ of (2.4.6), it is easy to check that $x \in (\mathbb{C}^\times)^N$ and that x is a solution to (2.4.3). Haagerup says solutions $(x, y) \in \mathbb{C}^N \times \mathbb{C}^N$ to (2.4.6) are *cyclic N-roots on the (x, y)-level*.

Third, Haagerup introduces the DFT into the mix, and proves that the system of equations (2.4.6) for the cyclic N-roots on the (x, y)-level are equivalent to the following system of equations for $(x, y) \in \mathbb{C}^N \times \mathbb{C}^N$:

$$\begin{cases} x_0 = y_0 = 1 \\ x_m y_m = 1, 1 \leqslant m \leqslant N-1 \\ \widehat{x}_n \widehat{y}_{-n} = 1, 1 \leqslant n \leqslant N-1. \end{cases} \tag{2.4.7}$$

Without providing the details, we see how the third equation of (2.4.7) is deduced from (2.4.6) by writing out the product $\widehat{x}_n \widehat{y}_{-n}$.

Since we began recording these equivalences with cyclic N-roots $z = (z_0, \ldots, z_N)$ as defined in Section 2.1 we wrote $x_m, \widehat{x}_n$ in (2.4.7), but this is really $x[m], \widehat{x}[n]$ in the notation for sequences we used for CAZACs.

None of the details in this subsection is difficult to prove, *but* Haagerup's strategy is dazzling! The transformations from the cyclic N-roots problem (2.4.1) to that of (2.4.7) preserve the number of distinct solutions, and so solving (2.4.7) is equivalent to solving (2.4.1), viz., if there are $0 \leqslant M \leqslant \infty$ solutions to one, then there are $0 \leqslant M \leqslant \infty$ solutions to the other. As such, Haagerup's proof that the set of cyclic p-roots is finite will be to solve (2.4.7).

In order to prove that the set of cyclic p-roots is finite (Theorem 2.4.5), Haagerup's strategy required Theorem 2.4.2 and Theorem 2.4.4. Theorem 2.4.2 is an uncertainty principle for the finite Abelian group $\mathbb{Z}/p\mathbb{Z}$, where p is prime. Its proof uses Chebotarëv's theorem, a fact known to Hagerup in 1996. We should point out that Gabidulin also understood the role of Chebotarëv's theorem if one were going to prove Theorem 2.4.5.

Theorem 2.4.1. *(Chebotarëv 1926) Let p be prime and let $\mathcal{D}_p$ be the unitary Fourier matrix on $\mathbb{C}^p$, defined as*

$$\mathcal{D}_N = \left[\frac{1}{N^{1/2}} W_N^{-mn} \right]_{m,n=0}^{N-1}, \tag{2.4.8}$$

see Definition 2.1.1. Then, all square submatrices of $\mathcal{D}_p$ have non-zero determinant.

There have been many different proofs of this theorem since Chebotarëv's original proof in 1926. A sampling of authors of published proofs is Danilevskii (1937), Reshetnyak (1955), Dieudonné (1970), M. Newman (1975), Evans and I. Stark (1977), Stevenhagen and Lenstra (1996), Goldstein, Guralnick, and Isaacs (c. 2004), and Tao (2005). There is also the proof by Frenkel (2004), that he first wrote down as a solution to a problem in the 1998 Schweitzer Competition! In fact, Chebotarëv's original proof provides much more information than Theorem 2.4.1 asserts, see [25].

Further, [25] is also a spectacular exposition of Chebotarëv's life and mathematical contributions, including his celebrated density theorem.

Independently, Tao [26] used Theorem 2.4.1 in order to prove Theorem 2.4.2. He also noted that the two results are equivalent, a fact discovered independently by András Biró. Theorem 2.4.2 itself is a refinement for the setting of $\mathbb{Z}/p\mathbb{Z}$ of the uncertainty principle inequality,

$$|\mathrm{supp}(u)|\,|\mathrm{supp}(\widehat{u})| \geqslant |G|, \tag{2.4.9}$$

where G is a finite Abelian group, $u : G \longrightarrow \mathbb{C}$ is a function, $\widehat{u}$ is the discrete Fourier transform of u, $|X|$ is the cardinality of X, and $\mathrm{supp}(u) = \{x \in G : u(x) \neq 0\}$ is the *support* of u, see [27] for a systematic treatment of the discrete Fourier transform. The inequality, (2.4.9), is due to Donoho and Stark [28], cf., [29]

Theorem 2.4.2. *If $u \neq 0 \in \mathbb{C}^p$ and $\widehat{u} = \mathcal{F}_p u$ is the discrete Fourier transform of u, then $|\mathrm{supp}(u)| + |\mathrm{supp}(\widehat{u})| \geqslant p + 1$, where $|\mathrm{supp}(u)|$, the support of u, denotes the number of non-zero coordinates of u.*

Algebraic varieties are a central object of study in algebraic geometry. Classically, and for us, an *algebraic variety* is defined as the set of solutions of a system of polynomial equations over the real or complex numbers. The following is a basic theorem.

Theorem 2.4.3. *A compact algebraic variety in $\mathbb{C}^N$ is a finite set, e.g., see [30], Theorem 13.3.*

Theorem 2.4.4. *Given $n \in \mathbb{N}$. If the number of solutions $(x, y) \in \mathbb{C}^n \times \mathbb{C}^n$ to (2.4.7) is infinite, then there are $u, v \in \mathbb{C}^n \backslash \{0\}$ such that $u_k v_k = 0$ and $\widehat{u}_k \widehat{v}_{-k} = 0$.*

Proof. Suppose there are infinitely many solutions to (2.4.7) and let $W \subseteq \mathbb{C}^N \times \mathbb{C}^N$ denote the set of solutions to (2.4.7). Since W is an algebraic variety, by both Theorem 2.4.3 and the Heine-Borel theorem, W must be unbounded. Pick a sequence $\{(x^{(m)}, y^{(m)})\}$ in W with

$$\lim_{m\to\infty} (||x^{(m)}||_2^2 + ||y^{(m)}||_2^2)^{1/2} = \infty. \tag{2.4.10}$$

Let $u^{(m)}$ and $y^{(m)}$ be the normalizations of $x^{(m)}$ and $y^{(m)}$, respectively. We get a sequence $\{(u^{(m)}, v^{(m)})\}$ in a compact set. Say that this sequence converges to (u, v), passing to a subsequence if necessary. Because each $(x^{(m)}, y^{(m)})$ is a solution to (2.4.7), $x_0^{(m)} = y_0^{(m)} = 1$ for all $m \in \mathbb{N}$. Thus $||x^m||_2^2 = 1 + c_m$ and $||y^{(m)}||_2^2 = 1 + d_m$, where $c_m, d_m > 0$. It follows that

$$||x^{(m)}||_2^2||y^{(m)}||_2^2 = (1+c_m)(1+d_m) \geqslant 1 + c_m + d_m = ||x^{(m)}||_2^2 + ||y^{(m)}||_2^2 - 1. \tag{2.4.11}$$

Thus, by our choice of $(x^{(m)}, y^{(m)})$,

$$\lim_{m\to\infty} ||x^{(m)}||_2^2||y^{(m)}||_2^2 = \infty. \tag{2.4.12}$$

Now, from (2.4.7), we know that $x_k^{(m)}y_k^{(m)} = \widehat{x^{(m)}}_k\widehat{y^{(m)}}_{-k} = 1$, and so $u_k v_k = \hat{u}_k\hat{v}_{-k} = \lim_{m\to\infty}(||x^{(m)}||_2||y^{(m)}||_2)^{-1}$ for $1 \leqslant k \leqslant n-1$. We can also say that $x_0^{(m)}y_0^{(m)} = \widehat{x_0^{(m)}}\widehat{y_0^{(m)}} = 1$ because $x_0^{(m)} = y_0^{(m)} = 1$. Since

$$\lim_{m\to\infty} ||x^{(m)}||_2||y^{(m)}||_2 = \infty, \tag{2.4.13}$$

we now have that $u_k v_k = \hat{u}_k\hat{v}_{-k} = 0$. □

Theorem 2.4.5. *(Haagerup) The set of cyclic p-roots is finite.*

Proof. Assume for the sake of obtaining a contradiction that the set of solutions to (2.4.7) is infinite. Then, by Theorem 2.4.4, there are $u, v \in \mathbb{C}^p\backslash\{0\}$ with $u_k v_k = 0$ and $\widehat{u}_k \widehat{v}_{-k} = 0$, $k = 0, 1, \ldots, p-1$.

This means that $\operatorname{supp}(u) \cap \operatorname{supp}(v) = \varnothing$ and $\operatorname{supp}(\widehat{u}) \cap (-\operatorname{supp}(\widehat{v})) = \varnothing$. In particular, we obtain $|\operatorname{supp}(u)| + |\operatorname{supp}(v)| \leqslant p$ and $|\operatorname{supp}(\widehat{u})| + |\operatorname{supp}(\hat{v})| \leqslant p$; and so,

$$|\operatorname{supp}(u)| + |\operatorname{supp}(v)| + |\operatorname{supp}(\widehat{u})| + |\operatorname{supp}(\widehat{v})| \leqslant 2p. \tag{2.4.14}$$

However, by Theorem 2.4.2, we have

$$|\operatorname{supp}(u)| + |\operatorname{supp}(v)| + |\operatorname{supp}(\widehat{u})| + |\operatorname{supp}(\widehat{v})| \geqslant 2(p+1), \tag{2.4.15}$$

and this gives the desired contradiction. □

Chapter 3: Applications of CAZAC Sequences to Tight Gabor Frames

3.1 Gabor Frames

Frames were introduced in 1952 by Duffin and Schaeffer [31] for their work on nonharmonic Fourier series. They used frames to compute the coefficients of a linear combination of vectors which spanned its Hilbert space, but were linearly dependent. Since then, frames have been used in applications such as the analysis of wavelets, and in signal and image processing [32–36]. Frames can be viewed as a generalization of orthonormal bases for Hilbert spaces. In the context of signal processing, the primary advantage of frames is that they provide stable representations of signals which are robust in the presense of erasures and noise [37,38]. We focus our attention on finite frames, i.e., frames on a finite dimensional Hilbert space, $\mathcal{H}$. Finite frames are of particular interest for engineering and computational applications, see [39–42].

Definition 3.1.1. Let $\mathcal{H}$ be an N-dimensional Hilbert space and let $\mathcal{F} = \{f_1, f_2, \cdots, f_M\} \subseteq \mathcal{H}$. We say that $\mathcal{F}$ is a *frame* for $\mathcal{H}$ if there exists $A, B > 0$ such that

$$A\|x\|_{\mathcal{H}}^2 \leqslant \sum_{k=1}^{M} |\langle x, f_k\rangle_{\mathcal{H}}|^2 \leqslant B\|x\|_{\mathcal{H}}^2 \tag{3.1.1}$$

for any $x \in \mathcal{H}$. If $A = B$ is possible, then we say $\mathcal{F}$ is a *tight frame.*

Tight frames are particularly desirable as it makes computing the inverse of the frame operator (Definition 3.1.3) very easy and allows for simple reconstruction of vectors given frame elments. This has motivates research into the discovery and construction of tight frames [43–47], as well as the transformation of frames into tight frames [48]. In the finite dimensional setting, we have the following lemma which gives an alternate, equivalent definition of a frame.

Lemma 3.1.2. *Let $\mathcal{H}$ be an n-dimensional Hilbert space and $\mathcal{F} \subset \mathcal{H}$. $\mathcal{F}$ is a frame for $\mathcal{H}$ if and only if $\mathcal{F}$ spans $\mathcal{H}$.*

Recall that part of the definition of a basis for a vector space is that the basis spans the vector space. In particular, given the right coefficients, one can construct any vector in the vector space as a linear combination of the basis set. Since frames span its Hilbert space, we should be able to do the same with frames. The following definitions and theorem shows how this is accopmlished.

Definition 3.1.3. Let $\mathcal{F} = \{f_1, \cdots, f_m\}$ be a frame for $\mathcal{H}$. The *analysis operator* of $\mathcal{F}$, $T : \mathcal{H} \to \mathbb{C}^m$, is defined by

$$T(x) = \{\langle x, f_k \rangle\}_{k=1}^{m}. \tag{3.1.2}$$

Its adjoint operator, $T^* : \mathbb{C}^m \to \mathcal{H}$, is called the *synthesis operator*, and is defined by

$$T^*(c) = \sum_{k=1}^{m} c_k f_k. \tag{3.1.3}$$

Finally, we define the *frame operator*, $S : \mathcal{H} \to \mathcal{H}$, by $S = T^*T$, i.e.

$$S(x) = \sum_{k=1}^{m} \langle x, f_k \rangle f_k. \tag{3.1.4}$$

Note that S is a self-adjoint operator since $S^* = (T^*T)^* = T^*T^{**} = T^*T = S$. Using this we obtain the reconstruction formula below.

Theorem 3.1.4. *Let $\mathcal{F} = \{f_1, \cdots, f_m\}$ be a frame for $\mathcal{H}$ and let $x \in \mathcal{H}$. Then,*

$$x = \sum_{k=1}^{m} \langle x, f_k \rangle S^{-1} f_k = \sum_{k=1}^{m} \langle x, S^{-1} f_k \rangle f_k. \tag{3.1.5}$$

Proof. The first equality comes immediately from applying the definition of S to $S^{-1}Sf$. For second equality we compute,

$$f = SS^{-1}f = \sum_{k=1}^{M} \langle S^{-1}x, f_k \rangle f_k = \sum_{k=1}^{M} \langle x, S^{-1} f_k \rangle f_k \tag{3.1.6}$$

where the last equality comes from the fact that S^{-1} is self-adjoint.

Although Theorem 3.1.4 does allow any vector in $\mathcal{H}$ to be reconstructed with frame elements, there is a computational drawback in that it requires that the inverse of S needs to be computed. If $\mathcal{F}$ is a tight frame, then $S = AId$, and the inverse is simple to compute. If $\mathcal{F}$ cannot be made into a tight frame, then one way around this difficulty is to use what is known as a *dual frame* to $\mathcal{F}$, which is given by the following definition.

Definition 3.1.5. Let $\mathcal{G} = \{g_k\}_{k=1}^{M} \subseteq \mathcal{H}$. $\mathcal{G}$ is a *dual frame* to $\mathcal{F}$ if,

$$\forall x \in \mathcal{H}, \; x = \sum_{k=1}^{M} \langle x, g_k \rangle f_k. \tag{3.1.7}$$

The reconstruction formula gives us one such $\mathcal{G}$. That is, $\mathcal{G} = \{S^{-1}f_k\} \subseteq \mathcal{H}$ is a dual frame to $\mathcal{F}$. This particular dual frame is called the *canonical dual frame* to $\mathcal{F}$.

Given a frame, the frame operator is defined by applying the analysis operator, then the synthesis operator, in that order. We can apply these operators in the reverse order, i.e. synthesis, and then analysis, to get a new operator. This operator is called the *Gram operator* and is defined by the following definition.

Definition 3.1.6. Let $\mathcal{F} = \{f_1, \cdots, f_M\}$ be a frame for $\mathcal{H}$. We define the *Gram operator*, $G : \mathbb{C}^M \to \mathbb{C}^M$, by

$$G(c) = \left\{ \sum_{i=1}^{M} \langle c_i f_i, f_j \rangle \right\}_{j=1}^{M}. \tag{3.1.8}$$

In particular, the *Gram matrix*, i.e. the matrix associated with linear operator G, can be written as

$$G_{i,j} = \langle f_i, f_j \rangle. \tag{3.1.9}$$

If we let $\mathcal{H} = \mathbb{C}^N$ then we can represent the analysis operator T as an $M \times N$ matrix where each row is represented by one of the $f_k \in \mathcal{F}$. In particular this allows for a matrix representation of S to be formed. The following theorem determines when a set of vectors gives a frame by looking at the eigenvalues of the proposed frame operator.

Theorem 3.1.7. *Let S be the frame operator associated to a set of vectors $\mathcal{F}$. Then, $\mathcal{F}$ is a frame if and only if all eigenvalues of S are nonzero.*

One particular area of interest within frame theory is that of Gabor frames, i.e. frames which consist of translations and modulations of a given generator vector in $\mathcal{H}$. This section is designed to give a quick overview of relevant concepts in Gabor frame theory that will be required. Deeper expositions can be found in [42, 49, 50]. We will only deal with the finite Hilbert space $\mathcal{H} = \mathbb{C}^N$.

Definition 3.1.8. Let $\varphi \in \mathbb{C}^N$ and let $\Lambda \subseteq \mathbb{Z}/N\mathbb{Z} \times (\mathbb{Z}/N\mathbb{Z})\hat{}$. We define the *Gabor system*, (φ, Λ), by

$$(\varphi, \Lambda) = \{e_\ell \tau_k \varphi : (k, \ell) \in \Lambda\}. \tag{3.1.10}$$

If (φ, Λ) forms a frame for $\mathbb{C}^N$, then we say that (φ, Λ) is a *Gabor frame* for $\mathbb{C}^N$.

Related to the idea of Gabor frames is that of the discrete short-time Fourier transform. The discrete Fourier transform, by itself, gives the exact frequency content of a signal $\varphi \in \mathbb{C}^N$. However, in this processes, one loses all temporal information in the sense that one cannot say at what times the signal observes these frequencies. A tempting problem is that of trying to analyze a signal to see which frequencies occur at exactly what time. To express this as a physical example, one could imagine trying to analyze a piece of music to determine which notes (frequencies) are played at which time. As it turns out, such methods are impossible in general due to the Heisenberg uncertainty principle. Simply stated, it says that it is impossible to have perfect resolution in time and frequency simultaneously.

Although it is impossible to say exactly which frequencies are contained in an instant in time, we can still get an idea of what frequencies are contained in a certain period of time by restricting our function to a "window" of time and analyzing the frequencies in that window. This idea is encapsulated by the discrete short-time Fourier transform, defined below.

Definition 3.1.9. Let $\varphi \in \mathbb{C}^N$. The *discrete short-time Fourier transform* (STFT) of φ with respect to window function $\psi \in \mathbb{C}^N$ is defined by

$$V_\psi(\varphi)[m, n] = \langle \varphi, e_n \tau_m \psi \rangle = \sum_{k=0}^{N-1} \varphi[k] \overline{\psi[k-m]} e^{-2\pi i n k/N} = (\varphi \tau_m(\overline{\psi}))\hat{}\,[n].$$

The inversion formula is given by

$$\varphi[k] = \frac{1}{N\|\psi\|_2^2} \sum_{n=0}^{N-1} \sum_{m=0}^{N-1} V_\psi(\varphi)[m,n] e_n \tau_m \psi.$$

We can connect this to Gabor frames by using φ itself as a window function. In particular, we can use the inversion formula to show that if one uses the full product group $\mathbb{Z}/N\mathbb{Z} \times (\mathbb{Z}/N\mathbb{Z})\hat{}$ one always gets a tight frame, regardless of the choice of φ (as long as it is not the zero vector).

Theorem 3.1.10. *Let $\varphi \in \mathbb{C}^N \backslash \{0\}$ and let $\Lambda = (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})\hat{}$. Then, the Gabor system (φ, Λ) is a tight frame with frame bound $N\|\varphi\|_2^2$.*

Proof. For every $x \in \mathbb{C}^N$ we compute $S(x)$,

$$S(x) = \sum_{n=0}^{N-1} \sum_{m=0}^{N-1} \langle x, e_n \tau_m \varphi \rangle e_n \tau_m \varphi = \sum_{n=0}^{N-1} \sum_{m=0}^{N-1} V_\varphi(x)[m,n] e_n \tau_m \varphi = N\|\varphi\|_2^2 x. \blacksquare$$

Although Theorem 3.1.10 does give tight frames, smaller tight Gabor frames would require less coefficients when analyzing signals, and smaller representations of those signals would be possible. Thus, in general, it is of interest to study Gabor frames which do not consist of all time-frequency translates of the generator.

The set of time-frequency operators themselves also can be made to form a group. To see this first we make the following computation,

$$e_b \tau_a e_\ell \tau_k \varphi[j] = (e_b \tau_a)(e^{2\pi i \ell j/N} \varphi[j-k]) = e^{2\pi i b j/N} e^{2\pi i \ell (j-a)/N} \varphi[j-k-a] \quad (3.1.11)$$

$$= e^{-2\pi i a \ell/N} e^{2\pi i (b+\ell) j/N} \varphi[j-k-a] = e^{-2\pi i a\ell/N} e_{b+\ell} \tau_{a+k} \varphi[j]. \quad (3.1.12)$$

Now, let $\omega_N = e^{2\pi i/N}$, and we can now write the above as

$$\omega_N^c e_b \tau_a \omega_N^m e_\ell \tau_k \varphi = \omega_N^{c+m-a\ell} e_{b+\ell} \tau_{a+k} \varphi \quad (3.1.13)$$

and can now define the following binary operation, $\cdot : (\mathbb{Z}/N\mathbb{Z})^3 \times (\mathbb{Z}/N\mathbb{Z})^3 \to (\mathbb{Z}/N\mathbb{Z})^3$ by

$$(a, b, c) \cdot (k, \ell, m) = (a + k, b + \ell, c + m - a\ell). \tag{3.1.14}$$

Definition 3.1.11. The group $((\mathbb{Z}/N\mathbb{Z})^3, \cdot)$, with $\cdot$ as defined by (3.1.14), is called the *Heisenberg group*. Each $(k, \ell, m) \in (\mathbb{Z}/N\mathbb{Z})^3$ corresponds to the time-frequency operator $\omega_N^m e_\ell \tau_k$ and $\cdot$ corresponds to the composition of the time-frequency operators (applying the left term first).

3.2 Tight Gabor Frames from Sparse Ambiguity Functions

The main result of this section, Theorem 3.2.7, can be summarized as: Gabor systems are tight frames if the discrete periodic ambiguity functions of their generating functions are sufficently sparse. To prove this we use Janssen's representation. Janssen's representation allows us to write the frame operator as a linear combination of time-frequency operators whose coefficients can be computed without knowing the input of the frame operator, cf. Walnut's representation [50] [51]. We also draw connections between the discrete periodic ambiguity function and short-time Fourier transform, as well as Theorem 3.2.7 and the Wexler-Raz theorem. For more details on frame theroy, [42] is a valuable resource. We begin by defining the discrete periodic ambiguity function.

Definition 3.2.1. Let $\varphi \in \mathbb{C}^N$. The *discrete periodic ambiguity function* (DPAF) of φ is the function $A_p(\varphi) : (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})\hat{} \to \mathbb{C}$ defined by

$$A_p(\varphi)[m,n] = \frac{1}{N}\sum_{k=0}^{N-1} \varphi[k+m]\overline{\varphi[k]}e^{-2\pi i n k/N} = \frac{1}{N}\langle \tau_{-m}\varphi, e_n\varphi\rangle. \tag{3.2.1}$$

We only provide a proof of Janssen's representation in the case $(\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})\hat{}$, but it can be proven in the more general setting of $G \times \widehat{G}$, where G is a finite abelian group and $\widehat{G}$ is the corresponding character group. A proof of this version can be found in [50]. To setup the proof of Janssen's representation, we first prove the following lemma.

Lemma 3.2.2. *For* $(k,\ell), (m,n) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})\hat{}$*, we have that*

$$e_\ell \tau_k e_n \tau_m = e^{-2\pi i k n/N} e_{\ell+n}\tau_{k+m} = e^{2\pi i (m\ell - kn)/N} e_n \tau_m e_\ell \tau_k \tag{3.2.2}$$

and

$$(e_\ell \tau_k)^{-1} = (e_\ell \tau_k)^* = e^{-2\pi i k\ell/N} e_{-\ell}\tau_{-k}. \tag{3.2.3}$$

Proof. We show both (3.2.2) and (3.2.3) by direct computation. Let $\varphi \in \mathbb{C}^N$. Then,

$$e_\ell \tau_k e_n \tau_m \varphi[j] = e_\ell \tau_k (e^{2\pi i n j/N}\ \varphi[j-k]) = e^{2\pi i \ell j/N} e^{2\pi i n(j-k)/N} \varphi[j-k-m] \tag{3.2.4}$$

$$= e^{-2\pi i k n/N} e_{\ell+n}\tau_{k+m}\varphi. \tag{3.2.5}$$

Switching the roles of (k,ℓ) and (m,n) in (3.2.4) and (3.2.5), we have that

$$e_n \tau_m e_\ell \tau_k \varphi = e^{-2\pi i \ell m/n} e_{\ell+n}\tau_{k+m}\varphi. \tag{3.2.6}$$

Thus, if we multiply both sides of (3.2.6) by $e^{2\pi i(m\ell - kn)/N}$, we get (3.2.5) and thus the left and right most parts of (3.2.2) are equated. For (3.2.3), it is sufficient to apply (3.2.2) to (k,ℓ) and $(-k,-\ell)$. □

Related to Lemma 3.2.2, we will also need the following definition, which is used in the statement of Janssen's represenatation. Janssen's representation uses the *adjoint subgroup* of a subgroup $\Lambda \subseteq (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})\hat{}$ to represent the frame operator without the input function.

Definition 3.2.3. Let $\Lambda \subseteq (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})\hat{}$ be a subgroup. The *adjoint subgroup*, Λ°, is the group given by $\Lambda^\circ = \{(m,n) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})\hat{} : e_n\tau_m e_\ell \tau_k = e_\ell\tau_k e_n \tau_m, \forall (k,\ell) \in \Lambda\}$. That is, Λ° generates all time-frequency operators which commute with all time-frequency operators generated by Λ.

Theorem 3.2.4 (Janssen)**.** *Let Λ be a subgroup of $(\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})\hat{}$ and Λ° be the adjoint subgroup of Λ. Let $\varphi, \psi \in \mathbb{C}^N \backslash \{0\}$. Then,*

$$\forall x \in \mathbb{C}^N, \quad \sum_{(k,\ell)\in\Lambda} \langle x, e_\ell\tau_k\varphi\rangle e_\ell\tau_k\psi = \frac{|\Lambda|}{N} \sum_{(m,n)\in\Lambda^\circ} \langle \psi, e_n\tau_m\varphi\rangle e_n\tau_m x. \tag{3.2.7}$$

Moreover, the Gabor frame operator of the Gabor system (φ, Λ) *can be written as*

$$S = \frac{|\Lambda|}{N} \sum_{(m,n)\in\Lambda^\circ} \langle e_n \tau_m \varphi, \varphi \rangle e_n \tau_m. \tag{3.2.8}$$

Proof. First, recall Theorem 3.2.5 which states that $\{1/\sqrt{N} e_\ell \tau_k\}_{(k,\ell)\in(\mathbb{Z}/N\mathbb{Z})\times(\mathbb{Z}/N\mathbb{Z})\hat{}}$ forms an orthonormal basis for the space of linear operators on $\mathbb{C}^N$ equpped with the Hilbert-Schmidt inner product. Hence for $\varphi, \psi \in \mathbb{C}^N$, the operator $S : \mathbb{C}^N \to \mathbb{C}^N$ given by

$$S(x) = \sum_{(k,\ell)\in\Lambda} \langle x, e_\ell \tau_k \varphi \rangle e_\ell \tau_k \psi \tag{3.2.9}$$

has a unique representation,

$$S = \sum_{n=1}^{N} \sum_{m=1}^{N} c_{m,n} e_n \tau_m. \tag{3.2.10}$$

Now applying (3.2.3) from Lemma 3.2.2 to (3.2.9) gives that for any $(k, \ell) \in \Lambda$,

$$\sum_{n=1}^{N} \sum_{m=1}^{N} c_{m,n} e_n \tau_m = S = (e_\ell \tau_k)^{-1} S e_\ell \tau_k = \sum_{n=1}^{N} \sum_{m=1}^{N} c_{m,n} (e_\ell \tau_k)^{-1} e_n \tau_m e_\ell \tau_k. \tag{3.2.11}$$

Equation (3.2.2) in Lemma 3.2.2 implies that $(e_\ell \tau_k)^{-1} e_n \tau_m e_\ell \tau_k$ is a scalar multiple of $e_n \tau_m$. Since the coefficients $c_{m,n}$ are unique, we have that either $c_{m,n} = 0$ or $(e_\ell \tau_k)^{-1} e_n \tau_m e_\ell tau_k = e_n \tau_m$. The latter option is exactly the condition that $(m, n) \in \Lambda^\circ$ and we conclude that $c_{m,n} = 0$ if $(m, n) \notin \Lambda^\circ$.

It remains to show that for $(m, n) \in \Lambda^\circ$, we have that $c_{m,n} = |\Lambda|/N \langle \psi, e_n \tau_m \varphi \rangle$. First, note that the operator $x \mapsto \langle x, \varphi \rangle \psi$ is represented by the matrix $\psi \varphi^*$. Furthermore, its Hilbert-Schmidt prodcut with another matrix M satisfies $\langle \psi \varphi^*, M \rangle_{HS} = \langle \psi, M \varphi \rangle$. Thus, for $(m, n) \in \Lambda^\circ$,

$$c_{m,n} = \frac{1}{N} \langle S, e_n \tau_m \rangle_{HS} = \frac{1}{N} \sum_{(k,\ell)\in\Lambda} \langle e_\ell \tau_k \psi (e_\ell \tau_k \varphi)^*, e_n \tau_m \rangle \tag{3.2.12}$$

$$= \frac{1}{N} \sum_{(k,\ell)\in\Lambda} \langle e_\ell \tau_k \psi, e_n \tau_m e_\ell \tau_k \varphi \rangle = \frac{1}{N} \sum_{(k,\ell)\in\Lambda} \langle e_\ell \tau_k \psi, e_\ell \tau_k e_n \tau_m \varphi \rangle \tag{3.2.13}$$

$$= \frac{1}{N} \sum_{(k,\ell)\in\Lambda} \langle \psi, e_n \tau_m \varphi \rangle = \frac{|\Lambda|}{N} \langle \psi, e_n \tau_m \varphi \rangle. \tag{3.2.14}$$

□

To prove Theorem 3.2.7 we require one more theorem. The space of linear operators on $\mathbb{C}^N$ forms an N^2-dimensional space. Moreover, given any orthonormal basis $\{e_i\}_{i=1}^N$, we can define the *Hilbert-Schmidt inner product* of two linear operators A, B by

$$\langle A, B \rangle_{HS} = \sum_{i=1}^{N} \sum_{j=1}^{N} \langle Ae_i, e_j \rangle \langle Be_i, e_j \rangle. \tag{3.2.15}$$

The Hilbert-Schimdt inner product is independent of choice of orthonormal basis. We call the space of linear operators on $\mathbb{C}^N$ equipped with the Hilbert-Schmidt inner product the *Hilbert-Schmidt space.* With this in mind, Theorem 3.2.5 is given without proof, but a proof can be found in [50].

Theorem 3.2.5. *The set of normalized time frequency translates* $\{\frac{1}{\sqrt{N}} e_\ell \tau_k : (k, \ell) \in (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})\hat{}\}$ *forms an orthonormal basis for the* N^2*-dimensional Hilbert-Schmidt space of linear operators on* $\mathbb{C}^N$*.*

Last, we introduce the notion of $A_p(\varphi)$ being Λ°-sparse. Theorem 3.2.7 will show that this is both a sufficient and necessary condition for the tightness of Gabor frames.

Definition 3.2.6. Let $\varphi \in \mathbb{C}^N$ and $\Lambda \subseteq (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})\hat{}$ be a subgroup. $A_p(\varphi)$ is Λ°*-sparse* if for every $(m, n) \in \Lambda^\circ \backslash \{(0, 0)\}$ we have that $A_p(\varphi)[m, n] = 0$.

Theorem 3.2.7. *Let $\varphi \in \mathbb{C}^N \backslash \{0\}$ and let $\Lambda \subseteq \mathbb{Z}/N\mathbb{Z} \times (\mathbb{Z}/N\mathbb{Z})\hat{}$ be a subgroup. (φ, Λ) is a tight frame if and only if $A_p(\varphi)$ is Λ°-sparse. Moreover, the frame bound is given by $|\Lambda| A_p(\varphi)[0,0]$.*

Proof. By Janssen's representation and using the definition of $A_p(\varphi)$ we have

$$S = \frac{|\Lambda|}{N} \sum_{(k,\ell) \in \Lambda^\circ} \langle e_\ell \tau_k \varphi, \varphi \rangle e_\ell \tau_k = \frac{|\Lambda|}{N} \sum_{(k,\ell) \in \Lambda^\circ} \langle \tau_k \varphi, e_{-\ell} \varphi \rangle e_\ell \tau_k \tag{3.2.16}$$

$$= |\Lambda| \sum_{(k,\ell) \in \Lambda^\circ} A_p(\varphi)[-k, -\ell] e_\ell \tau_k = |\Lambda| \sum_{(k,\ell) \in \Lambda^\circ} A_p(\varphi)[k, \ell] e_{-\ell} \tau_{-k} \tag{3.2.17}$$

The last equality comes from re-indexing by replacing (k, ℓ) with $(-k, -\ell)$ and using the fact that Λ° is a subgroup of $(\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})\hat{}$. Clearly, if $A_p(\varphi)$ is Λ°-sparse, then by (3.2.17) the frame operator will be $|\Lambda| A_p(\varphi)[0,0]$ times the identity. It remains to show that $A_p(\varphi)$ is a necessary condition. For S to be tight we need

$$S = |\Lambda| \sum_{(k,\ell) \in \Lambda^\circ} A_p(\varphi)[k, \ell] e_\ell \tau_k = A\, Id. \tag{3.2.18}$$

In particular, we can rewrite (3.2.18) to

$$\sum_{(k,\ell) \in \Lambda^\circ \backslash \{(0,0)\}} |\Lambda| A_p(\varphi)[k, \ell] e_\ell \tau_k + (|\Lambda| A_p(\varphi)[0,0] - A) Id = 0. \tag{3.2.19}$$

By Theorem 3.2.5, the set of linear operators $\{e_\ell \tau_k : (k, \ell) \in \Lambda^\circ\}$ is linearly independent. Thus, $A_p(\varphi)[k, \ell] = 0$ for every $(k, \ell) \in \Lambda^\circ \backslash \{(0,0)\}$ and $A = |\Lambda| A_p(\varphi)[0,0]$. We conclude that, $A_p(\varphi)$ is Λ°-sparse and the frame has the desired frame bound. □

Theorem 3.2.7 is closely connected to the Wexler-Raz criterion. The Wexler-Raz criterion checks whether a Gabor system $(\tilde{\varphi}, \Lambda)$ is a dual frame to another Gabor system, (φ, Λ). Every frame (φ, Λ) has at least one dual frame, $(S^{-1}\varphi, \Lambda)$, and this is known as its canonical dual frame. Theorem 3.2.7 is a special case of Wexler-Raz which confirms that the canonical dual frame associated with tight frames indeed satisfies the Wexler-Raz criterion. Again, a proof is not given but can be found in [50].

Theorem 3.2.8 (Wexler-Raz)**.** *Let Λ be a subgroup of $(\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})\hat{}$. For Gabor systems (φ, Λ) and $(\tilde{\varphi}, \Lambda)$ we have*

$$x = \sum_{(k,\ell)\in\Lambda} \langle x, e_\ell \tau_k \tilde{\varphi} \rangle e_\ell \tau_k \varphi, \qquad x \in \mathbb{C}^N, \tag{3.2.20}$$

if and only if

$$\langle \varphi, e_\ell \tau_k \tilde{\varphi} \rangle = \frac{N}{|\Lambda|} \delta_{(k,\ell),(0,0)}, \qquad (k,\ell) \in \Lambda^\circ. \tag{3.2.21}$$

If (φ, Λ) is a tight frame, then the cannonical dual frame to (φ, Λ) is $(A^{-1}\varphi, \Lambda)$, since $S^{-1} = A^{-1}Id$. Using the Wexler-Raz criteron and using that $A = |\Lambda| A_p(\varphi)[0,0]$ as in Theorem 3.2.7, then (3.2.20) holds if and only if,

$$\frac{1}{|\Lambda| A_p(\varphi)[0,0]} \langle \varphi, e_\ell \tau_k \varphi \rangle = \frac{N}{|\Lambda|} = \delta_{(k,\ell),(0,0)}, \qquad (k,\ell) \in \Lambda^\circ. \tag{3.2.22}$$

This can be rewritten as

$$A_p(\varphi)[k,\ell] = A_p(\varphi)[0,0]\delta_{(k,\ell),(0,0)} \quad (k,\ell) \in \Lambda^\circ. \tag{3.2.23}$$

This is the same condition as $A_p(\varphi)$ being Λ°-sparse.

We close this section with a few operations on φ which preservere the Λ°-sparsity of the ambiguity function.

Proposition 3.2.9. *Let $\varphi \in \mathbb{C}^N \backslash \{0\}$ and let $\Lambda \subseteq \mathbb{Z}/N\mathbb{Z} \times (\mathbb{Z}/N\mathbb{Z})\hat{}$ be a subgroup. Suppose that $A_p(\varphi)$ is Λ°-sparse. Then the following are also Λ°- sparse:*

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

(ii) $\forall \ell \in (\mathbb{Z}/N\mathbb{Z})\hat{},\ A_p(e_\ell\varphi)$

(iii) $\forall c \in \mathbb{C}\backslash\{0\},\ A_p(c\varphi)$

(iv) $A_p(\overline{\varphi})$.

Proof. Each part follows quickly from the left equality in (3.2.2). For each $(m,n) \in \Lambda^\circ$ we compute:

(i) Let $k \in (\mathbb{Z}/N\mathbb{Z})$. Then,

$$\langle \tau_{-m}\tau_k\varphi, e_n\tau_k\varphi\rangle = \langle \tau_{-m}\varphi, e_0\tau_{-k}e_n\tau_k\varphi\rangle = \langle \tau_{-m}\varphi, e_n\varphi\rangle = 0. \tag{3.2.24}$$

(ii) Let $\ell \in (\mathbb{Z}/N\mathbb{Z})\hat{}$. Then,

$$\langle \tau_{-m}e_\ell\varphi, e_ne_\ell\varphi\rangle = \langle e_{-n-\ell}\tau_{-m}e_\ell\tau_0\varphi, \varphi\rangle = e^{-2\pi i\ell m/N}\langle e_{-n}\tau_{-m}\varphi, \varphi\rangle \tag{3.2.25}$$

$$= e^{-2\pi i\ell m/N}\langle \tau_{-m}\varphi, e_n\varphi\rangle = 0. \tag{3.2.26}$$

(iii) Let $c \in \mathbb{C}\backslash\{0\}$. Then,

$$\langle \tau_{-m}c\varphi, e_nc\varphi\rangle = |c|^2\langle \tau_{-m}\varphi, e_n\varphi\rangle = 0. \tag{3.2.27}$$

(iv) We compute,

$$\langle \tau_{-m}\overline{\varphi}, e_n\overline{\varphi}\rangle = \langle e_n\varphi, \tau_{-m}\varphi\rangle = \langle \tau_me_n\varphi, \varphi\rangle = e^{-2\pi imn/N}\langle e_n\tau_m\varphi, \varphi\rangle \tag{3.2.28}$$

$$= e^{2\pi imn/N}\langle \tau_m\varphi, e_{-n}\varphi\rangle = 0, \tag{3.2.29}$$

since the product group inverse of (m,n), i.e., $(-m,-n)$, is in Λ°.

□

3.3 Tight Gabor Frames via CAZACS: Sparse AF Method

For most of the examples, we will use the following formulation of subgroup Λ: Let $K = \langle a \rangle$ and $L = \langle b \rangle$ where $N = abN'$ and $\gcd(a, b) = 1$. That is, K is the subgroup of $(\mathbb{Z}/N\mathbb{Z})$ generated by a: $\langle a \rangle = \{0, a, \cdots, (bN' - 1)a\}$ and L is the subgroup of $(\mathbb{Z}/N\mathbb{Z})\hat{}$ generated by b: $\langle b \rangle = \{0, b, \cdots, (aN' - 1)b\}$. Let $\Lambda = K \times L$. We first shall compute the adjoint subgroup of $\Lambda = K \times L$. This requires us to compute which time-frequency translates $e_n\tau_m$ commute with every time-frequency translate $e_\ell \tau_k$ with $(k, \ell) \in K \times L$. To that end, let $e_\ell\tau_k$ with $(k, \ell) \in K \times L$, and $e_n\tau_m$ be two time-frequency translates. We noted in Proposition 3.2.9 that $e_n\tau_m e_\ell\tau_k = e^{-2\pi i \ell m/N} e_{\ell+n}\tau_{k+m}$. Switching k and m, as well as ℓ and n, we have $e_\ell\tau_k e_n\tau_m = e^{-2\pi i kn/N} e_{\ell+n}\tau_{k+m}$. Thus, $(m, n) \in \Lambda^\circ$ if and only if

$$\ell m \equiv kn \mod N, \quad \forall (k, \ell) \in \Lambda. \tag{3.3.1}$$

Since $k \in K$ and $\ell \in L$ we can write $k = k'a$ and $\ell = \ell' b$ for some $k' \in (\mathbb{Z}/bN'\mathbb{Z})$ and $\ell' \in (\mathbb{Z}/aN'\mathbb{Z})$. Using this in (3.3.1) gives a new condition

$$\ell' bm \equiv k'an \mod N, \forall (k', \ell') \in (\mathbb{Z}/bN'\mathbb{Z}) \times (\mathbb{Z}/aN'\mathbb{Z}). \tag{3.3.2}$$

Lemma 3.3.1. *Let $N = abN'$ where $\gcd(a, b) = 1$. (m, n) is a solution to (3.3.2) if and only if m is a multiple of $N'a$ and n is a multiple of $N'b$. In particular, if $\Lambda = K \times L$ where $K = \langle a \rangle$ and $L = \langle b \rangle$, then $\Lambda^\circ = N'K \times N'L = \langle N'a \rangle \times \langle N'b \rangle$.*

Proof. First note that if $m = rN'a$ and $n = sN'b$ for some $r \in (\mathbb{Z}/b\mathbb{Z})$ and $s \in (\mathbb{Z}/a\mathbb{Z})$ then the left hand side of (3.3.2) becomes

$$\ell' b(rN'a) \equiv \ell' r(abN') \equiv 0 \mod N. \tag{3.3.3}$$

The right hand side of (3.3.2) becomes

$$k'a(sN'b) \equiv k's(abN') \equiv 0 \mod N. \tag{3.3.4}$$

Since (3.3.3) and (3.3.4) are equal we have that $N'K \times N'L \subseteq \Lambda^\circ$. Conversely, note that since $\gcd(a, b) = 1$, m must be a multiple of a, and n must be a multiple of b. In other words, $\Lambda^\circ \subseteq K \times L$. Now, suppose $m = ra$ and $n = sb$. Then, condition (3.3.2) becomes

$$\ell' rab \equiv k' sab \mod N, \forall (k', \ell') \in (\mathbb{Z}/bN'\mathbb{Z}) \times (\mathbb{Z}/aN'\mathbb{Z}). \tag{3.3.5}$$

If $N' = 1$, the above is always true since $N = abN' = ab$ and thus $\Lambda^\circ = N'K \times N'L = K \times L$. Assume that $N' > 1$ and without loss of generality, assume $N' \nmid r$. Then, choose $\ell' = 1$ and $k' = 0$. We now have that the right hand side is 0 while the left hand side cannot be a multiple of N. Thus, (3.3.5) cannot hold, $N' \mid r$ and $N' \mid s$ is necessary, and we get $\Lambda^\circ \subseteq N'K \times N'L$. □

The following examples rely on knowing where the discrete periodic ambiguity function of the generating $\varphi \in \mathbb{C}^N$ is zero. To this end, we now compute the discrete periodic ambiguity functions for the Chu, P4, Wiener (odd and even), and Björck-Saffari sequences. The Milewski sequence has its discrete periodic ambiguity function written without proof. To begin, the computation of the DPAF of the Chu sequence is as follows,

$$A_p(\varphi)[m, n] = \frac{1}{N} \sum_{k=0}^{N-1} e^{\pi i(k+m)(k+m-1)/N} e^{-\pi i k(k-1)/N} e^{-2\pi i n k/N} \tag{3.3.6}$$

$$= \frac{1}{N} \sum_{k=0}^{N-1} e^{\pi i[(k+m)(k+m-1)-k(k-1)-2nk]/N} \tag{3.3.7}$$

$$= \frac{1}{N}\sum_{k=0}^{N-1} e^{\pi i(k^2+2km+m^2-k-m-k^2+k-2nk)/N} \tag{3.3.8}$$

$$= \frac{1}{N}\sum_{k=0}^{N-1} e^{\pi i(2km+m^2-m-2nk)/N} \tag{3.3.9}$$

$$= \frac{1}{N}e^{\pi i(m^2-m)/N}\sum_{k=0}^{N-1} e^{2\pi ik(m-n)/N} \tag{3.3.10}$$

$$= \begin{cases} e^{\pi i(m^2-m)/N}, & \text{if } m \equiv n \mod N \\ 0, & \text{otherwise.} \end{cases} \tag{3.3.11}$$

Note that in particular, everything off of the line $n = m$ returns a zero. We will leverage this fact in several of the examples. Next, we compute the DPAF of the P4 sequence.

$$A_p(\varphi)[m,n] = \frac{1}{N}\sum_{k=0}^{N-1} e^{\pi i(k+m)(k+m-N)/N}e^{-\pi ik(k-N)/N}e^{-2\pi ink/N} \tag{3.3.12}$$

$$= \frac{1}{N}\sum_{k=0}^{N-1} e^{\pi i[(k+m)(k+m-N)-k(k-N)-2nk]/N} \tag{3.3.13}$$

$$= \frac{1}{N}\sum_{k=0}^{N-1} e^{\pi i(k^2+2km+m^2-Nk-Nm-k^2+Nk-2nk)/N} \tag{3.3.14}$$

$$= \frac{1}{N}\sum_{k=0}^{N-1} e^{\pi i(m^2-Nm+2mk-2nk)/N} \tag{3.3.15}$$

$$= \frac{1}{N}(-1)^m e^{\pi im^2/N}\sum_{k=0}^{N-1} e^{2\pi i(m-n)k/N} \tag{3.3.16}$$

$$= \begin{cases} (-1)^m e^{\pi im^2/N}, & \text{if } m \equiv n \mod N \\ 0, & \text{otherwise.} \end{cases} \tag{3.3.17}$$

Like the Chu sequence, the DPAF of the P4 sequence is also only nonzero on the diagonal $n = m$. Due to this fact, the Chu and P4 sequences will be used interchangably in the examples. For the Wiener sequences, we start with the case when

N is odd. In that case, φ has the form

$$\forall k \in (\mathbb{Z}/N\mathbb{Z}),\ \varphi[k] = e^{2\pi i s k^2/N}. \tag{3.3.18}$$

Then, the computation of the DPAF is as follows,

$$\begin{aligned} A_p(\varphi)[m,n] &= \frac{1}{N}\sum_{k=0}^{N-1} e^{2\pi i s(k+m)^2/N} e^{-2\pi i s k^2/N} e^{-2\pi i n k/N} && (3.3.19)\\ &= \frac{1}{N}\sum_{k=0}^{N-1} e^{2\pi i(sk^2+2skm+sm^2-sk^2-nk)/N} && (3.3.20)\\ &= \frac{1}{N}\sum_{k=0}^{N-1} e^{2\pi i(sm^2+2skm-nk)/N} && (3.3.21)\\ &= \frac{1}{N} e^{2\pi i s m^2/N}\sum_{k=0}^{N-1} e^{2\pi i(2sm-n)k/N} && (3.3.22)\\ &= \begin{cases} e^{2\pi i s m^2/N}, & \text{if } 2sm \equiv n \mod N \\ 0, & \text{otherwise.} \end{cases} && (3.3.23) \end{aligned}$$

Next, we do the case where N is even. In this case, φ has the form

$$\forall k \in (\mathbb{Z}/N\mathbb{Z}),\ \varphi[k] = e^{\pi i s k^2/N}. \tag{3.3.24}$$

In this case, the computation of the DPAF is as follows,

$$\begin{aligned} A_p(\varphi)[m,n] &= \frac{1}{N}\sum_{k=0}^{N-1} e^{\pi i s(k+m)^2/N} e^{-\pi i s k^2/N} e^{-2\pi i n k/N} && (3.3.25)\\ &= \frac{1}{N}\sum_{k=0}^{N-1} e^{\pi i(sk^2+2skm+sm^2-sk^2-2nk)/N} && (3.3.26)\\ &= \frac{1}{N}\sum_{k=0}^{N-1} e^{\pi i(sm^2+2skm-2kn)/N} && (3.3.27)\\ &= e^{\pi i s m^2/N}\frac{1}{N}\sum_{k=0}^{N-1} e^{2\pi i(sm-n)k/N} && (3.3.28) \end{aligned}$$

$$= \begin{cases} e^{\pi i s m^2/N}, & \text{if } sm \equiv n \mod N \\ 0, & \text{otherwise.} \end{cases} \tag{3.3.29}$$

The last computation we have is for the square length Björck-Saffari sequence. The computation of its DPAF proceeds as follows,

$$A_p(\varphi)[sN+t, kN+\ell]$$

$$= \frac{1}{N^2} \sum_{r=0}^{N-1} \sum_{h=0}^{N-1} \varphi[(r+s)N + (h+t)]\overline{\varphi[rN+h]} e^{-2\pi i(kN+\ell)(rN+h)/N^2} \tag{3.3.30}$$

$$= \frac{1}{N^2} \sum_{r=0}^{N-1} \sum_{h=0}^{N-1} c[h+t]\overline{c[h]} e^{2\pi i(r+s+\lfloor \frac{(h+t)}{N} \rfloor)\sigma(h+t)/N} e^{-2\pi i r\sigma(h)/N} e^{-2\pi i[(kh+r\ell)N+\ell h]/N^2} \tag{3.3.31}$$

$$= \frac{1}{N^2} \sum_{h=0}^{N-1} c[h+t]\overline{c[h]} e^{2\pi i(s+\lfloor \frac{(h+t)}{N} \rfloor)\sigma(h+t)/N} e^{-2\pi i(khN+\ell h)/N^2} \sum_{r=0}^{N-1} e^{2\pi i(\sigma(h+t)-\sigma(h)-\ell)r/N} \tag{3.3.32}$$

$$= \frac{1}{N} \sum_{h=0}^{N-1} c[h+t]\overline{c[h]} e^{2\pi i(s+\lfloor \frac{(h+t)}{N} \rfloor)\sigma(h+t)/N} e^{-2\pi i(khN+\ell h)/N^2} \tag{3.3.33}$$

if $\sigma(h+t) - \sigma(h) - \ell \equiv 0 \mod N$, and 0 otherwise. In particular, if $\sigma(h) = h$ for all h, then the above condition reduces to $t \equiv \ell \mod N$.

The DPAF of the Milewski sequence is written here without computation, but the computation can be found in [10]. For the DPAF of the Milewski sequence, $A_p(\varphi)$ we have that $NA_p(\varphi)[kN+\ell, s]$ is computed by

$$\begin{cases} 0, & \text{if } m \not\equiv n \mod N \\ \sum_{j=0}^{N-1} e^{2\pi i\left(k+\lfloor \frac{j+\ell}{N} \rfloor - js\right)/MN} A_p(v)\left[k + \lfloor \frac{j+\ell}{N} \rfloor, \frac{s-\ell}{N}\right], & \text{if } m \equiv n \mod N. \end{cases} \tag{3.3.34}$$

We now proceed to examples utilizing Theorem 3.2.7. The first example uses the $K \times L$ setup and applies it to the Chu and P4 sequence. As seen in (3.3.11) and

(3.3.17), if φ is the Chu or P4 sequence, $A_p(\varphi)[m,n]$ only has nonzero entries along the diagonal $m = n$. We will leverage this fact for an easy proof of Proposition 3.3.2. It should also be noted that some slight modifications can be made to easily extend Proposition 3.3.2 to Wiener sequences.

Proposition 3.3.2. *Let $\varphi \in \mathbb{C}^N$ be either the Chu or P4 sequence and let $K = \langle a \rangle$ and $L = \langle b \rangle$ with gcd$(a,b) = 1$ and $N = abN'$. Then, the Gabor system $(\varphi, K \times L)$ is a tight Gabor frame with frame bound NN'.*

Proof. Using Lemma 3.3.1, we have that $(m,n) \in (K \times L)^\circ$ if and only if $m = raN'$ and $n = sbN'$ for some $r \in (\mathbb{Z}/bN'\mathbb{Z})$ and $s \in (\mathbb{Z}/aN'\mathbb{Z})$. However, $A_p(\varphi)[m,n] \neq 0$ if and only if $m \equiv n \mod N$, i.e. $m, n \in N'K \cap N'L$. This intersection is generated by $\mathrm{lcm}(N'a, N'b) = abN' = N$. Thus, for $(m,n) \in (K \times L)^\circ$, $A_p(\varphi)[m,n] \neq 0$ if and only if $m = n = 0$. By Theorem 3.2.7, we have that $(\varphi, K \times L)$ is a tight frame with frame bound $|\Lambda| = NN'$. □

Note that other subgroups besides the $K \times L$ type subgroups can be used in Proposition 3.3.2 to obtain the same result. The proof only required that for every $(m,n) \in \Lambda^\circ$, $m \not\equiv n \mod N$ unless $(m,n) = (0,0)$. We provide an example illustrating this idea, Proposition 3.3.3.

Proposition 3.3.3. *Let $\varphi \in \mathbb{C}^N$ be either the Chu or P4 sequence and let $\Lambda = \langle (a,b) \rangle$ where $a \neq b$ and gcd$(a,N) =$ gcd$(b,N) = 1$. Then, the Gabor system (φ, Λ) is a tight Gabor frame with frame bound N.*

Proof. Suppose $\gcd(a,b) = d$. Let $a = da'$ and $b = db'$. Since $\gcd(a,N) = 1$ and $\gcd(b,N) = 1$, the order of Λ is N and is the same subgroup as the one generated by (a', b'). Thus, without loss of generality, we can assume that $\gcd(a, b) = 1$. Then, by (3.3.1), we know that $(m, n) \in \Lambda^\circ$ if and only if

$$kn \equiv \ell m \mod N \tag{3.3.35}$$

which can be rewritten as

$$san \equiv sbm \mod N. \tag{3.3.36}$$

Letting $s = 1$, we see that $an \equiv bm \mod N$ is a necessary condition and since $\gcd(a, b) = 1$ we need that n is a multiple of b and m is a multiple of a. It is clear that multiples of (a, b) also work for $s \neq 1$ and so we have that $\Lambda^\circ = \Lambda$. Since $\gcd(a, b) = 1$, we have that $m = n$ if and only if $m = n = 0$. Thus, $A_p(\varphi)[m, n] = 0$ for every $(m, n) \in \Lambda^\circ$ except at $(0, 0)$. Since $|\Lambda| = N$, we have that (φ, Λ) is a tight frame with frame bound N. □

Next, we examine the square length Björck-Saffari sequence. From (3.3.33), the DPAF of the square length Björck-Saffari sequence is still sparse, and the nonzero entries have regular structure when we use the identity permutation $\sigma(m) = m$. We leverage this fact to prove Proposition 3.3.4 and apply the same techniques as in Proposition 3.3.2.

Proposition 3.3.4. *Let $c \in \mathbb{C}^N$ and let $\varphi \in \mathbb{C}^{N^2}$ be the square length Björck-Saffari sequence generated by c and $\sigma(h) = h$. Let $K = \langle a \rangle$ and $L = \langle b \rangle$ with $\gcd(a, b) = 1$ and $N^2 = abN'$. Then, the Gabor system $(\varphi, K \times L)$ is a tight Gabor frame with frame bound $N^2 N'$.*

Proof. Using Lemma 3.3.1, $\sigma(h) = h$, and (3.3.33) , if $(rN'a, sN'b) \in N'K \times N'L$, then $A_p(\varphi)[rN'a, sN'b] \neq 0$ only if

$$rN'a \equiv sN'b \mod N \tag{3.3.37}$$

for some $r, s \in (\mathbb{Z}/N\mathbb{Z})$. From the proof of Proposition 3.3.2, we know that $N'K \cap N'L$ is generated by $\operatorname{lcm}(aN', bN')$. We have that $\operatorname{lcm}(N'a, N'b) = N' \operatorname{lcm}(a, b) = abN' = N^2 \equiv 0 \mod N$. Moreover, if $A_p(\varphi)[rN'a, sN'b] \neq 0$, then $r = s = 0$. By Theorem 3.2.7, we have that $(\varphi, K \times L)$ is a tight Gabor frame, and the frame bound is $|\Lambda| = N^2N'$. □

The next example utilizes Theorem 3.2.7, but has the opposite theme: the discrete periodic amibguity function is mostly nonzero except for the "right" spots. That is, $A_p(\varphi)[m, n] \neq 0$ for nearly every $(m, n) \notin \Lambda^\circ$ but $A_p(\varphi)$ will still be Λ°-sparse.

Proposition 3.3.5. *Let $u \in \mathbb{C}^M$ be CAZAC, $v \in \mathbb{C}^N$ be CA, and $\varphi \in \mathbb{C}^{MN}$ be defined by*

$$\varphi = u \otimes v \tag{3.3.38}$$

where $\otimes$ is the Kronecker product. Assume gcd$(M, N) = 1$ and let $\Lambda = \langle M \rangle \times \langle N \rangle$. Then, (φ, Λ) is a tight frame with frame bound MN.

Proof. We can write the $(rN + s)$-th term of φ as

$$\varphi[rN + s] = u[r]v[s] \tag{3.3.39}$$

where $r \in (\mathbb{Z}/M\mathbb{Z})$ and $s \in (\mathbb{Z}/N\mathbb{Z})$. We now compute the DPAF,

$$A_p(\varphi)[rN + s, \ell]$$

$$= \frac{1}{MN} \sum_{j=0}^{M-1} \sum_{k=0}^{N-1} u\left[j + r + \left\lfloor \frac{s+k}{N} \right\rfloor\right] v[s+k]\overline{u[j]v[k]}e^{-2\pi i(jN+k)\ell/MN} \tag{3.3.40}$$

$$= \frac{1}{N} \sum_{k=0}^{N-1} v[s+k]\overline{v[k]}e^{-2\pi ik\ell/MN} \frac{1}{M} \sum_{j=0}^{M-1} u\left[j + r + \left\lfloor \frac{s+k}{N} \right\rfloor\right] \overline{u[j]}e^{-2\pi ij\ell/M} \tag{3.3.41}$$

$$= \frac{1}{N} \sum_{k=0}^{N-1} v[s+k]\overline{v[k]}e^{-2\pi ik\ell/MN} A_p(u)\left[r + \left\lfloor \frac{s+k}{N} \right\rfloor, \ell\right]. \tag{3.3.42}$$

By Lemma 3.3.1 we have that $\Lambda^\circ = \Lambda$. Using (3.3.42), we can see that for $(rN, \ell M) \in \Lambda^\circ \backslash \{(0,0)\}$ we have

$$A_p(\varphi)[rN, \ell M] = \frac{1}{N} \sum_{k=0}^{N-1} v[k]\overline{v[k]}e^{-2\pi ik\ell/N} A_p(u)[r, \ell M] \tag{3.3.43}$$

$$= \frac{A_p(u)[r,0]}{N} \sum_{k=0}^{N-1} |v[k]|^2 e^{-2\pi ik\ell/N} = 0 \tag{3.3.44}$$

since one of r or ℓ is nonzero. Indeed, if r is nonzero, then since u has zero autocorrelation, we have a multiplier of zero outside of the sum. On the other hand, if $r = 0$ but $\ell \neq 0$, then the sum will add up to zero since $|v[k]|^2 = 1$ for every k. We now conclude by Theorem 3.2.7 that (φ, Λ) is a tight frame with frame bound MN. □

Although $A_p(\varphi)$ is Λ°-sparse, (3.3.42) implies that most of the entries for $A_p(\varphi)$ are nonzero. This is illustrated by Figure 3.3.1. In Figure 3.3.1, u is the Björck sequence efined in Section 2.1.

Proposition 3.3.6. *Let $\varphi \in \mathbb{C}^{MN^2}$ be a Milewski sequence where the generating $v \in \mathbb{C}^M$ is either the Chu or P4 sequence, and let a, b, j, N' be such that gcd$(a,b) = 1$,*

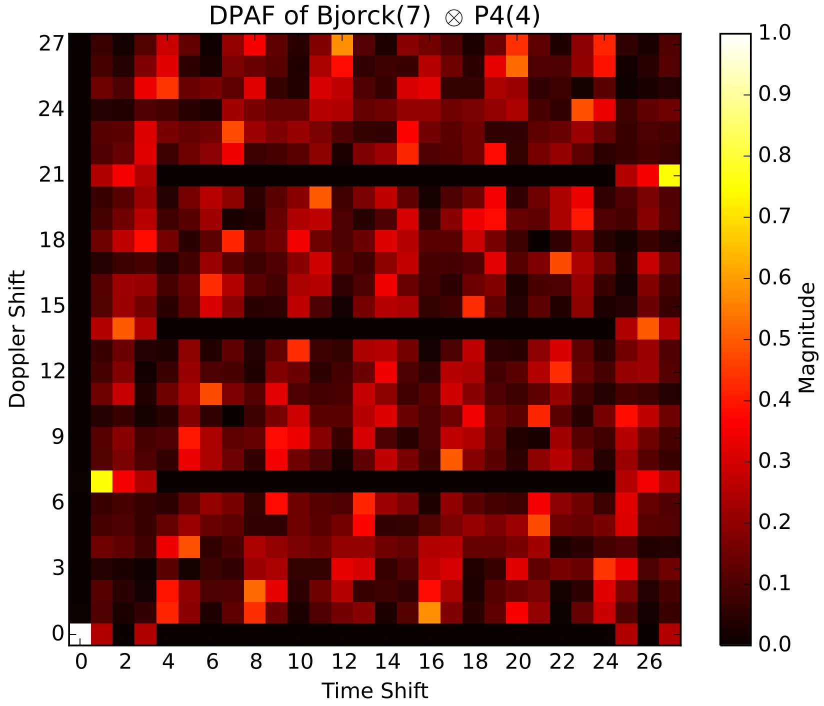

Figure 3.3.1: DPAF of $\varphi = u \otimes v$ where u is the length 7 Björck sequence and v is the length 4 P4 sequence.

$j \mid MN$, $N' = jN$, and $abN' = MN^2$. Let $\Lambda = K \times L$ where $K = \langle a \rangle$, and $L = \langle b \rangle$. Then, (φ, Λ) is a tight frame with frame bound jMN^3.

Proof. By Lemma 3.3.1, we have that $\Lambda^\circ = N'K \times N'L$. In particular, for every $(m, n) \in \Lambda^\circ$ we have that $m \equiv n \equiv 0 \mod N$. Thus, using the second line of (3.3.34), for $(m, n) \in \Lambda^\circ$ we can write $A_p(\varphi)[m, n]$ in the form

$$NA_p(\varphi)[m, n] = \sum_{j=0}^{N-1} e^{\theta[j]} A_p(v)[m', n'] \tag{3.3.45}$$

where $m' = m/N$ and $n' = n/N$. Since v is the Chu or P4 sequence, we have that $A_p(v)[m', n'] \neq 0$ if and only if $m' \equiv n' \mod M$. Furthermore, $\Lambda^\circ = \langle aN' \rangle \times \langle bN' \rangle = \langle ajN \rangle \times \langle bjN \rangle$ and so we have that $m' \in \langle aj \rangle$ and $n' \in \langle bj \rangle$. Thus, we have that $m' \equiv n' \mod M$ if and only if $m', n' \in \langle aj \rangle \cap \langle bj \rangle = \langle \text{lcm}(aj, bj) \rangle$. Since $\gcd(a, b) = 1$, $\text{lcm}(aj, bj) = abj = MN$ since $abjN = abN' = MN^2$. We want to view $\langle aj \rangle$ and $\langle bj \rangle$ as being subgroups of $(\mathbb{Z}/MN\mathbb{Z})$, thus we have that $m' \equiv n' \mod MN$ if and only if $m' \equiv n' \equiv 0 \mod MN$. Therefore, if $(m, n) \in \Lambda^\circ$, then $A_p(\varphi) = 0$ except for $(m, n) = (0, 0)$. By Theorem 3.2.7, we conclude that (φ, Λ) is a tight frame with frame bound jMN^3. □

3.4 Tight Gabor Frames via CAZACs: Gram Matrix Method

The framework of this last section is as follows: First, we explicitly compute the entries of the Gram matrix by using the discrete periodic ambiguity function. Then, we show that the first N columns or rows have disjoint supports. Last, we show that every other column or row is a constant multiple of one of the first N rows or columns, and show that there is only one nonzero eigenvalue. This allows us to conclude that the Gabor system is indeed a tight frame.

First, we show that the Gram matrix of a Gabor system (φ, Λ) can be written in terms of the discrete periodic ambiguity function of φ. To start, we establish the main tool for determining when frames are tight via its Gram matrix.

Theorem 3.4.1. *Let $\mathcal{H}$ be an N-dimensional Hilbert space and let $\mathcal{F} = \{v_i\}_{i=1}^M$ be a frame for $\mathcal{H}$. $\mathcal{F}$ is a tight frame if and only if rank$(G) = N$ and G has a single eigenvalue.*

For all that follows let $\varphi \in \mathbb{C}^N \backslash \{0\}$ and let us write out the Gabor system as $\mathcal{F} = \{e_{\ell_m}\tau_{k_m}\varphi : m \in 0, \cdots, M\}$. Then, we can compute the (m,n)-th entry of the Gram matrix:

$$G_{m,n} = \langle e_{\ell_m}\tau_{k_m}\varphi, \overline{e_{\ell_n}\tau_{k_n}\varphi}\rangle = \sum_{j=0}^{N} e^{2\pi i \ell_m j/N}\varphi[j-k_m]e^{-2\pi i \ell_n j/N}\overline{\varphi[j-k_n]} \tag{3.4.1}$$

$$= \sum_{j=0}^{N} e^{-2\pi i(\ell_n-\ell_m)j/N}\varphi[j-k_m]\overline{\varphi[j-k_n]} \tag{3.4.2}$$

$$= \sum_{j=0}^{N} e^{-2\pi i(\ell_n-\ell_m)(j-k_n+k_n)/N}\varphi[j-k_n+(k_n-k_m)]\overline{\varphi[j-k_n]} \tag{3.4.3}$$

$$= e^{-2\pi i k_n(\ell_n-\ell_m)/N}\sum_{j=0}^{N}\varphi[j+(k_n-k_m)]\overline{\varphi[j]}e^{-2\pi i(\ell_n-\ell_m)j/N} \tag{3.4.4}$$

$$= Ne^{-2\pi i k_n(\ell_n - \ell_m)/N} A_p(\varphi)[k_n - k_m, \ell_n - \ell_m] \tag{3.4.5}$$

Next, we apply (3.4.5) to (3.3.11), (3.3.17), (3.3.23), and (3.3.29) to explicitly write down the Gabor matrix of the Chu, P4, and Wiener CAZAC sequences. For convenience, we define $r_{mn} :\equiv (k_n - k_m) \equiv (\ell_n - \ell_m)$. Using this notation, we get the following Gram matrices:

Chu sequence:

$$G_{mn} = \begin{cases} Ne^{-2\pi i[k_n r_{mn} - \frac{1}{2}(r_{mn}^2 - r_{mn})]/N}, & \text{if } (\ell_n - \ell_m) \equiv (k_n - k_m) \mod N \\ 0, & \text{otherwise.} \end{cases} \tag{3.4.6}$$

P4 Sequence:

$$G_{mn} = \begin{cases} N(-1)^{r_{mn}} e^{-2\pi i[k_n r_{mn} - \frac{1}{2} r_{mn}^2]/N}, & \text{if } (k_n - k_m) \equiv (\ell_n - \ell_m) \mod N \\ 0, & \text{otherwise.} \end{cases} \tag{3.4.7}$$

Odd Length Wiener Sequence:

$$G_{mn} = \begin{cases} Ne^{-4\pi i s k_n r_{mn}/N} e^{2\pi i s r_{mn}^2/N}, & \text{if } 2s(k_n - k_m) \equiv (\ell_n - \ell_m) \mod N \\ 0, & \text{otherwise.} \end{cases}$$

Even Length Wiener Sequence:

$$G_{mn} = \begin{cases} Ne^{-2\pi i s k_n r_{mn}/N} e^{\pi i s m^2/N}, & \text{if } s(k_n - k_m) \equiv (\ell_n - \ell_m) \mod N \\ 0, & \text{otherwise.} \end{cases}$$

We now apply the outlined method to the the Chu and P4 sequence. We treat these two cases simultaneously since both have the property that $A_p(\varphi)[m,n] = 0$ if

$m \neq n$, and are nonzero when $m = n$. The computation in Lemma 3.4.4 is different for the P4 case, but the same ideas can be used achieve the same result. The Wiener case has direct analogues of the results in the Chu and P4 cases, and we will only highlight the key differences in the proofs instead of reiterating the details. Before proceeding, we need a useful fact about the Gram matrix which can easily be derived from the singular value decomposition of the analysis operator.

Lemma 3.4.2. *Let F be an $m \times n$ complex-valued matrix and let $G := FF^*$. Then, rank(G) = rank(F).*

Proof. First, we write F in terms of its SVD: $F = UDV^*$ where D is an $m \times n$ rectangular diagonal matrix and U and V are $m \times m$ and $n \times n$ unitary matrices, respectively. Note that $G = FF^* = UDV^*VD^*U^* = UDD^*U^* = UD^2U^*$. In particular, $D_{ij}^2 = |D_{ij}|^2$ and from this we conclude $\text{rank}(G) = \text{rank}(F)$. □

For the following propostions, we shall use the following arrangement for the Gram matrix. Let $(\varphi, K \times L)$ be a Gabor system in $\mathbb{C}^N$. We shall iterate by modulation first, then iterate by translations. In other words, the analysis operator, F, will be a $|K||L| \times N$ matrix where the m-th row is given by $m = r|L| + s$, $r \in (\mathbb{Z}/|K|\mathbb{Z})$, $s \in (\mathbb{Z}/|L|\mathbb{Z})$, and the $m = r|L| + s$-th row corresponds to $e_{\ell_s}\tau_{k_r}\varphi$.

Proposition 3.4.3. *Let $N = ab$ with gcd$(a, b) = 1$ and let $\varphi \in \mathbb{C}^N$ be either the Chu or P4 sequence. Let $K = \langle a \rangle$ and $L = \langle b \rangle$. Then, the Gabor system $(\varphi, K \times L)$ is a tight frame with frame bound N.*

Proof. By construction, $|K| = b$, $|L| = a$ and so the Gabor system $(\varphi, K \times L)$ has $ab = N$ vectors. Since $\text{lcm}(a, b) = N$, we have that $K \cap L = \{0\}$. From Section

???, we have that $G_{m,n} \neq 0$ if and only if $(\ell_n - \ell_m) = (k_n - k_m)$. By design of K and L, we have that $(\ell_n - \ell_m) = jb$ and $(k_n - k_m) = \tilde{j}a$ for some $j, \tilde{j}$. In particular, $(k_n - k_m) \in K$ and $(\ell_n - \ell_m) \in L$, and can only be equal if both belong to $K \cap L$. Thus, $G_{m,n} \neq 0$ if and only if $(\ell_n - \ell_m) = (k_n - k_m) = 0$, i.e. $j = \tilde{j} = 0$. We conclude that the nonzero entries lie only on the diagonal of G. Using formulas (3.4.6) and (3.4.7), we see that for each $n \in (\mathbb{Z}/N\mathbb{Z})$, $G_{n,n} = N$ and $G = NId_N$. Thus, the Gabor system $(\varphi, K \times L)$ is a tight frame with frame bound N. □

Lemma 3.4.4. *Let $\varphi \in \mathbb{C}^N$ be either 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, there exist functions $f, g : \mathbb{N} \cup \{0\} \to \mathbb{C}$ such that $G_{mn}/N = f(n)g(m)$ wherever $G_{mn} \neq 0$.*

Proof. We will only cover the case of the Chu sequence. The case of the P4 sequence follows by replacing $e^{-\pi i r_{mn}/N}$ with $(-1)^{r_{mn}}$ and carrying out the same computations. If $G_{mn} \neq 0$, then we have

$$G_{mn}/N = e^{-2\pi i k_n r_{mn}/N} e^{-\pi i r_{mn}/N} e^{\pi i r_{mn}^2/N} \tag{3.4.8}$$

where

$$r_{mn} = k_n - k_m = \ell_n - \ell_m = jab. \tag{3.4.9}$$

Note that $k_n = c_n ab + d_n a$ and $k_m = c_m ab + d_m a$ where $c_n, c_m \in (\mathbb{Z}/N'\mathbb{Z}), d_n, d_m \in (\mathbb{Z}/b\mathbb{Z})$. However, by (3.4.9), $j = c_n - c_m$ and $d_n = d_m$. Putting this back into (3.4.8) and using $\omega = e^{2\pi i/N}$ and $\zeta = e^{2\pi i/N'}$, we have

$$G_{mn}/N = \omega^{-(c_n ab + d_n a)(c_n - c_m)ab} \omega^{-(c_n - c_m)ab/2} \omega^{(c_n - c_m)^2 a^2 b^2/2} \tag{3.4.10}$$

$$= \zeta^{-c_n ab(c_n - c_m)} \zeta^{-d_n a(c_n - c_m)} \zeta^{-(c_n - c_m)/2} \zeta^{ab(c_n^2 - 2c_n c_m + c_m^2)/2} \tag{3.4.11}$$

$$= \zeta^{-c_n^2 ab} \zeta^{c_n c_m ab} \zeta^{-d_n a(c_n - c_m)} \zeta^{-(c_n - c_m)/2} \zeta^{ab(c_n^2 + c_m^2)/2} \zeta^{-abc_n c_m} \tag{3.4.12}$$

$$= \zeta^{-c_n^2 ab/2} \zeta^{-d_n c_n a} \zeta^{-c_n/2} \zeta^{c_m^2 ab/2} \zeta^{d_m c_m a} \zeta^{c_m/2}. \tag{3.4.13}$$

Here we have used the crucial fact that $d_n = d_m$. Thus, we can write nonzero entries of G_{mn} as $f(n)g(m)$ where

$$f(n) = \zeta^{-c_n^2 ab/2} \zeta^{-d_n c_n a} \zeta^{-c_n/2} \tag{3.4.14}$$

and

$$g(m) = \zeta^{\pi i c_m^2 ab/2} \zeta^{d_m c_m a} \zeta^{c_m/2}. \tag{3.4.15}$$

□

Lemma 3.4.5. *Let $\varphi \in \mathbb{C}^N$ be either 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, the support of the rows (or columns) of G either completely coincide or are completely disjoint.*

Proof. Let us denote the m-th row of G as g_m, and all indices are implictly taken modulo N. We shall show that if there is at least one index $n \in (\mathbb{Z}/N\mathbb{Z})$ such that $g_m[n] = g_{m'}[n] \neq 0$, and $m \neq m'$, then $\text{supp}(g_m) = \text{supp}(g_{m'})$. Suppose that $g_m[n] = g_{m'}[n] \neq 0$. Then, $k_n - k_m = \ell_n - \ell_m = jab$ and $k_n - k_{m'} = \ell_n - \ell_{m'} = j'ab$. We can rearrange these two equations to obtain the following

$$k_m = k_n - jab \tag{3.4.16}$$

and

$$k_n = k_{m'} + j'ab. \tag{3.4.17}$$

Now suppose there is another $n' \in (\mathbb{Z}/N\mathbb{Z})$ where $g_m[n'] \neq 0$. Then, we have

$$k_{n'} - k_m = \tilde{j}ab. \tag{3.4.18}$$

Substiuting (3.4.16) and (3.4.17) into (3.4.18), we have

$$\tilde{j}ab = k_{n'} - k_m = k_{n'} - k_n + jab = k_{n'} - k_{m'} - j'ab + jab,$$

which can be rearranged to obtain

$$(j' + \tilde{j} - j)ab = k_{n'} - k_{m'}.$$

Note that $(j' + \tilde{j} - j) \in (\mathbb{Z}/N\mathbb{Z})$ and that these same computations can be done replacing k with ℓ. Thus, $g_{m'}[n'] \neq 0$ as well and the result is proved. □

Remark 3.4.6. Let $\gcd(a,b) = 1$, $N = abN'$, $K = \langle a \rangle$, $L = \langle b \rangle$, $\varphi \in \mathbb{C}^N$ be the Chu and P4 sequence, and consider the system $(\varphi, K \times L)$. In light of Lemma 3.4.4 and Lemma 3.4.5, if two rows of the Gram matrix G have supports which coincide, they must be constant multiples of each other, where this multiple has modulus 1. Indeed, if g_m and $g_{m'}$ have coinciding supports then for each n where they are nonzero we have

$$\frac{G_{mn}}{G_{m'n}} = \frac{Nf(n)g(m)}{Nf(n)g(m')} = \frac{g(m)}{g(m')}.$$

This also gives us a formula for finding the constant multiple, should we desire it. This idea is illustrated with Figure 3.4.1, where two sets of rows with coinciding supports are highlighted in red and blue, respectively.

Theorem 3.4.7. *Let $K = \langle a \rangle$, $L = \langle b \rangle$, and $N = abN'$ with gcd$(a,b) = 1$. Furthermore, let $\varphi \in \mathbb{C}^N$ be either the Chu or P4 sequence. Then, the Gabor system $(\varphi, K \times L)$ has the following properties:*

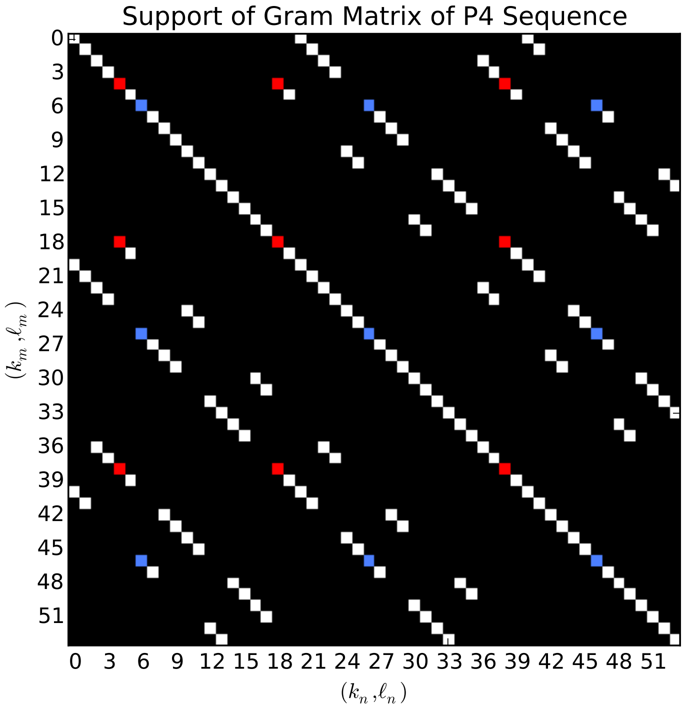

Figure 3.4.1: Support of G in the case $N = 18$, φ is the P4 sequence, $a = 2$, $b = 3$, and $N' = 3$.

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

(ii) The nonzero eigenvalues of G *are* NN'.

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

Proof. (i) We shall show that the support of the first N columns are disjoint, and then conclude that rank$(G) = N$. K and L are subgroups of $(\mathbb{Z}/N\mathbb{Z})$ and that $K \cap L = \langle ab \rangle$. Moreover, $G_{mn} \neq 0$ if and only if $(\ell_n - \ell_m) \equiv (k_n - k_m) \mod N$. Since K and L are subgroups, this can only happen if the subtractions lie in the intersections of the two groups. That is, $G_{mn} \neq 0$ if and only if

$$(\ell_n - \ell_m) \equiv (k_n - k_m) \equiv jab \mod N \tag{3.4.19}$$

where $j \in (\mathbb{Z}/N'\mathbb{Z})$. Let $m \in (\mathbb{Z}/N\mathbb{Z})$. By (3.4.19), we have that for $G_{mn} \neq 0$ we must have that $k_n = (k_m + jab)$ for some j. Since $k_m \in K$, we have that

$$k_n = (j_m a + jab) = a(j_m + jb) \tag{3.4.20}$$

for some $j_m \in (\mathbb{Z}/bN'\mathbb{Z})$ and some $j \in (\mathbb{Z}/N'\mathbb{Z})$.

By the ordering we used for the columns of G, we can write the index for column n in terms of k_n and ℓ_n by

$$n = (k_n/a)aN' + \ell_n/b = k_n N' + \ell_n/b. \tag{3.4.21}$$

In particular, we would like $n \leqslant N$, and for that we need that $k_n < ab$. Looking at (3.4.20), we need $(j_m + jb) < b$. There is exactly one such $j \in (\mathbb{Z}/N'\mathbb{Z})$ which can achieve this and it is obtained by setting $j = -\lfloor j_m/b \rfloor$. Thus, for each row m, there is exactly 1 column $n \leqslant N$ where $G_{mn} \neq 0$, and therefore the first N columns of G are linearly independent. Thus, we conclude $\operatorname{rank}(G) \geqslant N$. By Lemma 3.4.2, we know that $\operatorname{rank}(G) = \operatorname{rank}(L)$. Since L is an $M \times N$ matrix, we have that $\operatorname{rank}(G) \leqslant N$ and we have that $\operatorname{rank}(G) = N$.

(ii) Let g_n be the n-th column of G, with $n \leqslant N$. We wish to show that $Gg_n = NN'g_n$. Note that $Gg_n[m]$ is given by the inner product of the m-th row and the n-th column of G. Furthermore, since G is self-adjoint, the n-th column is also the conjugate of the n-th row. If $g_n[m] \neq 0$, then $G_{mn} \neq 0$ and $G_{nn} \neq 0$. Thus, by Lemma 3.4.5 rows m and n have supports that coincide. By Lemma 3.4.4,

$G_{m(\cdot)} = C_m g_n^*$, where $|C_m| = 1$. Thus, $Gg_n[m] = C_m \|g_n\|_2^2 = N^2 N' C_m$. It is easily computed that $G_{nn} = N$, so by Lemma 3.4.4, we have that $g_n[m] = NC_m$. In particular, we get $Gg_n[m] = (NN')(NC_m)$. Thus, the first N columns of G are eigenvectors of G and all have eigenvalue NN'. It now follows that the system is a tight frame with frame bound NN'. □

Remark 3.4.8. In general, if $\gcd(a, b) > 1$, then the above result will not hold. Let $\varphi \in \mathbb{C}^4$ be the P4 sequence. That is, $\varphi = (1, -\sqrt{2}/2 - i\sqrt{2}/2, -1, -\sqrt{2}/2 - i\sqrt{2}/2)$. Let $K = \{0, 2\}$ and $L = \{0, 2\}$. Note that this would give $a = b = \gcd(a, b) = 2$. The Gabor system $(\varphi, K \times L)$ is given by

$$(\varphi, K \times L) = \{\pi(0,0)\varphi, \pi(0,2)\varphi, \pi(2,0)\varphi, \pi(2,2)\varphi\}$$

$$= \left\{ \begin{pmatrix} 1 \\ -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i \\ -1 \\ -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i \end{pmatrix}, \begin{pmatrix} 1 \\ \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\ -1 \\ \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \end{pmatrix}, \begin{pmatrix} -1 \\ -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i \\ 1 \\ -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i \end{pmatrix}, \begin{pmatrix} -1 \\ \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\ 1 \\ \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \end{pmatrix}, \right\}.$$

Note that the first and fourth vectors are multiples of each other, as well as the second and third vectors. Specifically,

$$\pi(0,0)\varphi = -\pi(2,2)\varphi \quad \text{and} \quad \pi(0,2)\varphi = -\pi(2,0)\varphi. \tag{3.4.22}$$

We conclude from this that the dimension of the span of the Gabor system $(\varphi, K \times L)$ is only 2, and the Gabor system in question is not a frame.

We close this section with brief mentions about the proofs in the Wiener sequence case. To simplify further, we only mention the odd length case, but one can easily make the highlighted adjustments in the even case as well.

Lemma 3.4.9. *Let $\varphi \in \mathbb{C}^N$ be a Wiener sequence of odd length 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, there exist functions $f, g : \mathbb{N} \cup \{0\} \to \mathbb{C}$ such that $G_{mn}/N = f(n)g(m)$ wherever $G_{mn} \neq 0$.*

To prove Lemma 3.4.9, the same technique used in Lemma 3.4.4 of writing $k_n = c_n ab + d_n a$ and $k_m = c_m ab + d_m a$ can be used, and the result follows from similar computations to Lemma 3.4.4.

Lemma 3.4.10. *Let $\varphi \in \mathbb{C}^N$ be a Wiener sequence of odd length and let $N = abN'$ where gcd$(a, b) = 1$. Suppose G is the Gram matrix generated by $(\varphi, K \times L)$, where $K = \langle a \rangle$ and $L = \langle b \rangle$. Then, the support of the rows (and columns) of G either completely coincide or are completely disjoint.*

To prove Lemma 3.4.10, one needs to replace jab, $j'ab$, $\tilde{j}ab$ in Lemma 3.4.5 with $2sjab$, $2sj'ab$, and $2s\tilde{j}ab$, and the same result will hold.

Theorem 3.4.11. *Let $K = \langle a \rangle$, $L = \langle b \rangle$, and $N = abN'$ with gcd$(a, b) = 1$. Furthermore, let $\varphi \in \mathbb{C}^N$ be a Wiener sequence of odd length. Then, the Gabor system $(\varphi, K \times L)$ has the following properties:*

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

(ii) The nonzero eigenvalues of G are NN'.

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

As with the modification used in Lemma 3.4.10, one only needs to change any instance of jab in Theorem 3.4.7 with $2sjab$ and apply the appropriate computations to prove Theorem 3.4.11.

Chapter 4: Generalizing the CAZAC Property

4.1 Generalizing CAZAC: Introduction and Motivation

In this chapter we explore possible generalizations of the CAZAC property to $\mathbb{T}$ and $\mathbb{R}$. Given that the autocorrelation function in $\mathbb{C}^N$ can be viewed as inner products of a vector and its translates, the most natural definition of autocorrelation on the real line would be to use the inner product for the Hilbert space $L^2(\mathbb{R})$.

Definition 4.1.1. For $f \in L^2(\mathbb{R})$ define its *autocorrelation function*, $A(f)$ by,

$$\forall x \in \mathbb{R}, A(f)(x) = \int_{\mathbb{R}} f(t+x)\overline{f(t)}\, dt. \tag{4.1.1}$$

However, if we wish to make an analogue of CAZAC sequences for functions on $\mathbb{R}$, it is clear that $L^2(\mathbb{R})$ is not an appropriate space to consider since if f is such that $|f(x)| = 1$ for every $x \in \mathbb{R}$, it is obvious that $f \notin L^2(\mathbb{R})$. The following theorem shows that even if we ignore the constant amplitude condition for the time being, $L^2(\mathbb{R})$ still is not an appropriate space for searching for zero autocorrelation functions as it merely leads to the zero function.

Theorem 4.1.2. *Let $f \in L^2(\mathbb{R})$, and suppose we have that,*

$$\forall x \in \mathbb{R}, x \neq 0,\ A(f)(x) = \int_{\mathbb{R}} f(t+x)\overline{f(t)}\, dt = 0. \tag{4.1.2}$$

Then, $f = 0$ a.e.

Proof. Let $\{g_n\}_{n=1}^{\infty} \subseteq C_c^{\infty}(\mathbb{R})$ be such that for every n, $\|f - g_n\|_2 \leqslant 1/(2\|f\|_2 + 1)n$. Then, for every $x \in \mathbb{R}$,

$$|A(f)(x) - A(g_n)(x)| = |\langle \tau_{-x} f, f\rangle - \langle \tau_{-x} g_n, g_n\rangle| \tag{4.1.3}$$

$$= |\langle \tau_{-x} f, f\rangle - \langle \tau_{-x} g_n, f\rangle + \langle \tau_{-x} g_n, f\rangle - \langle \tau_{-x} g_n, g_n\rangle| \tag{4.1.4}$$

$$\leqslant |\langle \tau_{-x}(f - g_n), f\rangle| + |\langle \tau_{-x} g_n, (f - g_n)\rangle| \tag{4.1.5}$$

$$\leqslant \|f - g_n\|_2 \|f\|_2 + \|g_n\|_2 \|f - g_n\|_2 \tag{4.1.6}$$

$$\leqslant \frac{\|f\|_2}{(2\|f\|_2 + 1)n} + \frac{\|f\|_2 + 1}{(2\|f\|_2 + 1)n} = \frac{1}{n}. \tag{4.1.7}$$

Thus, $A(g_n)$ converges to $A(f)$ uniformly. Since $A(g_n)$ is defined by a convolution integral, we have that $A(g_n) \in \mathbb{C}_c^{\infty}(\mathbb{R})$. We conclude that $A(f)$ must be continuous and that $A(f)(0) = 0$. In particular,

$$A(f)(0) = \int_{\mathbb{R}} |f(t)|^2 \, dt = 0 \tag{4.1.8}$$

implies that $f = 0$ a.e. □

To circumvent the problems outlined above, we examien two possible alternatives: distribution theory and Wiener's theory of generalized harmonic analysis.

The reason for trying distribtuion theory is natural. For zero autocorrelation we would want the autocorrelation to be zero almost everywhere except at the origin where the constant amplitude property would make the autocorrelation "infinity". This sounds much like the delta "function" and even more naturally if we formally take the Fourier transform of both sides of the equation

$$S * S = \delta, \tag{4.1.9}$$

then we obtain

$$|\widehat{S}|^2 = 1. \tag{4.1.10}$$

As for Wiener's generalized harmonic analysis, Wiener originally developed this theory to do harmonic analysis of white light which is not $L^2(\mathbb{R})$ but is $L^\infty(\mathbb{R})$ [5]. In particular, Wiener's generalized harmonic analysis theory was developed for non-periodic functions which were not$L^1(\mathbb{R})$ or $L^2(\mathbb{R})$. We will provide a brief overview of the generalized harmonic analysis theory which is relevant for analyzing the class of CAZAC functions on $\mathbb{R}$, but will first motivate it by showing that the autocorrelation function given in generalized harmonic analysis theory does allow for at least one non-trivial CAZAC function on $\mathbb{R}$ with respect to this autocorrelation.

4.2 CAZAC Property for Periodic Functions

The main focus of this section is to define the ambiguity function of $finL^2(\mathbb{T})$ and to then relate it to the discrete periodic ambiguity function in the discrete case. What Theorem 4.2.2 shows is that the ambiguity function on the torus can be approximated by uniformly sampling the function $f \in L^2(\mathbb{T})$ and computing the discrete periodic ambiguity function using those samples as the input vector. We finish this section giving an explicit example using Theorem 4.2.2.

Definition 4.2.1. Let $f \in L^2(\mathbb{T})$. We define the *ambiguity function* of f, $A(f) : \mathbb{T} \times \mathbb{Z} \to \mathbb{C}$, by

$$A(f)(x,n) = \int_{-1/2}^{1/2} f(t+x)\overline{f(t)}e^{-2\pi int}\,dt = \int_0^1 f(t+x)\overline{f(t)}e^{-2\pi int}\,dt. \tag{4.2.1}$$

Theorem 4.2.2. *Let $f \in C(\mathbb{T})$ and let $x = p/q \in \mathbb{Q}$. Define $f_{k,q} \in \mathbb{C}^{kq}$ by*

$$\forall j \in (\mathbb{Z}/kq\mathbb{Z}), f_{k,q}[j] = f\left(\frac{j}{kq}\right), \tag{4.2.2}$$

Then,

$$\forall n \in \mathbb{Z}, A(f)(x,n) = \lim_{k\to\infty} A_p(f_{k,q})[kp,n] \tag{4.2.3}$$

Proof. Using a Riemann sum with kq uniform width rectangles, $k \in \mathbb{N}$, we compute

$$\int_0^1 f(t+x)\overline{f(t)}e^{-2\pi int}\,dt = \lim_{k\to\infty}\frac{1}{kq}\sum_{j=0}^{kq-1} f\left(\frac{j}{kq}+\frac{p}{q}\right)\overline{f\left(\frac{j}{kq}\right)}e^{-2\pi inj/kq} \tag{4.2.4}$$

$$= \lim_{k\to\infty}\frac{1}{kq}\sum_{j=0}^{kq-1} f\left(\frac{j+kp}{kq}\right)\overline{f\left(\frac{j}{kq}\right)}e^{-2\pi inj/kq} \tag{4.2.5}$$

$$= \lim_{k\to\infty}\frac{1}{kq}\sum_{j=0}^{kq-1} f_{k,q}[j+kp]\overline{f_{k,q}[j]}e^{-2\pi inj/kq} \tag{4.2.6}$$

$$= A_p(f_{k,q})[kp,n].$$

□

In particular, Theorem 4.2.2 allows us to approximate the ambiguity function for functions on the torus by using discrete approximations of the function and computing the ambiguity function of the discrete sequence. We can adapt Theorem 4.2.2 for the torus of length $2T$ (as opposed to length 1, i.e. $\mathbb{T}$) and obtain discrete approximations to the mean autocorrelation function.

Theorem 4.2.3. *Let $\Phi \in L^\infty(\mathbb{R})$, $x = p/q \in \mathbb{Q}$, and define $\Phi_{T,q} \in \mathbb{C}^{Tq}$, $T \in \mathbb{N}$, by*

$$\Phi_{T,q}[j] = \Phi\left(2T\left(-\frac{1}{2} + \frac{j}{2Tq}\right)\right). \tag{4.2.7}$$

Then,

$$R(\Phi)(x) = \lim_{T\to\infty} A_p(\Phi_{T,q})[p, 0]. \tag{4.2.8}$$

Proof. Using a Riemann sum with uniform width rectangles of width $2Tq$,

$$\begin{aligned}
R(\Phi)(x) &= \lim_{T\to\infty} \frac{1}{2T}\int_{-T}^{T} \Phi(t+x)\overline{\Phi(t)}\,dt && (4.2.9)\\
&= \lim_{T\to\infty} \int_{-1/2}^{1/2} \Phi(2Ts+x)\overline{\Phi(2Ts)}\,ds && (4.2.10)\\
&= \lim_{T\to\infty} \int_{-1/2}^{1/2} \Phi\left(\frac{2Tsq+p}{q}\right)\overline{\Phi(2Ts)}\,ds && (4.2.11)\\
&= \lim_{T\to\infty} \frac{1}{2Tq}\sum_{j=0}^{2Tq-1} \Phi\left(2T\left(-\frac{1}{2}+\frac{j+p}{2Tq}\right)\right)\overline{\Phi\left(2T\left(-\frac{1}{2}+\frac{j}{2Tq}\right)\right)} && (4.2.12)\\
&= \lim_{T\to\infty} \frac{1}{2Tq}\sum_{j=0}^{2Tq-1} \Phi_{T,q}[j+p]\overline{\Phi_{T,q}[j]} && (4.2.13)\\
&= \lim_{T\to\infty} A_p(\Phi_{T,q})[p,0]. && \square
\end{aligned}$$

We now give a specific example illustrating Theorem 4.2.2. We will compute the ambiguity function using both the integral version and using the formula given by (4.2.3). Let, $f(t) = e^{2\pi i t^2}$, $p/q \in \mathbb{Q}$, and $n \in \mathbb{Z}$. First, we compute $A(f)(p/q, n)$

using the integral form,

$$\begin{aligned}
A(f)(p/q,n) &= \int_0^1 e^{2\pi i\left(t+\frac{p}{q}\right)^2} e^{-2\pi i t^2} e^{-2\pi i n t}\,dt && (4.2.14)\\
&= \int_0^1 e^{2\pi i\left[\left(t^2+\frac{2p}{q}t+\frac{p^2}{q^2}\right)-t^2-nt\right]}\,dt && (4.2.15)\\
&= e^{2\pi i p^2/q^2}\int_0^1 e^{(4p-2nq)\pi i t/q}\,dt && (4.2.16)\\
&= \frac{e^{2\pi i p^2/q^2}}{(4p-2nq)\pi i q}\left(e^{(4p-2nq)\pi i/q}-1\right) && (4.2.17)\\
&= \frac{q e^{2\pi i p^2/q^2} e^{(2p-nq)\pi i/q}}{(2p-nq)\pi}\cdot\frac{e^{(2p-nq)\pi i/q}-e^{-(2p-nq)\pi i/q}}{2i} && (4.2.18)\\
&= e^{2\pi i p^2/q^2} e^{(2p-nq)\pi i/q}\mathrm{sinc}((2p-nq)\pi/q). && (4.2.19)
\end{aligned}$$

Now, we turn to the limit form given by (4.2.3). We will show that we will ultimately get the same result as in (4.2.19). We compute,

$$\begin{aligned}
\lim_{k\to\infty} A_p(f_{k,q})[kp,n] &= \lim_{k\to\infty}\frac{1}{kq}\sum_{j=0}^{kq-1} f_{k,q}[j+kp]\overline{f_{k,q}[j]}e^{-2\pi i n j/kq} && (4.2.20)\\
&= \lim_{k\to\infty}\frac{1}{kq}\sum_{j=0}^{kq-1} f\left(\frac{j+kp}{kq}\right) f\left(\overline{\frac{j}{kq}}\right) e^{-2\pi i n j/kq} && (4.2.21)\\
&= \lim_{k\to\infty}\frac{1}{kq}\sum_{j=0}^{kq-1} e^{2\pi i\left(\frac{j+kp}{kq}\right)^2} e^{-2\pi i j^2/k^2q^2} e^{-2\pi i n j/kq} && (4.2.22)\\
&= e^{2\pi i p^2/q^2}\lim_{k\to\infty}\frac{1}{kq}\sum_{j=0}^{kq-1} e^{(4p-2nq)\pi i j/kq^2} && (4.2.23)\\
&= e^{2\pi i p^2/q^2}\lim_{k\to\infty}\frac{1}{kq}\cdot\frac{e^{(4p-2nq)\pi i kq/kq^2}-1}{e^{(4p-2nq)\pi i/kq^2}} && (4.2.24)\\
&= e^{2\pi i p^2/q^2}(e^{(4p-2nq)\pi i/q}-1)\lim_{k\to\infty}\frac{1}{kq}\cdot\frac{1}{e^{(4p-2nq)\pi i/kq^2}-1} && (4.2.25)\\
&= e^{2\pi i p^2/q^2} e^{(2p-nq)\pi i/q}\mathrm{sinc}((2p-nq)\pi/q). && (4.2.26)
\end{aligned}$$

4.3 CAZAC Property Using Distribution Theory

In this section we instead extend the CAZAC property to $\mathbb{R}$ using distribution theory. We begin with a brief exposition of distribution theory and relevant theorems and then define the CAZAC property for tempered distributions. We prove that this property leads to a "CAZAC if and only if the Fourier transform is CAZAC" property.

Definition 4.3.1.

(a) Let $f : \mathbb{R} \to \mathbb{C}$ be an infinitely differentiable function. f is an element of the *Schwartz space* $\mathcal{S}(\mathbb{R})$ if

$$\forall n \in \mathbb{N} \cup \{0\}, \ \|f\|_{(n)} = \sup_{0 \leqslant j \leqslant n} \sup_{t \in \mathbb{R}} (1 + |t|^2)^n |f^{(j)}(t)| < \infty. \tag{4.3.1}$$

(b) The following subspace inclusions hold,

$$C_c^\infty(\mathbb{R}) \subseteq \mathcal{S}(\mathbb{R}) \subseteq L^1(\mathbb{R}) \cap L^2(\mathbb{R}) \cap A(\mathbb{R}).$$

(c) Using (4.3.1) we define the function $\rho : \mathcal{S}(\mathbb{R}) \times \mathcal{S}(\mathbb{R}) \to \mathbb{R}^+$ as

$$\forall f, g \in \mathcal{S}(\mathbb{R}), \ \rho(f, g) = \sum_{n=0}^{\infty} \frac{1}{2^n} \frac{\|f - g\|_{(n)}}{1 + \|f - g\|_{(n)}}. \tag{4.3.2}$$

The major motivation of defining the Schwartz space here is to get an analogue of the $L^2(\mathbb{R})$ theory of Fourier transforms. That is, we want to establish the property that Fourier transforms of Schwartz functions are Schwartz functions. This will in turn, allow us to motivate Fourier transforms of tempered distrubutions. The following theorem establishes the desired property.

Theorem 4.3.2.

(a) *The mapping* $\mathcal{S}(\mathbb{R}) \to \mathcal{S}(\widehat{\mathbb{R}}), f \mapsto \widehat{f}$, *is a bijection.*

(b) *The mapping* ρ *defined by* (4.3.2) *is a metric on* $\mathcal{S}(\mathbb{R})$, *and the metric space* $\mathcal{S}(\mathbb{R})$ *equipped with* ρ *is complete.*

(c) *The Fourier transform mapping of part (a), where* $\mathcal{S}(\mathbb{R})$ *is given the metrizable topology from part (b) is bicontinuous. In particular, the Fourier transform mapping is a matric space isomorphism.*

Definition 4.3.3. A linear function $T : \mathcal{S}(\mathbb{R}) \to \mathbb{C}$, $f \mapsto T(f)$ is a *tempered distribution* if for every sequence $\{f_n\} \subseteq \mathcal{S}(\mathbb{R})$ satisfying

$$\forall k, m \geqslant 0, \lim_{n\to\infty} \|t^m f_n^{(k)}(t)\|_\infty = 0, \tag{4.3.3}$$

we have that $T(f_n) \to 0$. We denote the space of all tempered distributions on $\mathbb{R}$ as $\mathcal{S}'(\mathbb{R})$.

One can show that (4.3.3) is an equivalent condition to $f_n \to 0$ with the metric defined by ρ. Since $\mathcal{S}(\mathbb{R}) \subseteq L^1(\mathbb{R})$, and the Banach dual of $L^1(\mathbb{R})$ is $L^\infty(\mathbb{R})$, we have that $L^\infty(\mathbb{R}) \subseteq \mathcal{S}'(\mathbb{R})$. In particular, this motivates the idea of defining the CAZAC property on $L^\infty(\mathbb{R})$ functions by using the theory of tempered distributions. To make this happen, first we need to define Fourier transform of a tempered distribution. Recall Parseval's formula:

$$\forall f, g \in L^2(\mathbb{R}), \quad \int_{\mathbb{R}} f(t)\overline{g(t)}\, dt = \int_{\mathbb{R}} \widehat{f}(\gamma)\overline{\widehat{g}(\gamma)}\, d\gamma. \tag{4.3.4}$$

By the Riesz Representation Theorem, we can instead view g and $\widehat{g}$ as a test functions, f and $\widehat{f}$ as linear functionals, T_f and $T_{\widehat{f}}$, and now rewrite (4.3.4) instead as

$$\forall f, g \in L^2(\mathbb{R}),\ T_f(\overline{g}) = T_{\widehat{f}}(\overline{\widehat{g}}). \tag{4.3.5}$$

By replacing the test functions in $L^2(\mathbb{R})$ with $\mathcal{S}(\mathbb{R})$ and the linear functionals from $L^2(\mathbb{R})$ with $\mathcal{S}'(\mathbb{R})$ we can define the Fourier transform of tempered distributions as follows.

Definition 4.3.4. Let $T \in \mathcal{S}'(\mathbb{R})$. We define $\widehat{T} \in \mathcal{S}'(\mathbb{R})$ to be the tempered distribution which satisfies

$$\forall f \in \mathcal{S}(\mathbb{R}),\ \widehat{T}(\overline{\widehat{f}}) = T(\overline{f}). \tag{4.3.6}$$

Note that the $L^2(\mathbb{R})$ autocorrelation as defined in Section 4.1 can also be written as $A(f)(-x) = f * \tilde{f}$. Moreover, the proof that a sequence is CAZAC if and only if CAZAC essentially relied upon the exchange formula: $\widehat{f * g} = \widehat{f}\widehat{g}$. To properly establish the CAZAC property we need to make sense of convolving two tempered distributions and multiplying two tempered distributions. To motivate convolution, first let $f, g, h \in \mathcal{S}(\mathbb{R})$. Then,

$$\begin{aligned}
(f * g)(h) &= \int_{\mathbb{R}} (f * g)(t)h(t)\,dt = \int_{\mathbb{R}}\int_{\mathbb{R}} g(t-x)f(x)h(t)\,dx\,dt && (4.3.7)\\
&= \int_{\mathbb{R}} f(x) \int_{\mathbb{R}} g(t-x)h(t)\,dt\ dx && (4.3.8)\\
&= \int_{\mathbb{R}} f(x) \int_{\mathbb{R}} g(y)h(x+y)\,dy\ dx && (4.3.9)
\end{aligned}$$

Imagining f and g as distributions instead, we define the convolution of $S, T \in \mathcal{S}'(\mathbb{R})$ as the following.

Definition 4.3.5. Let $S, T \in \mathcal{S}'(\mathbb{R})$. Then, we define the *convolution of* S and T, $S * T$ by

$$\forall f \in \mathcal{S}(\mathbb{R}),\ (S * T)(f) = S(u)[T(v)[f(u+v)]]. \tag{4.3.10}$$

Definition 4.3.5 is does not give a well-defined definition of convolution for tempered distributions. The main problem is that $T(v)[f(u+v)]$ might not return a function which is in $\mathcal{S}(\mathbb{R})$ in the u variable. To see this, let $S = T = 1 \in \mathcal{S}'(\mathbb{R})$. Let $f \in \mathcal{S}(\mathbb{R})$ be such that $f > 0$ (e.g. $f(t) = \exp(-\pi t^2)$. Then, we have that

$$T(v)[f(u+v)] = \int_{\mathbb{R}} f(u+v)\, dv = \|f\|_1. \tag{4.3.11}$$

In particular, this is a constant function in the u variable which is nonzero. Thus, $S(u)[\|f\|_1] = \infty$ and the convolution is undefined.

Setting aside the question of the existence of the convolution, the final goal is to obtain an exchange formula for tempered distributions, i.e. for $S, T \in \mathcal{S}'(\mathbb{R})$, $S * T = \widehat{S}\widehat{T}$, for certain tempered distributions S and T. The following definition leads to a sufficient condition under which S and T will have an exchange formula.

Definition 4.3.6. Let $S, T \in \mathcal{S}'(\mathbb{R})$. The $\mathcal{S}'(\mathbb{R})$*-convolution of* $S * T$ exists if

$$\forall f, g \in \mathcal{S}(\mathbb{R}),\ (S * f)(\tilde{T} * g) \in L^1(\mathbb{R}), \tag{4.3.12}$$

where $\tilde{T}(t)[g(t)] := T(t)g(-t)$.

It should be noted that if $S \in \mathcal{S}'(\mathbb{R})$ and $f \in \mathcal{S}(\mathbb{R})$, and returning to the formula (4.3.7), we can write $(S * f)$ as $(S * f)(v) = S(u)f(v-u)$. In particular, we can view $S(u)f(v-u)$ as the evaluation of $S(v)[f(v-u)]$ with v as a parameter. Looking at

(4.3.9), we note that for any $g \in \mathcal{S}(\mathbb{R})$, we also have that $(S*f)(g) = S(u)[f*\tilde{g}(-u)]$, where $\tilde{g}(u) = g(-u)$. Since the convolution of two Schwartz functions is still a Schwartz function, $S(u)[(f*\tilde{g})] \leqslant \|S\|_{\mathcal{S}'(\mathbb{R})}\|(f*\tilde{g})\|_{(\mathcal{S}(\mathbb{R}),\rho)}$. In particular, we have that $(S*f)(v)$ is a function on $\mathbb{R}$ and $(S*f)(v) \in \mathbb{C}_b(\mathbb{R})$. Thus, the multiplication in (4.3.12) is well-defined and is in the sense of pointwise multiplication of functions.

Theorem 4.3.7. *Let $S, T \in \mathcal{S}'(\mathbb{R})$ and assume the $\mathcal{S}'(\mathbb{R})$-convoluion of S and T exists. Then, $S*T \in \mathcal{S}'(\mathbb{R})$ and $\widehat{S}$ and $\widehat{T}$ are multiplicable in the sense that,*

$$\widehat{S}\widehat{T} = (S*T)\hat{}. \tag{4.3.13}$$

The multiplication of distributions is a rich theory with many applications, but we shall not go into those details here. We instead turn to defining the CAZAC property for tempered distributions.

Definition 4.3.8. Let $S \in \mathcal{S}'(\mathbb{R})$. We say that S is *constant amplitude* if

$$|\widehat{S}| = 1, \text{ a.e.} \tag{4.3.14}$$

and we say that S is *zero autocorrelation* if the $\mathcal{S}'$-convolution of S with itself exists and,

$$S*S = \delta. \tag{4.3.15}$$

We say that S is *CAZAC* if it satsifes both (4.3.14) and (4.3.15).

Theorem 4.3.9. *Let $S \in \mathcal{S}'(\mathbb{R})$. Furthermore, suppose that the $\mathcal{S}'$-convolution of $\widehat{S}$ with itself exists. Then, S is CAZAC if and only if $\widehat{S}$ is also CAZAC.*

Proof. Suppose S is zero autocorrelation. Since, the $\mathcal{S}'$-convolution exists, by Theorem 4.3.7, we have that

$$(S * S)\widehat{} = |\widehat{S}|^2 = \widehat{\delta} = 1. \tag{4.3.16}$$

In particular, $\widehat{S}$ is constant amplitude. Suppose that S is constant amplitude. Again, by Theorem 4.3.7, we have that

$$(\widehat{S} * \widehat{S}) = (|S|^2)\check{} = \check{1} = \delta. \tag{4.3.17}$$

□

Since $L^\infty(\mathbb{R}) \subseteq \mathcal{S}'(\mathbb{R})$ and the Fourier transform of $f(t) = e^{-2\pi i t^2}$ is $\widehat{f}(\omega) = e^{\pi i \omega^2/2}$, f satisfies this definition of CAZAC property (i.e. for tempered distributions), and more importantly, at least one non-trivial example exists. To close this section, we briefly explain the distributional derivative, which clarifies some of the theory contained in Wiener's original work on generalized harmonic analysis [5] in the next section. To that end, first recall the classic real variable integration by parts formula: For $f, g \in C_c^\infty(\mathbb{R})$,

$$\int_{\mathbb{R}} f'(t)g(t)\,dt = -\int_{\mathbb{R}} f(t)g'(t)\,dt. \tag{4.3.18}$$

From this we obtain the definition of the distributional derivative by instead replacing $f'(t)$ with a linear functional S, $g(t)$ with a Schwartz class function, and view the integration as evaluating the linear functional.

Definition 4.3.10. Let $S \in \mathcal{S}'(\mathbb{R})$. We define the distributional derivative S' to be the S' which satisfies

$$\forall f \in \mathcal{S}(\mathbb{R}),\ S'(f) := -S(f'). \tag{4.3.19}$$

4.4 CAZAC Property Using Wiener's Genrealized Harmonic Analysis

In 1930, Norbert Wiener explored generalizations of the Fourier transform for functions which were in $L^\infty(\mathbb{R})$ but not $L^2(\mathbb{R})$. His primary motivation was to study the spectrum of white light. The result was what he called generalized harmonic analysis, or GHA for short. We present a modernized version of Wiener's GHA with the context of Schwarz's distribution theory added in. A detailed exposition of Wiener's generalized harmonic analysis, as well as many of its mathematical applications, can be found in [13]. The goal of this section is to provide a foundation for analyzing the CAZAC property given by Wiener's generalized harmonic analysis.

Definition 4.4.1. The Banach space dual of $A(\widehat{\mathbb{R}})$ is denoted as $A'(\widehat{\mathbb{R}})$ and is called the space of *pseudo-measures* on $\widehat{\mathbb{R}}$.

If we let $F : L^1(\mathbb{R}) \to A(\widehat{\mathbb{R}})$ be the Fourier transform map and recall that the Banach space dual of $L^1(\mathbb{R})$ is $L^\infty(\mathbb{R})$. Then, the transpose map of F, $F^* : A'(\widehat{\mathbb{R}}) \to L^\infty(\mathbb{R})$ is defined by

$$\forall S \in A'(\widehat{\mathbb{R}}) \text{ and } \forall f \in L^1(\mathbb{R}),\ \langle F^*S, f\rangle = \langle S, Ff\rangle. \tag{4.4.1}$$

Equation 4.4.1 is a small abuse of notation in the sense that given $f \in L^\infty(\mathbb{R}), g \in L^1(\mathbb{R})$ or $f \in A'(\widehat{\mathbb{R}}), g \in A(\widehat{\mathbb{R}})$, by $\langle f, g\rangle$ we really mean $\langle f, g\rangle = T_f(g)$ where T_f is the linear functional associated with f. We shall write $F^*S = \widehat{S}$ and call $\widehat{S} \in L^\infty(\mathbb{R})$ the Fourier transform of S. The cannonical norm on $A'(\widehat{\mathbb{R}})$ is given by $\|S\|_{A'} = \|\widehat{S}\|_\infty$.

Let $S \in A'(\widehat{\mathbb{R}})$, and $\widehat{S} = \Phi \in L^\infty(\mathbb{R})$. We define,

$$\Phi_\Omega(x) := \frac{1}{2\Omega} \int_{-\Omega}^{\Omega} \Phi(t+x)\overline{\Phi(t)}\, dt. \tag{4.4.2}$$

Definition 4.4.2. We define the space $A'_c(\widehat{\mathbb{R}})$, the space of *continuous pseudo-measures*, as the pseudo-measures $S \in A'(\widehat{\mathbb{R}})$ for which

$$\lim_{\Omega\to\infty} \frac{1}{2\Omega} \int_{-\Omega}^{\Omega} |\widehat{S}(t)|^2\, dt = 0. \tag{4.4.3}$$

This definition is primarily inpsired by Wiener's thoerem which characterizes continuous measures, Theorem 4.4.3

Theorem 4.4.3. *Let μ be a Radon measure. μ is continuous if and only if*

$$\lim_{N\to\infty} \frac{1}{2N+1} \sum_{k=-N}^{N} |\widehat{\mu}(k)|^2 = 0. \tag{4.4.4}$$

Next, we define the Wiener transform of a function $\Phi \in L^\infty(\mathbb{R})$. What we will show in Theorem 4.4.5, is that the distributional derivative of the Wiener transform of Φ is the Fourier transform of Φ.

Definition 4.4.4. Let $\Phi \in L^\infty(\mathbb{R})$ and define

$$w_{\Phi,1}(\gamma) = -\int_{|t|>1} \frac{\Phi(t)}{2\pi i t} e^{-2\pi i t\gamma}\, dt, \tag{4.4.5}$$

and

$$w_{\Phi,2}(\gamma) = -\int_{-1}^{1} \frac{\Phi(t)}{2\pi i t} (e^{-2\pi i t\gamma} - 1)\, dt. \tag{4.4.6}$$

The *Wiener transform* of Φ, w_Φ is defined to be $w_\Phi = w_{\Phi,1} + w_{\Phi,2}$.

Theorem 4.4.5. *Let $S \in A'(\widehat{\mathbb{R}})$, and let $\widehat{S} = \Phi \in L^\infty(\mathbb{R})$. Then, $w_\Phi \in L^1_{loc}(\mathbb{R})$ and S is the distributional derivative of w_Φ. Moreover, if we define*

$$\Delta_\varepsilon w_\Phi(\gamma) = \frac{1}{2}(w_\Phi(\gamma+\varepsilon) - w_\Phi(\gamma-\varepsilon)), \tag{4.4.7}$$

then $\Delta_\varepsilon w_\Phi \in L^2(\widehat{\mathbb{R}})$ *and*

$$\widehat{\Delta_\varepsilon w_\Phi}(t) = \varepsilon \Phi(t) \operatorname{sinc}(2\pi\varepsilon t). \tag{4.4.8}$$

Proof. First, note that $\widehat{w_{\Phi,1}}(t) = \Phi(t)\mathbb{1}_{\mathbb{R}\setminus[-1,1]}(t)/(2\pi i t) \in L^2(\mathbb{R})$. Thus, by Plancherel's theorem, $w_{\Phi,1} \in L^2(\widehat{\mathbb{R}})$. Next, note that close to 0, $(e^{-2\pi i t\gamma} - 1)/(2\pi i t)$ converges to $e'(0) = 1$ and thus $w_{\Phi,2} \in L^\infty(\widehat{\mathbb{R}})$. We now conclude that $w_\Phi \in L^2_{\text{loc}}(\widehat{\mathbb{R}}) \subseteq L^1_{\text{loc}}(\widehat{\mathbb{R}})$.

To show that $S = w'_\Phi$, first let $\widehat{f} \in C_c^\infty(\widehat{\mathbb{R}})$. By Parseval's formula and the definition of distributional derivative we have

$$w'_{\Phi,1}(\widehat{f}) = -\int_{\widehat{\mathbb{R}}} w_{\Phi,1}\widehat{f}'(\gamma) = -\langle w_{\Phi,1}, \widehat{f}'\rangle = -\langle \widetilde{w_{\Phi,1}}, (\widehat{f}')\check{}\,\rangle = \langle \Phi, f\rangle. \tag{4.4.9}$$

Next, by Fubini's Theorem and the fact that $\int_{\widehat{\mathbb{R}}} \widehat{f}'(\gamma)\, d\gamma = 0$ [52] we compute

$$\begin{aligned} w'_{\Phi,2}(\widehat{f}) &= -\int_{\widehat{\mathbb{R}}} w_{\Phi,2}(\gamma)\widehat{f}'(\gamma)\, d\gamma = \int_{\widehat{\mathbb{R}}}\int_{-1}^{1} \frac{\Phi(t)}{2\pi i t}(e^{-2\pi i t\gamma} - 1)\widehat{f}'(\gamma)\, dt\, d\gamma && (4.4.10)\\ &= \int_{-1}^{1}\int_{\widehat{\mathbb{R}}} \frac{\Phi(t)}{2\pi i t}(e^{-2\pi i t\gamma} - 1)\widehat{f}'(\gamma)\, d\gamma\, dt && (4.4.11)\\ &= \int_{-1}^{1} \Phi(t)\int_{\widehat{\mathbb{R}}} \widehat{f}'(\gamma)\frac{e^{-2\pi i t\gamma}}{2\pi i t}\, d\gamma\, dt = \int_{-1,1} \Phi(t)f(t)\, dt. && (4.4.12) \end{aligned}$$

Combining (4.4.9) and (4.4.12) gives us that $w'_\Phi = S$.

Finally, to show that $\Delta_\varepsilon w_\Phi \in L^2(\widehat{\mathbb{R}})$ we formally compute the following:

$$\begin{aligned} \frac{1}{2}(w_\Phi(\gamma+\varepsilon) - w_\Phi(\gamma-\varepsilon)) &= -\frac{1}{2}\int_{\mathbb{R}} \Phi(t)\left(\frac{(e^{-2\pi i t(\gamma+\varepsilon)} - e^{-2\pi i t(\gamma-\varepsilon)}}{2\pi i t}\, dt\right) && (4.4.13)\\ &= \int_{\mathbb{R}} \Phi(t)\frac{e^{-2\pi i t\gamma}}{2\pi t}\cdot\frac{e^{2\pi i t\varepsilon} - e^{-2\pi i t\varepsilon}}{2i}\, dt && (4.4.14)\\ &= \int_{\mathbb{R}} \varepsilon\Phi(t)\operatorname{sinc}(2\pi\varepsilon t)e^{-2\pi i t\gamma}\, dt, && (4.4.15) \end{aligned}$$

where the integral in (4.4.15) is understood in the $L^2(\mathbb{R})$ Fourier transform sense. Specifically, $\varepsilon\Phi(t)\operatorname{sinc}(2\pi t\varepsilon) \in L^2(\mathbb{R})$ and so $\Delta_\varepsilon w_\Phi \in L^2(\widehat{\mathbb{R}})$ and its Fourier transform is $\varepsilon\Phi(t)\operatorname{sinc}(2\pi\varepsilon t)$. □

Theorem 4.4.6 (Wiener-Plancharel)**.** *Let $S \in A'(\widehat{\mathbb{R}})$ and $\widehat{S} = \Phi \in L^\infty(\mathbb{R})$. Then $S \in A'_*(\widehat{\mathbb{R}})$ if and only if,*

$$\lim_{\Omega\to\infty} \frac{1}{2\Omega} \int_{-\Omega}^{\Omega} \Phi(t+x)\overline{\Phi(t)}\,dt = \lim_{\varepsilon\to 0} \frac{2}{\varepsilon} \int_{\widehat{\mathbb{R}}} |\Delta_\varepsilon s_\Phi(\gamma)|^2 e^{-2\pi i\gamma x}\,d\gamma. \tag{4.4.16}$$

We now turn to trying to define a CAZAC property using the mean autocorrelation. We begin first by defining the zero autocorrelation property using the mean autocorrelation function.

Definition 4.4.7.

(a) Let $\Phi \in L^\infty(\mathbb{R})$. We say that $\widehat{\Phi} \in A'_*(\widehat{\mathbb{R}}) \subseteq A'(\widehat{\mathbb{R}})$ if $R_T(\Phi)$ converges in the weak-$*$ topology.

(b) $\Phi \in L^\infty(\mathbb{R})$ is said to have *zero mean autocorrelation* if $\widehat{\Phi} \in A'_*(\widehat{\mathbb{R}})$ and $\Phi_\Omega \to 0$ in weak-$*$.

Lemma 4.4.8 is a useful lemma for establishing a sufficient condition under which Φ will have the zero mean autocorrelation property, i.e. Theorem 4.4.9.

Lemma 4.4.8. *Suppose $\{f_n\} \subseteq L^\infty(\mathbb{R})$ is uniformly bounded by K and $\{f_n\} \to f$ almost everywhere. Then, f_n converges to f in the weak-$*$ topology.*

Proof. Fix $g \in L^1(\mathbb{R})$. Our goal is to show that $(f_n - f)[g] \to 0$ as $n \to \infty$. Fix $\varepsilon > 0$. By the monotone convergence theorem, there exists an N such that if $E = [-N, N]$, then

$$\int_{E^c} |g|\,dt < \frac{\varepsilon}{3(K + \|f\|_\infty)}.$$

Furthermore, there exists $\delta > 0$ such that if $\mu(A) < \delta$, then

$$\int_A |g|\,dt < \frac{\varepsilon}{3(K + \|f\|_\infty)}.$$

By Egorov's Theorem there exists another set $F \subseteq E$ such that $f_n \to f$ converges uniformly on F, and $\mu(E\backslash F) < \delta$. In particular, there exists M so that for $n > M$, $\|f_n - f\|_{L^\infty(F)} \leqslant \varepsilon/(3\|g\|_{L^1(F)})$. Thus,

$$\begin{aligned}\left|\int_{\mathbb{R}} (f_n - f)g\,dt\right| &= \left|\int_F (f_n - f)g\,dt + \int_{E\backslash F} (f_n - f)g\,dt + \int_{E^c} (f_n - f)g\,dt\right| \\ &\leqslant \left|\int_F (f_n - f)g\,dt\right| + \left|\int_{E\backslash F} (f_n - f)g\,dt\right| + \left|\int_{E^c} (f_n - f)g\,dt\right| \\ &\leqslant \|f_n - f\|_{L^\infty(F)}\|g\|_{L^1(F)} + \|f_n - f\|_{L^\infty(F\backslash E)}\|g\|_{L^1(F\backslash E)} + \|f_n - f\|_{L^\infty(E^c)}\|g\|_{L^1(E^c)} \\ &\leqslant \varepsilon/3 + \varepsilon/3 + \varepsilon/3 = \varepsilon. \qquad (4.4.17)\end{aligned}$$

□

Theorem 4.4.9. *Let $\Phi \in L^\infty(\mathbb{R})$. Suppose $R_T(\Phi)$ converges pointwise almost everywhere, and suppose $\widehat{\Phi} \in A'(\widehat{\mathbb{R}}) \cap L^\infty(\widehat{\mathbb{R}})$. Then, the ZAC property holds for Φ.*

Proof. By Lemma 4.4.8, we have that $\widehat{\Phi} \in A'_*(\widehat{\mathbb{R}})$. Thus, by Theorem 4.4.6, we have that $R(\Phi)$ is the Fourier transform of $\lim_{\varepsilon\to 0} \frac{2}{\varepsilon}|\Delta_\varepsilon s_\Phi|^2$. We compute,

$$\begin{aligned}|\Delta_\varepsilon s_\Phi(\gamma)|^2 &= \left|\varepsilon \int_{\mathbb{R}} \Phi(t) e^{-2\pi i t\gamma} \operatorname{sinc}(2\pi t\varepsilon)\,dt\right|^2 = \left|\frac{1}{2\pi}\int_{\gamma-\pi\varepsilon}^{\gamma+\pi\varepsilon} \widehat{\Phi}(\omega)\,d\omega\right|^2 \\ &\leqslant \left(\frac{1}{2\pi}\int_{\gamma-\pi\varepsilon}^{\gamma+\pi\varepsilon} |\widehat{\Phi}(\omega)|\,d\omega\right)^2 \leqslant \|\widehat{\Phi}\|_\infty^2 \varepsilon^2.\end{aligned}$$

Thus,

$$\lim_{\varepsilon\to 0} \frac{2}{\varepsilon}|\Delta_\varepsilon s_\Phi(\gamma)| \leqslant \lim_{\varepsilon\to 0} \frac{2}{\varepsilon} \cdot \|\widehat{\Phi}\|_\infty^2 \varepsilon^2 = 0,$$

and we have that μ_Φ must be the zero measure. It then follows that the weak-$*$ limit of $R_T(\Phi)$ must be the zero function. □

Next, we show that $\Phi(t)e^{-2\pi i t^2}$ has the zero mean autocorrelation property.

Proposition 4.4.10. *Let $\Phi(t) = e^{-2\pi i t^2}$. Then, Φ has the zero mean autocorrelation property.*

Proof. This follows from elementary computation:

$$\begin{aligned}
\lim_{\Omega\to\infty} \int_{-\Omega}^{\Omega} \Phi(t+x)\overline{\Phi(t)}\,dt &= \lim_{\Omega\to\infty} \frac{1}{2\Omega}\int_{-\Omega}^{\Omega} e^{-2\pi i(t+x)^2} e^{2\pi i t^2}\,dt && (4.4.18)\\
&= \lim_{\Omega\to\infty} \frac{1}{2\Omega}\int_{-\Omega}^{\Omega} e^{-2\pi i(2tx+x^2)}\,dt && (4.4.19)\\
&= \lim_{\Omega\to\infty} \frac{e^{-2\pi i x^2}}{2\Omega}\cdot \frac{e^{-4\pi i t x}}{-4\pi i x}\Big|_{-\Omega}^{\Omega} && (4.4.20)\\
&= \lim_{\Omega\to\infty} \frac{e^{-2\pi i x^2}\left(e^{-4\pi i \Omega x} - e^{4\pi i \Omega x}\right)}{-8\pi i \Omega x} && (4.4.21)\\
&= 0. && \square
\end{aligned}$$

If $\Phi(t) = e^{-2\pi i t^2}$, then we have seen that $\widehat{\Phi}(\gamma) \in L^\infty(\widehat{\mathbb{R}})$ and $\widehat{\Phi}(\gamma) = e^{\pi i \gamma^2/2}$. Thus, in view of Proposition 4.4.10 and Theorem 4.4.9, it is tempting to define constant amplitude to be the natural definition of constant amplitude if $|\Phi| = 1$ almost everywhere and see if a property along the lines of Φ is CAZAC if and only if $\widehat{\Phi}$ is CAZAC can be proven. However, the following computations will show this is not the case.

Lemma 4.4.11. *Let $\Phi \in L^1(\mathbb{R}) \cap L^\infty(\mathbb{R})$. Then, Φ has the zero mean autocorrelation property.*

Proof. This follows immediately using Hölder's inequality:

$$\lim_{\Omega\to\infty} \frac{1}{2\Omega}\left|\int_{-\Omega}^{\Omega} \Phi(t+x)\overline{\Phi(t)}\,dt\right| \leqslant \lim_{\Omega\to\infty} \frac{\|\Phi\|_\infty \|\Phi\|_1}{2\Omega} = 0. \tag{4.4.22}$$

□

Note as well that if $\Phi \in L^1(\mathbb{R}) \cap L^\infty(\mathbb{R})$, then $\widehat{\Phi} \in A(\widehat{\mathbb{R}}) \cap A'(\widehat{\mathbb{R}})$. Since $A(\widehat{\mathbb{R}}) \subseteq C_0(\widehat{\mathbb{R}}) \subseteq L^\infty(\widehat{\mathbb{R}})$, we have that $\widehat{\Phi} \in A'(\widehat{\mathbb{R}}) \cap L^\infty(\widehat{\mathbb{R}})$. Thus, we can also arrive at the same conclusion using Theorem 4.4.9. We can now see that the Fourier transform of $\Phi \in L^\infty(\mathbb{R})$ being constant amplitude will not be a necessary property for showing Φ has the zero mean autocorrelation property.

Two things still remain unclear: How do we define an appropriate version of the constant amplitude property? The example $\Phi(t) = e^{-2\pi i t^2} + \mathbb{1}_{[-1/2,1/2)}(t)$ is a case where both Φ and $\widehat{\Phi}$ have the zero mean autocorrelation property but neither is constant amplitude. Since $\mathbb{1}_{[-1/2,1/2)}(t)$ and its Fourier transform $\operatorname{sinc}(\pi\gamma)$ go to zero at infinity. It is tempting to define a mean constant amplitude property by asking for convergence to a non-zero value at infinity, but this is also does not work well if we replace $\mathbb{1}_{[-1/2,1/2)}(t)$ with a function that is also in $L^1(\mathbb{R}) \cap L^\infty(\mathbb{R})$ but does not converge at infinity such as

$$\Phi(t) = \sum_{k=1}^{\infty} \mathbb{1}_{[k,k+2^{-k})}(t). \tag{4.4.23}$$

One key property to note though is that if $\Phi(t) = e^{-2\pi i t^2}$, then $\widehat{\Phi} \notin A'_c(\widehat{\mathbb{R}})$ and so it seems that perhaps non-continuous pseudo-measures are the key.

The other question that remains is: What are necessary and sufficient conditions for $\widehat{\Phi} \in A'(\widehat{\mathbb{R}})$ to be in $L^\infty(\widehat{\mathbb{R}})$. Can the mean autocorrelation of Φ be used to establish these conditions? The main thing to hope for is that zero mean autocorrelation is sufficient, and there the results of this section imply that it may be possible.

Chapter 5: Single Pixel Camera Imaging

5.1 The Single Pixel Camera

A modern consumer camera typically contains a single charge-coupled device (CCD) or complementary metal-oxide semiconductor (CMOS) sensor that captures light on a regular grid of picture elements, called pixels. The intensity of light falling on each individual pixel is translated into a numerical value, and theses quantities are in turn processed to render an image.

A Bayer color filter array (CFA) [53] is typically used on the surface of the sensor to obtain red, green, and blue color light sample values at specific pixel locations. The processing of scenes captured with a Bayer CFA require the extra processing step of demosaicing to produce full color images, as opposed to the simpler case of processing grayscale images.

In today's age of megapixel cameras, we can cheaply manufacture a sensor with millions of pixels that is sensitive to the visible light spectrum. Problems arise when we desire similar resolutions for light spectra where the sensors are much more expensive, e.g. infrared or ultra-violet sensors.

Richard G. Baraniuk et al. describe in [54] a single-pixel camera using a digital micromirror device (DMD) and compressed sensing techniques to produce grayscale images. The goal of this brief chapter is to describe an experimental design of an approach that uses a liquid crystal display (LCD) instead of a DMD to implement a single-pixel camera. One of the reasons for this idea is that this design completely linearizes the transmission of light within the device.

The idea is to simulate a pixel grid with an LCD filter and "sum up" the resulting light that comes through it with only a single-pixel light sensor. One hopes that if this is performed correctly, we can obtain a resolution equal to that of the LCD dislplay, with reasonable quality, but at a cheaper cost since we require only a single-pixel sensor.

5.2 Compressed Sensing and the Single Pixel Camera

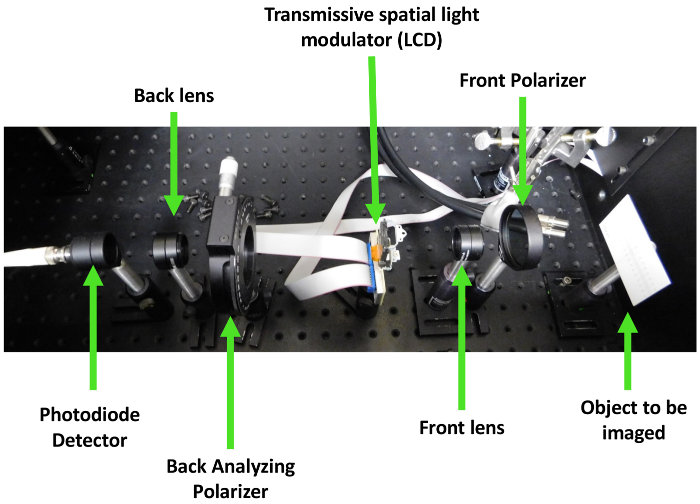

Figure 5.2.1: Physical experimental design. Photo modified from an original provided courtesy of David Bowen, Laboratory for Physical Sciences.

The experimental design that we use is outlined in Figure 5.2.1. Ambient light reflects off the target and passes through the front lens. This lens focuses the light into a beam which is directed at an LCD. The LCD is a grid of squares, say 1024 by 768, which are equivalent to pixels in a sensor. Each square can be switched on or off. This either allows light to pass through, or not, said square, respectively. The total admitted light is captured by the back lens, which then concentrates the light into a single-pixel CCD or CMOS sensor. This sensor counts the incoming photons and gives out a corresponding output voltage, which can be measured.

To model this mathematically, first we can imagine our image as a function $f : \Omega \to \mathbb{R}$, where $\Omega \subseteq \mathbb{R}^2$ can be thought of as the plane containing the image to be captured and the output $f(\mathbf{x})$ can be thought of as the intensity of light per surface unit at point $\mathbf{x} \in \Omega$. We can then discretize the image by splitting it into a rectangular grid of size $m \times n$, where each rectangle corresponds to a single image pixel. We determine the value of light intensity at pixel (i, j) by computing the integral

$$v_{i,j} = \int_{Q_{i,j}} f(\mathbf{x})\, d\mathbf{x},$$

where $Q_{i,j} \subset \Omega$ is the square on the image that corresponds to pixel (i, j). In other words, $v_{i,j}$ is the light intensity of the image at square $Q_{i,j}$, which is the image sample value associated to pixel (i, j). The LCD can be modeled as a vector $\mathbf{p} = (p_0, p_1, \ldots, p_{mn-1})^{\mathrm{T}}$ of length mn, where each entry p_k is either 0 or 1. An entry $p_k = 1$ corresponds to letting the light from $Q_{i,j}$ pass through, and $p_k = 0$ corresponds to blocking it. Note that we have implicitly defined a bijection $(i, j) \leftrightarrow veck$, where vec maps the coordinates (i, j) to their corresponding position k in $\mathbf{p}$. The sensor at the end captures the total light intensity of all the image squares that were not blocked by mask $\mathbf{p}$. Its value is given by the sum,

$$y_{\mathbf{p}} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} v_{i,j} p_{vec(i,j)}. \tag{5.2.1}$$

It is easy to see from Equation (5.2.1) that if we set $p_{vec(0,0)} = 1$, and $p_{vec(i,j)} = 0$ for $i, j \neq 0$, then $y_{\mathbf{p}} = v_{0,0}$. Making a similar arrangement for all possible coordinate pairs (i, j) we can construct mn vectors $\mathbf{p}$ that allow us to recover all mn values $\{v_{i,j}\}$ necessary to recover the discretized image implied by f when using an $m \times n$ LCD. However, this is not very efficient. We can do much better than this.

With a slight adjustment to the formulation given, our experimental setup fits into the framework of compressed sensing [55]. The overall goal is to take $K \ll mn$

measurements and still recover the discretized image described by the set of values $\{v_{i,j}\}$. We organize $\{v_{i,j}\}$ into a vector $\mathbf{v} \in \mathbb{R}^M$, where $M = mn$, utilizing the bijection *vec*, by setting $\mathbf{v} = (v_0, v_1, \ldots, v_{mn-1})^{\mathrm{T}}$, where $v_k = v_{i,j}$ if and only if $k = vec(i, j)$. Then we can write Equation (5.2.1) as the inner product

$$y_{\mathbf{p}} = \langle \mathbf{p}, \mathbf{v} \rangle.$$

We repeat this process to collect K samples $\{y_{\mathbf{p}_l}\}$, with K distinct $\{\mathbf{p}_l\}$ sampling masks, each corresponding to a different LCD configuration. We write in condensed form all K measurements in matrix notation

$$\mathbf{y} = \mathbf{P}^{\mathrm{T}}\mathbf{v},$$

where $\mathbf{P} = (\mathbf{p}_0\ \mathbf{p}_1\ \ldots\ \mathbf{p}_{K-1})$ is the measurement matrix formed with the K column vectors $\{\mathbf{p}_l\}$ corresponding each to a different LCD configuration.

Finally, if there is a basis or frame $\mathbf{A} \in \mathbb{R}^{M \times N}$, with $M \leqslant N$, where image $\mathbf{v}$ has a sparse representation, then we can formulate the problem of reconstructing $\mathbf{v}$ as a compressed sensing problem:

Given $\mathbf{y} \in \mathbb{R}^K$, $\mathbf{P} \in \mathbb{R}^{M \times K}$, and $\epsilon > 0$, find $\mathbf{x}^* \in \mathbb{R}^N$ solving

$$\min_{\mathbf{x} \in \mathbb{R}^N} \|\mathbf{x}\|_0, \quad \text{subject to} \quad \left\|\mathbf{y} - \mathbf{P}^{\mathrm{T}}\mathbf{A}\mathbf{x}\right\|_2 < \epsilon, \tag{5.2.2}$$

where $\|\mathbf{x}\|_0 = \#\{x_i : x_i \neq 0,\ \mathbf{x} = (x_0, x_1, \ldots, x_{N-1})^{\mathrm{T}}\}$.

If image $\mathbf{v}$ is $\epsilon > 0$ close to a sparse representation in the basis or frame $\mathbf{A}$ with at most s nonzero elements, then the theory of compressed sensing can guarantee that we can find a solution $\mathbf{x}^*$ to problem (5.2.2) provided $K = O(s \log(N/s))$.

Algorithms for finding such minimizing $\mathbf{x}^*$ include the Orthogonal Matching Pursuit (OMP) algorithm [56, 57], for example.

With this framework in mind, there are several questions that need to be answered. What $\mathbf{P}$ can we use to obtain a good reconstruction of the original image $\mathbf{v}$? Similarly, what basis or frame matrix $\mathbf{A}$ will lead to good results? Suitable candidates include the Discrete Cosine Transform (DCT) or a wavelet basis tailored for image processing, but these topics need to be explored further. Also, what values of K and ϵ are good choices?

Let $\Phi \in \mathbb{R}^{K\times N}$. Thinking of Φ as $\mathbf{P}^{\mathrm{T}}\mathbf{A}$, then the goal is to figure out what conditions we need on Φ to reconstruct our picture and what algorithms to use. To start, we try to solve the following problem,

$$\min_{\mathbf{x}\in\mathbb{R}^N} \|\mathbf{x}\|_0, \quad \text{subject to } \Phi\mathbf{x} = \mathbf{y}. \tag{5.2.3}$$

This is different than solving problem (5.2.2) in that this seeks exact solutions, ignores noise, and doesn't take into account that computers introduce round-off errors. This problem is easier to treat mathematically, but we will discuss relaxations of (5.2.3) to allow for errors. There are many excellent resources for an introduction to the theory of compressed sensing, but the remainder of this exposition is from an SIAM review article of Bruckstein, Donoho, and Elad [14]. To attack this problem, the first key property is known as the *spark* of matrix Φ.

Definition 5.2.1. The *spark* of a matrix Φ is the smallest number of column vectors of Φ needed to obtain a linearly dependent set.

The spark of a matrix gives a simple criterion for uniqueness of a sparse solution to $\Phi\mathbf{x} = \mathbf{y}$. The idea is that a vector $\mathbf{x}$ in the null-space of Φ must satisfy $\|\mathbf{x}\|_0 \geqslant \text{spark}(\Phi)$. Using this, we get the following theorem.

Theorem 5.2.2. *If a system of linear equations $\Phi\mathbf{x} = \mathbf{y}$ has a solution $\mathbf{x}$ obeying $\|\mathbf{x}\|_0 < spark(\Phi)/2$, then this solution is necessarily the sparest possible solution.*

There is a large computational difficulty in computing the spark of a matrix. This stems from the fact that computing the spark of a matrix would involve a combinatorial search over all possible subsets of columns of Φ, which would require at worst, 2^N checks. One way to circumvent this is to look at the *mutual coherence* of the matrix Φ.

Definition 5.2.3. Let $\Phi \in \mathbb{R}^{K\times N}$ and denote the i-th column of Φ as ϕ_i. The *mutual coherence* of Φ is given by

$$\mu(\Phi) = \max_{1\leqslant i,j\leqslant N, i\neq j} \frac{|\langle \phi_i, \phi_j \rangle|}{\|\phi_i\|_2 \|\phi_j\|_2}.$$

It is known that for full-rank matrices of size $K \times N$, the mutual coherence is bounded below by

$$\mu \geqslant \sqrt{\frac{N-K}{K(N-1)}}.$$

The mutual coherence is much easier to compute than the spark, and the following theorem gives us that the mutual coherence is a lower bound for the spark of a matrix.

Theorem 5.2.4. *For any matrix $\Phi \in \mathbb{R}^{K\times N}$, the following relationship holds,*

$$spark(\Phi) \geqslant 1 + \frac{1}{\mu(\Phi)}.$$

In particular, we can combine this with Theorem 5.2.2, and obtain the following,

Theorem 5.2.5. *If a system of linear equations* $\Phi\mathbf{x} = \mathbf{y}$ *has a solution* $\mathbf{x}$ *obeying*

$$\|\mathbf{x}\|_0 < \frac{1}{2}\left(1 + \frac{1}{\mu(\Phi)}\right),$$

then this solution is necessarily the sparest possible.

As previously mentioned, one of the algorithms which can solve this problem is known as the Orthogonal Matching Pursuit (OMP). This algorithm is detailed beginning on the next page. If the desired solution $\mathbf{x}$ meets the same sparsity requirements as Theorem 5.2.5, then the following theorem states that OMP will always find this solution.

Theorem 5.2.6. *For a system of linear equations* $\Phi\mathbf{x} = \mathbf{y}$ *(*$\Phi \in \mathbb{R}^{K\times N}$ *full-rank), if a solution* $\mathbf{x}$ *exists obeying*

$$\|\mathbf{x}\|_0 < \frac{1}{2}\left(1 + \frac{1}{\mu(\Phi)}\right),$$

then OMP run with threshold parameter $\epsilon = 0$ *is guaranteed to find it exactly.*

Orthogonal Matching Pursuit Algorithm

Task: Approximate the solution of (5.2.3): $\min_{\mathbf{x}} \|\mathbf{x}\|_0$ subject to $\Phi\mathbf{x} = \mathbf{y}$.

Parameters: We are given Φ, $\mathbf{y}$, and the error threshold, ϵ_0.

Initialization: Initialize $k = 0$ and set:

- The initial solution $\mathbf{x}^0 = 0$.
- The initial residue: $\mathbf{r}^0 = \mathbf{y} - \Phi\mathbf{x} = \mathbf{y}$.
- The initial solution support: $\mathcal{S}^0 = \text{supp}(\mathbf{x}^0) = \varnothing$.

Main Iteration: Increment k by 1 and peform the following:

- **Sweep:** Compute the errors $\epsilon(j) = \min_{z_j} \|\phi_j z_j - \mathbf{r}^{k-1}\|_2^2$ for all j using the optimal choice $z_j^* = \phi_j^T \mathbf{r}^{k-1}/\|\phi_j\|_2^2$.
- **Update Support:** Find a minimizer j_0 of $\epsilon(j) : \forall j \notin \mathcal{S}^{k-1}, \epsilon(j_0) \leqslant \epsilon(j)$ and update $\mathcal{S}^k = \mathcal{S}^{k-1} \cup \{j_0\}$.
- **Update Provisional Solution:** Compute $\mathbf{x}^k$, the minimizer of $\|\Phi\mathbf{x} - \mathbf{y}\|_2^2$ subject to $\text{supp}(\mathbf{x}) = \mathcal{S}^k$.
- **Update Residual:** Compute $\mathbf{r}^k = \mathbf{y} - \Phi\mathbf{x}^k$.
- If $\|\mathbf{r}^k\|_2 < \epsilon_0$, then stop. Otherwise, apply another iteration.

Output: The proposed solution x^k is obtained after k iterations.

We now turn to the problem of allowing error or noise in our setup. To be specific, we wish to solve

$$\min_{\mathbf{x}\in\mathbb{R}^N} \|\mathbf{x}\|_0, \quad \text{subject to } \|\Phi\mathbf{x} - \mathbf{y}\|_2 < \epsilon. \tag{5.2.4}$$

With regards to the OMP algorithm, this simply corresponds to running the OMP algorithm with $\epsilon_0 > 0$ as the stopping parameter. Since this leads to an earlier stopping time, this will necessarily lead to a solution at least as sparse as it would find for an exact solution. We also have the following stability result:

Theorem 5.2.7. *Consider the problem (5.2.4). Suppose a sparse vector* $\mathbf{x} \in \mathbb{R}^N$ *satisfies the sparsity constraint* $\|\mathbf{x}_0\|_0 < \frac{1}{2}(1 + 1/\mu(\Phi))$ *and gives a representation of* $\mathbf{y}$ *to within error tolerance* ϵ *(that is,* $\|\mathbf{y} - \Phi\mathbf{x}_0\|_2 \leqslant \epsilon$*). Every solution* $\mathbf{x}_\mathbf{0}^\epsilon$ *to (5.2.4) must obey*

$$\|\mathbf{x}_0^\epsilon - \mathbf{x}_0\|_2^2 \leqslant \frac{4\epsilon^2}{1 - \mu(A)(2\|\mathbf{x}_0\|_0 - 1)}. \tag{5.2.5}$$

5.3 Super-resolution and mosaicing

This final section is a small glipse of the work in progress with Alfredo Nava-Tudela, John Benedetto, and Dave Bowen of the Universty of Maryland Laboratory for the Physical Sciences. As this is all a work in progress, it is hard to capture and quantify all of the plans we have for this project, but this sections serves as a small highlight of the possible avenues we can pursue.

With regards to multiple image super-resolution, one question which arises is: Given two sets of evenly spaced points on $\mathbb{R}$, $\{0, a_1, \cdots, a_M\}$ and $\{0, b_1, \cdots, b_N\}$, can we construct a new set of evenly spaced points $\{0, c_1, \cdots, c_{N'}\}$ where the original two sets are subsets? This question is a 1-dimensional version of trying to align two images where one of them is a sub-pixel shift of the other that also possibly has warping. Unfortunately, the answer to the question as is, is no. If we combine the sets of a_i and b_j into a new increasing sequene $\{0, x_1, x_2, \cdots, x_{M+N}\}$, then if there was a lattice containing both there would be a d such that $md = x_1$ and $nd = x_2$, where m and n are positive integers. Thus,

$$d = \frac{c_1}{m} = \frac{c_2}{n} \implies \frac{m}{n} = \frac{c_1}{c_2}.$$

However, if $c_1 \in \mathbb{R}\backslash\mathbb{Q}$ and $c_2 \in \mathbb{Q}$, this creates a contradiction as the left side is rational and the right side is not.

Digital computer images are comprised of three color channels arranged into layers: red, green, and blue. With this setup, a digital camera needs to capture the red, green, and blue color information from the incoming light at each pixel. This requires a prism to seperate the light into the desired components and a sensor for each of the three channels. In order to cut costs, one would like to reduce the number of sensors per pixel but still be able to represent the image with a reasonable level of quality. To accomplish this, cheaper digital cameras are designed with a filter that lets in color information for only one of the three channels per pixel, but arranges which color each pixel admits in specific patterns. This technique is known as *mosaicing* and the arrangement of color filters used is known as a *color filter array*. The most commonly used color filter array is known as the Bayer filter. The Bayer filter is illustrated with Figure 5.3.1. The result is an image which has incomplete color information in each of the three channels, as illustrated by Figure 5.3.2.

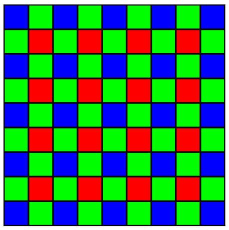

Figure 5.3.1: RGB arrangement of the Bayer color filter.

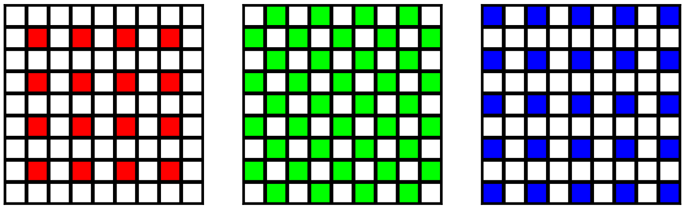

Figure 5.3.2: The RGB componenets of the Bayer color filter seperated.

Note that in the Bayer filter, the pixels tagged with a green color filter comprise 50% of the pixels while the red and the blue channels only comprise 25% of the pixels each. This is because humans are more sensitive to some colors than others. In particular, humans are more sensitive to green than other colors, and so the green light has the largest weight in our perception of how bright or dark an image is. The Bayer color filter leverages this phenomena and takes in more green information since it also doubles as strong luminosity information.

The processing of creating the full image from the mosaic of filtered color information can be seen as a super-resolution problem in the sense that we can view the incomplete color channels as multiple low resolution images which we wish to merge into one higher resolution image. We wish to accomplish this task using the algorithm outlined by Alfredo Nava-Tudela in [58]. The algorithm seeks to restore an image which have some pixels where the information is either missing or corrupted. The algorithm assumes that the locations of bad pixels are known. The process of improving the resolution of multiple low resolution images can be done by taking the low resolution image, placing it on a higher resolution grid, and filling in the missing pixel gaps. As such, it seems suitable to apply Nava-Tudela's algorithm to accomplish reversing mosaicing via super-resolution.

Bibliography

[1] Nadav Levanon and Eli Mozeson. *Radar Signals*. John Wiley & Sons, 2004.

[2] Zukang Shen, Aris Papasakellariou, Juan Montojo, Dirk Gerstenberger, and Fangli Xu. Overview of 3gpp lte-advanced carrier aggregation for 4g wireless communications. *IEEE Communications Magazine*, 50(2), 2012.

[3] Krzysztof Wesołowski, Adrian Langowski, and Krzysztof Bakowski. A novel pilot scheme for 5g downlink transmission. In *Wireless Communication Systems (ISWCS), 2015 International Symposium on*, pages 161–165. IEEE, 2015.

[4] Longsheng Li, Meihua Bi, Weikang Jia, Xin Miao, and Weisheng Hu. Improvement of optical modulation depth tolerance in analog rof by employing cazac and nonlinearity compensation. In *Opto-Electronics and Communications Conference (OECC) and Photonics Global Conference (PGC), 2017*, pages 1–3. IEEE, 2017.

[5] Norbert Wiener. Generalized harmonic analysis. *Acta mathematica*, 55(1):117–258, 1930.

[6] Qi Pian, Ruoyang Yao, Lingling Zhao, and Xavier Intes. Hyperspectral time-resolved wide-field fluorescence molecular tomography based on structured light and single-pixel detection. *Optics letters*, 40(3):431–434, 2015.

[7] Wai Lam Chan, Kriti Charan, Dharmpal Takhar, Kevin F Kelly, Richard G Baraniuk, and Daniel M Mittleman. A single-pixel terahertz imaging system based on compressed sensing. *Applied Physics Letters*, 93(12):121105, 2008.

[8] John J. Benedetto, Katherine Cordwell, and Mark Magsino. CAZAC sequences and Haagerup's characterization of cyclic n-roots. In C. Cabrelli, U. Molter, et al., editors, *New Trends in Applied Harmonic Analysis: Sparse Representations, Compressed Sensing, and Multifractal Analysis II*. Birkhäuser, 2018. to appear.

[9] John J. Benedetto, Ioannis Konstantinidis, and Muralidhar Rangaswamy. Phase-coded waveforms and their design. *IEEE Signal Processing Magazine*, 26(1):22–33, 2009.

[10] John J. Benedetto and Jeffrey J. Donatelli. Ambiguity function and frame-theoretic properties of periodic zero-autocorrelation waveforms. *IEEE Journal of Selected Topics in Signal Processing*, 1(1):6–20, 2007.

[11] Mark Magsino. Constructing tight Gabor frames using CAZAC sequences. *Sampling Theory in Signal and Image Processing*, 16:73–99, 2017.

[12] John J Benedetto. *Harmonic analysis and applications*, volume 23. CRC Press, 1996.

[13] John J Benedetto. *Spectral synthesis*, volume 66. Academic press, 1976.

[14] Alfred Bruckstein, David Donoho, and Michael Elad. From sparse solutions of systems of equations to sparse modeling of signals and images. *SIAM Review*, 51(1):34–81, 2009.

[15] Uffe Haagerup. Cyclic p-roots of prime lengths and complex Hadamard matrices. *arXiv preprint arXiv:0803.2629*, 2008.

[16] Göran Björck and Bahman 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*, 320(3):319–324, 1995.

[17] Andrzej Milewski. Periodic sequences with optimal properties for channel estimation and fast start-up equalization. *IBM Journal of Research and Development*, 27(5):426–431, 1983.

[18] Wojciech Bruzda, Wojciech Tadej, and Karol Życzkowski. Complex Hadamard matrices–a catalogue. http://chaos.if.uj.edu.pl/ karol/hadamard/?q=catalogue.

[19] Ingemar Bengtsson, Wojciech Bruzda, Åsa Ericsson, Jan-Åke Larsson, Wojciech Tadej, and Karol Życzkowski. Mutually unbiased bases and hadamard matrices of order six. *Journal of mathematical physics*, 48(5):052106, 2007.

[20] Göran 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*, pages 131–140. Springer, 1990.

[21] John J. Benedetto, Robert L. Benedetto, and Joseph T. Woodworth. Optimal ambiguity functions and Weil's exponential sum bound. *Journal of Fourier Analysis and Applications*, 18(3):471–487, 2012.

[22] Andrew Kebo, Ioannis Konstantinidis, John J. Benedetto, Michael R. Dellomo, and Jeffrey M. Sieracki. Ambiguity and sidelobe behavior of CAZAC coded waveforms. In *2007 IEEE Radar Conference*, pages 99–103. IEEE, 2007.

[23] Uffe Haagerup. *Orthogonal maximal abelian-subalgebras of the nxn matrices and cyclic n-roots*. Citeseer, 1996.

[24] Göran Björck and Ralf Fröberg. A faster way to count the solutions of inhomogeneous systems of algebraic equations, with applications to cyclic n-roots. *Journal of Symbolic Computation*, 12(3):329–336, 1991.

[25] Peter Stevenhagen and Hendrik Willem Lenstra. Chebotarëv and his density theorem. *The Mathematical Intelligencer*, 18(2):26–37, 1996.

[26] Terence Tao. An uncertainty principle for cyclic groups of prime order. *Mathematics Research Letters*, 12:121–127, 2005.

[27] Audrey Terras. *Fourier analysis on finite groups and applications*, volume 43. Cambridge University Press, 1999.

[28] David L. Donoho and Philip B. Stark. Uncertainty principles and signal recovery. *SIAM Journal on Applied Mathematics*, 49(3):906–931, June 1989.

[29] Kennan T Smith. The uncertainty principle on groups. *SIAM Journal on Applied Mathematics*, 50(3):876–882, 1990.

[30] Walter Rudin. *Function theory in the unit ball of Cn*, volume 241. Springer Science & Business Media, 2012.

[31] Richard J. Duffin and Albert C. Schaeffer. A class of nonharmonic Fourier series. *Transactions of the American Mathematics Society*, 72(2):341–366, 1952.

[32] Ingrid Daubechies. *Ten Lecutres on Wavelets*, volume 61. SIAM, 1992.

[33] Stéphane Mallat. *A Wavelet Tour of Signal Processing*. Academic press, 1999.

[34] Dustin Mixon. Sparse signal processing with frame theory. *arXiv preprint arXiv:1204.5958*, 2012.

[35] Götz Pfander and David Walnut. Measurement of time-variant linear channels. *IEEE Transactions on Information Theory*, 52(11):4808–4820, 2006.

[36] Thomas Strohmer. Approximation of dual Gabor frames, window decay, and wireless communications. *Applied and Computational Harmonic Analysis*, 11(2):243–262, 2001.

[37] Jelena Kovačević and Amina Chebira. Life beyond bases: The advent of frames. *IEEE Signal Processing Magazine*, 2007.

[38] Jelena Kovačević and Amina Chebira. Life beyond bases: The advent of frames (part ii). *IEEE Signal Processing Magazine*, 5(24):115–125, 2007.

[39] Radu Balan, Peter G. Casazza, Christopher Heil, and Zeph Landau. Density, overcompleteness, and localization of frames. I. Theory. *Journal of Fourier Analysis and Applications*, 12(2):105–143, 2006.

[40] Radu Balan, Peter G. Casazza, Christopher Heil, and Zeph Landau. Density, overcompleteness, and localization of frames. II. Gabor systems. *Journal of Fourier Analysis and Applications*, 12(3):307–344, 2006.

[41] Peter G. Casazza and Gitta Kutyniok, editors. *Finite Frames: Theory and Applications.* Birkhäuser Basel, 2013.

[42] Ole Christensen. *An Introduction to Frames and Riesz Bases.* Applied and Numerical Harmonic Analysis. Springer International Publishing, 2016.

[43] John J. Benedetto and Matthew Fickus. Finite normalized tight frames. *Advances in Computational Mathematics*, 18(2-4):357–385, 2003.

[44] Peter G. Casazza and Jelena Kovačević. Equal-norm tight frames with erasures. *Advances in Computational Mathematics*, 18(2-4):387–430, 2003.

[45] Ingrid Daubechies, Bin Han, Amos Ron, and Zuowei Shen. Framelets: MRA-based constructions of wavelet frames. *Applied and Computational Harmonic Analysis*, 14(1):1–46, 2003.

[46] Richard Vale and Shayne Waldron. Tight frames and their symmetries. *Constructive Approximation*, 21(1):83–112, 2004.

[47] Richard Vale and Shayne Waldron. Tight frames generated by finite nonabelian groups. *Numerical Algorithms*, 48(1-3):11–27, 2008.

[48] Gitta Kutyniok, Kasso A. Okoudjou, Friedrich Philipp, and Elizabeth K. Tuley. Scalable frames. *Linear Algebra and its Applications*, 438(5):2225–2238, 2013.

[49] Karlheinz Gröchenig. *Foundations of Time-Frequency Analysis.* Springer Science & Business Media, 2013.

[50] Götz Pfander. Gabor frames in finite dimensions. In *Finite Frames*, pages 193–239. Springer, 2013.

[51] David F. Walnut. *Weyl-Heisenberg Wavelet Expansions: Existance and Stability in Weighted Spaces.* PhD thesis, University of Maryland, 1989.

[52] John J Benedetto and Wojciech Czaja. *Integration and modern analysis.* Springer Science & Business Media, 2010.

[53] Bryce E. Bayer. Color imaging array, July 1976. US Patent 3,971,065.

[54] Marco F. Duarte, Mark A. Davenport, Dharmpal Takhar, Jason N. Laska, Ting Sun, Kevin F. Kelly, and Richard G. Baraniuk. Single-pixel imaging via compressive sampling. *IEEE Signal Processing Magazine*, 25(2):83 – 91, March 2008.

[55] Dana Mackenzie. *Compressed Sensing Makes Every Pixel Count*, volume 7 of *What's Happening in the Mathematical Sciences*, pages 114 – 127. American Mathematical Society, 2009.

[56] Y. Pati, R. Rezaiifar, and P. Krishnaprasad. Orthogonal matching pursuit: recursive function approximation with application to wavelet decomposition. In *27th Asilomar Conference on Signals, Systems and Computers, 1993*, pages 40–44, 1993.

[57] Stéphane G. Mallat and Zhifeng Zhang. Matching pursuits with time-frequency dictionaries. *IEEE Transactions on Signal Processing*, 41(12):3397–3415, December 1993.

[58] Alfredo Nava-Tudela. A recommender system to restore images with impulse noise. https://arxiv.org/abs/1702.07679, February 2016. arXiv:1702.07679 [cs.CV].