# Perfect Sequences and Arrays of Unbounded Lengths and Sizes over the Basic Quaternions

Santiago Barrera Acevedo

Submitted in total fulfilment of the requirements of the degree of

Doctor of Philosophy

School of Mathematical Sciences
MONASH UNIVERSITY

January 2013

# DECLARATION

This is to certify that

1. the thesis comprises only my original work towards the PhD,
2. due acknowledgement has been made in the text to all other material used,
3. the thesis is less than 100,000 words in length, exclusive of tables, maps, bibliographies and appendices.

Santiago Barrera Acevedo, January 2013

# ACKNOWLEDGEMENTS

In preparation of this thesis, I gratefully acknowledge the assistance and support provided by my supervisor, Dr. Tom Eric Hall, for giving me the opportunity to undertake Ph.D. Studies and do research; for his encouragement, insightful comments and helpful suggestions.

I would also like to thank the School of Mathematical Sciences, in particular, Mrs. Gertrude Nayak, manager of the school, for her selfless concern for my well-being and all her assistance and support throughout my studies.

Finally, I would like to thank my parents for their love and support throughout these years.

# ABSTRACT

THE aim of this Thesis is to provide new understanding of the existence of perfect sequences and arrays over the alphabets of quaternions and complex numbers, and multi-dimensional arrays with recursive autocorrelation.

Perfect sequences over the quaternion algebra $\mathbb{H}$ were first introduced by O. Kuznetsov in 2009. The quaternion algebra is a non-commutative ring, and for this reason, the concepts of right and left autocorrelation and right and left perfection were introduced. Kuznetsov showed that the concepts of right and left perfection are equivalent.

One year later, O. Kuznetsov and T. Hall showed a construction of a perfect sequence of length $5,354,228,880$ over a quaternion alphabet with 24 elements, namely the double-trahedron group $\mathbb{H}_{24}$. The authors made the following conjecture: there are perfect sequences of unbounded lengths over the double tetrahedron group $\mathbb{H}_{24}$.

We worked on this conjecture and found a family of perfect sequences of **unbounded lengths** over $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, which is an alphabet more likely to be implemented in Electronic Communication, being smaller than $\mathbb{H}_{24}$ and easier to handle.

In our proof of Kuznetsov and Hall's conjecture, we show that Lee sequences, which are defined over the alphabet $\{0, 1, -1, i, -i\}$ and exist for unbounded lengths, can always be converted, with perfection preserved, into sequences over the basic quaternions $\{1, -1, i, -i, j\}$.

More generally, we show that every sequence over the complex numbers, that is palindromic about one or two zero-centres, can be converted into a sequence over the quaternions $\mathbb{H}$, preserving its off-peak autocorrelation values. Then, we use the existence of Lee sequences of unbounded lengths to show the existence of perfect sequences over the basic quaternions $\{1, -1, i, -i, j\}$ of unbounded lengths. We call these sequences over the basic quaternions, by the name, modified Lee sequences.

We then use Lee sequences and modified Lee sequences to show the existence of perfect sequences of odd unbounded lengths over the following alphabets: $G = \{\pm 1 \pm i, i\}$, $U_4^* = \{\pm 1, \pm i, \frac{1 \pm i}{2}\}$ and $T = \{\pm 1 \pm i, 1 \pm j\}$.

Once the question of the existence of perfect sequences of unbounded lengths over the basic quaternions is answered, the next question posed in this work concerns arrays: can the array inflation algorithm by Arasu and de Launey be extended to perfect arrays over the basic quaternions? In order to answer this second question, we show that Arasu and de Launey's algorithm can be modified to inflate perfect arrays over the basic quaternions, preserving perfection and giving approximately equal numbers of the eight basic quaternions $1, -1, i, -i, j, -j, k$ and $-k$.

We also show that all modified Lee Sequences of length $m = p + 1 \equiv 2(mod\ 4)$, where $p$ is a prime number, can be folded into a perfect two-dimensional array (with only one occurrence of the element $j$) of size $2 \times \frac{m}{2}$, with $GCD(2, \frac{m}{2}) = 1$. Each of these arrays can then be inflated into a perfect array of size $2p \times \frac{m}{2}p$, with approximately equal numbers of the eight basic quaternions $1, -1, i, -i, j, -j, k$ and $-k$. And so, we have a family of perfect arrays of unbounded sizes over the basic quaternions.

# CONTENTS

CHAPTER

# 1

# INTRODUCTION

## 1.1 Introduction

THIS work shows the existence of **perfect sequences of unbounded lengths** and **perfect arrays of unbounded sizes**, over the basic quaternion alphabet $\{1, -1, i, -i, j, -j, k, -k\}$. This work also shows the existence of **perfect sequences of odd unbounded lengths** over the complex and quaternion alphabets $\{\pm 1, \pm i, \frac{1 \pm i}{2}\}$, $\{\pm 1 \pm i, i\}$ and $\{\pm 1 \pm i, 1 \pm j\}$. In addition, this work shows a construction of **muti-dimensional arrays** with **recursive autocorrelation function**.

Perfect sequences over the **quaternion algebra** $\mathbb{H} = \{a + bi + cj + dk | a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1, ij = -ji = k\}$ were first introduced by O. Kuznetsov in 2009 [45]. The quaternion algebra is a non-commutative ring, that is, there are quaternions $p$ and $q$ in $\mathbb{H}$, for which $pq \neq qp$. For this reason, the concepts of right and left autocorrelation, and right and left perfection, were introduced. Kuznetsov showed that the concepts of right and left perfection are equivalent [45].

One year later, O. Kuznetsov and T. Hall showed a construction of a perfect sequence of length $5,354,228,880$ over a quaternion alphabet with 24 elements, namely the double-tetrahedron group $\mathbb{H}_{24} = \{\pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2}\} \subset \mathbb{H}$ [47]. The authors made the following conjecture: there are perfect sequences of unbounded lengths over the double-tetrahedron group $\mathbb{H}_{24}$.

We worked on this conjecture and found a family of perfect sequences of **unbounded lengths** over $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, which is an alphabet more likely to be implemented in Electronic Communication, being smaller than $\mathbb{H}_{24}$ and easier to handle.

In our solution of Kuznetsov and Hall's conjecture, we show that all **Lee sequences**, which are defined over the alphabet $\{0, 1, -1, i, -i\}$ [49], can always be converted, with perfection preserved, into sequences over the basic quaternions $\{1, -1, i, -i, j\} \subset \mathbb{H}_8$.

More generally, we show that every sequence over the complex numbers, that is palindromic about one or two zero-centres, can be converted into a sequence over the quaternions $\mathbb{H}$, preserving its off-peak autocorrelation values. Then, we use the existence of Lee sequences of unbounded lengths [49], [54] to show the existence of sequences over the basic quaternions $\{1, -1, i, -i, j\} \subset \mathbb{H}$ of unbounded lengths. We call these perfect sequences over the basic quaternions, by the name, **modified Lee sequences**.

It is known that perfect sequences, whose lengths are a product of two co-prime numbers, can be transformed into perfect sequences of smaller lengths by the Sequence-of-balances-of-decimations Theorem [46]. We use this result combined with Lee sequences and modified Lee sequences to construct new families of perfect sequences over the following alphabets: $G = \{\pm 1 \pm i, i\}$, $U_4^* = \{\pm 1, \pm i, \frac{1 \pm i}{2}\}$ and $GH = \{\pm 1 \pm i, 1 \pm j\}$.

Regarding perfect arrays, in this work we state and answer the questions: are there perfect two-dimensional arrays of unbounded sizes over the basic quaternions $\{1, -1, i, -i, j, -j, k, -k\}$? If so, can we produce these arrays with random occurrences of the elements $1, -1, i, -i, j, -j, k, -k$? In order to answer these two questions, we first show that **Arasu and de Launey's algorithm**, to inflate **perfect quaternary arrays** [4], can be used to inflate perfect arrays over the basic quaternions, and preserve their perfection. We also show that all modified Lee sequences (in the sense [10]) of length $m = p + 1 \equiv 2 \ (mod\ 4)$, where $p$ is a prime number, can be folded into a perfect two-dimensional array (with only one occurrence of the element $j$) of size $2 \times \frac{m}{2}$, with $GCD(2, \frac{m}{2}) = 1$. Each of these arrays can be inflated into a perfect array of size $2p \times \frac{m}{2}p$, with random occurrences of all the elements $1, -1, i, -i, j, -j, k, -k$.

Regarding **multi-dimensional arrays**, Antweiler et al [2] showed that the kronecker product of a perfect sequence with a two-dimensional aperiodic perfect array is also a perfect array. Using this idea, they showed that perfect three and higher dimensional arrays can be constructed. Following on from their work, we construct new arrays by combining a finite sequence $S$ of length $n_0$ with special selected shifts of a finite $(m-1)$-dimensional array $\boldsymbol{A}$ of size $n_1 \times \cdots \times n_{m-1}$, that is, we modify the construction in [2] by (1) using a new shift of $\boldsymbol{A}$ for each multiplication by an element of $S$ and (2) with not necessarily all shifts of $\boldsymbol{A}$ involved. The autocorrelation function of the new $m$-dimensional array is the product of the autocorrelation functions of the sequence $S$ and the array $\boldsymbol{A}$. So, if the seed sequence and array have perfect autocorrelation, then the newly constructed array also has perfect autocorrelation.

We generalise our construction to the use of any sequence whose length is any multiple of $LCM(\frac{n_1}{d_1}, \ldots, \frac{n_{m-1}}{d_{m-1}})$, where each $d_i$ is any chosen divisor of $n_i$ ( in the case where each $d_i = n_i$, the diagonal construction is obtained). There need be no bound on the length of the seed sequence, since, while there is very likely to be a bound of $n^2$ on the length of perfect sequences over the $n$-roots of unity, there also exist several types of sequences over real numbers, complex numbers, and recently quaternions, which are perfect and of unbounded lengths. There are also arrays, over 4 roots of unity, of unbounded sizes, constructed by Arasu and de Launey [4], that can be used in our construction.

## 1.2 Summary

The present work consists of 12 Chapters.

- In Chapter 1, Introduction, a brief overview of the material that follows is given.

**Literature Survey: Perfect Sequences and Arrays**.

- In Chapter 2, Notation and Definitions, some general definitions, used in the following Chapters, are given, and notation, adopted throughout this work, is introduced.
- In Chapter 3, Perfect Sequences and Arrays over the Complex Numbers $\mathbb{C}$, properties of perfect sequences are introduced, conditions for perfection are discussed, known constructions of perfect sequences are presented and some facts about the non-existence of perfect sequences are considered. Then, perfect Multidimensional Arrays over the Complex Numbers

$\mathbb{C}$, properties of perfect arrays are introduced and known constructions of perfect arrays are presented and some results on the existence of perfect binary, ternary and quaternary arrays are considered.

- In Chapter 4, Perfect Sequences over the Quaternions $\mathbb{H}$, the concepts of left and right autocorrelation is presented, likewise the concepts of left and right perfection are presented and the equivalence between these concepts is shown.
- In Chapter 5, Lee Sequences, an introduction to Lee sequences, their properties and discovery is presented. The existence of infinitely many Lee sequences is also considered.

Together, Chapters 3, 4 and 5 can be regarded as the literature review. Chapter 4 and 5 also provide a background for understanding the material that follows. More specific concepts will be explained in each particular chapter.

**Research Results: Perfect Sequences and Arrays**.

- In Chapter 6, Perfect Sequences of Unbounded Lengths over the Basic Quaternions, the concepts of palindromic sequences about one and two zero-centres are introduced. Some results on transformations, that preserve autocorrelation, of palindromic sequences about one and two zero-centres, over the complex numbers, into quaternion sequences, are presented. The existence of perfect sequences of unbounded lengths over the basic quaternions $\{1, -1, i, -i, j, -j, k, -k\}$ is shown.
- In Chapter 7, Perfect Sequences of Odd Unbounded Lengths over the Quaternions, the existence of perfect sequences of unbounded lengths over the alphabets $\{\pm 1 \pm i, i\}$, $\{\pm 1, \pm i, \frac{1 \pm i}{2}\}$ and $\{\pm 1 \pm i, 1 \pm j\}$ is shown.
- In Chapter 8, Inflation and Size Reduction of Perfect Arrays over the Basic Quaternions, the important inflation algorithm of Arasu and de Launy is

generalised to perfect arrays over the basic quaternions.

- In Chapter 9, Perfect Arrays over the Basic Quaternions of Unbounded Sizes, a family of perfect arrays over the basic quaternions, of unbounded sizes, is shown.
- In Chapter 10, Perfect $m$-Dimensional Arrays with a Recursive Autocorrelation Function, two generalisations of the Product Theorem of composition of sequences are presented. These constructions produce perfect $m$-dimensional arrays with recursive autocorrelation function.
- In Chapter 11, Conclusion.
- In Chapter 12, Bibliography.

# Part I

# Literature Review: Perfect Sequences and Arrays

CHAPTER

# 2

# NOTATION AND DEFINITIONS

IN this chapter, we present the general definitions and notations used throughout this work. More specific concepts will be explained in each particular chapter.

## 2.1 Sequences

**Definition 2.1.** *Finite sequence.*
*An ordered $n$-tuple $\boldsymbol{S} = (s_0, s_1, \ldots, s_{n-1})$ of elements from a set $\mathcal{A}$ is called a **sequence**. The set $\mathcal{A}$ is called the **alphabet** and $n$ is called the **length** of the sequence $\boldsymbol{S}$.*

**Definition 2.2.** *Period of a sequence.*

*Let $\boldsymbol{S} = (s_0, s_1, \ldots, s_{n-1})$ be a sequence over an alphabet $\mathcal{A}$. The smallest positive integer $l$, such that $s_{i+l} = s_i$, for $0 \leq i \leq n-1$, is called the* ***period*** *of the sequence $\boldsymbol{S}$.*

**Definition 2.3.** *Norm of a sequence.*

*The* ***norm*** *of a sequence is defined as the sum of the norms of all its elements*

$$||\boldsymbol{S}|| = \sum_{i=0}^{n-1} ||s_i||. \tag{2.1}$$

**Definition 2.4.** *Balance of a sequence.*

*The sum of all elements of a sequence $\boldsymbol{S}$ is called the* ***balance*** *of the sequence $\boldsymbol{S}$ and it is denoted by $\sum s$.*

**Definition 2.5.** *Shift of a sequence.*

*For every integer $\tau \geq 0$, the $\tau$-**shift** (to the left) of the sequence $\boldsymbol{S} = (s_0, s_1, \ldots, s_{n-1})$, denoted by $\boldsymbol{S}^\tau$, is the sequence $\boldsymbol{S}^\tau = (s_\tau, s_{\tau+1}, \ldots, s_{\tau+n-1})$, where the indices $\tau, \tau+1, \ldots, \tau+n-1$ are calculated modulo $n$.*

**Definition 2.6.** *Dot product of sequences.*

*Let $\boldsymbol{S} = (s_0, s_1, \ldots, s_{n-1})$ and $\boldsymbol{T} = (t_0, t_1, \ldots, t_{n-1})$ be two sequences of same length. The* ***dot product*** *of sequences $\boldsymbol{S}$ and $\boldsymbol{T}$ is*

$$\boldsymbol{S} \cdot \boldsymbol{T} = \sum_{i=0}^{n-1} s_i t_i^* \ , \tag{2.2}$$

*where $t_i^*$ denotes the complex conjugate of $t_i$.*

**Definition 2.7.** *Periodic cross-correlation and autocorrelation of sequences.*

*For an integer $\tau \geq 0$, the* ***periodic cross-correlation*** *of two same-length sequences $\boldsymbol{S} = (s_0, s_1, \ldots, s_{n-1})$ and $\boldsymbol{T} = (t_0, t_1, \ldots, t_{n-1})$, for the shift $\tau$ is*

$$CC_{\boldsymbol{S},\boldsymbol{T}}(\tau) = \sum_{i=0}^{n-1} s_i t_{i+\tau}^* \ , \tag{2.3}$$

*where $i+\tau$ is calculated modulo n. When $\boldsymbol{S}=\boldsymbol{T}$, we write $CC_{\boldsymbol{S},\boldsymbol{T}}(\tau)=AC_{\boldsymbol{S}}(\tau)$ and $AC_{\boldsymbol{S}}(\tau)$ is called the* ***periodic autocorrelation*** *value of the sequence* $\boldsymbol{S}$*, for the shift* $\tau$*. In terms of the dot product, the autocorrelation value for the shift* $\tau$ *is*

$$AC_{\boldsymbol{S}}(\tau)=\boldsymbol{S}\cdot\boldsymbol{S}^{\tau}=\sum_{i=0}^{n-1}s_i s_{i+\tau}^{*}. \tag{2.4}$$

**Definition 2.8.** *Peak and off-peak values of a sequence.*
*Let $\boldsymbol{S}=(s_0,s_1,\ldots,s_{n-1})$ be a sequence over an alphabet $\mathcal{A}$. The autocorrelation value of S, for the shit $\tau=0$, is called the* ***peak value****. The autocorrelation values of S, for all shifts $\tau\neq 0$, are called* ***off-peak values****.*

**Definition 2.9.** *Decimation of a sequence.*
*Let $\boldsymbol{S}=(s_i)$ be a sequence of period n and length l, over an alphabet $\mathcal{A}$. Now, for $j>0$, consider the sequence defined by $t_i=s_{ij}$, for $i=0,\ldots,n-1$, where the product ij is calculated mod l. The sequence $\boldsymbol{T}=(t_i)$ is said to be the* ***decimation*** *by j of the sequence $\boldsymbol{S}=(s_i)$. If j divides n, then $\boldsymbol{T}$ has period $\frac{n}{j}$. If $gcd(n,j)=1$, then the period of $\boldsymbol{T}$ is n and the decimation is said to be* ***proper****. In general, a decimation by j of the sequence with period n produces a sequence with period $\frac{n}{gcd(n,j)}$.*

**Definition 2.10.** *Perfect sequence.*
*A sequence $\boldsymbol{S}=(s_0,s_1,\ldots,s_{n-1})$ over the alphabet $\mathcal{A}$ is called* ***perfect*** *if all off-peak values are zero, that is, for all shifts $\tau\neq 0$, we have $AC_{\boldsymbol{S}}(\tau)=0$.*

**Example 2.1.** *Let i be a fourth root of unity. The sequence $\boldsymbol{S}=(1,i,-1,i)$ of length 4 is perfect, since $AC_{\boldsymbol{S}}(\tau)=0$, for $\tau\neq 0$.*

## 2.2 Arrays

We now introduce the basic definitions regarding multi-dimensional arrays.

**Definition 2.11.** *Multi-dimensional array.*

*A **finite m-dimensional array** $\{a(i_0, i_1, \ldots, i_{m-1})\}$, where $0 \le i_j \le n_j - 1$ and $0 \le j \le m-1$, over the set $\mathcal{A}$, is a collection of $n_0 \times n_1 \times \cdots \times n_{m-1}$ elements taken from $\mathcal{A}$, where repetition is allowed. The expression $n_0 \times n_1 \times \cdots \times n_{m-1}$ is called the size of the array and $\mathcal{A}$ is called the alphabet. In particular, a finite two-dimensional array is a matrix and a finite one-dimensional array is a finite sequence.*

**Definition 2.12.** *Period of an array.*

*Let $\boldsymbol{A} = \{a(i_0, i_1, \ldots, i_{m-1})\}$ be an array over an alphabet $\mathcal{A}$, where $0 \le i_j \le n_j - 1$ and $0 \le j \le m-1$. The list of the smallest positive integers $l_0, l_1, \ldots, l_{m-1}$, such that*

$$a(i_0 + l_0, i_1 + l_1, \ldots, i_{m-1} + l_{m-1}) = a(i_0, i_1, \ldots, i_{m-1}) , \tag{2.5}$$

*for $0 \le i_j \le n_j - 1$ and $0 \le j \le m-1$, is called the **period** of the array $\boldsymbol{A}$.*

**Definition 2.13.** *Shift of an array.*

*For an m-tuple $(j_0, j_1, \ldots, j_{m-1})$, the m-shift of an array $\boldsymbol{A} = \{a(i_0, i_1, \ldots, i_{m-1})\}$, denoted by $\boldsymbol{A}^{(j_0, j_1, \ldots, j_{m-1})}$, is the array*

$$\boldsymbol{A}^{(j_0, j_1, \ldots, j_{m-1})} = \{a(i_0 + j_0, i_1 + j_1, \ldots, i_{m-1} + j_{m-1})\} , \tag{2.6}$$

*where indices are calculated modulo $n_j$, for $0 \le j \le m-1$.*

**Definition 2.14.** *Dot product of arrays.*

*Let $\boldsymbol{A} = \{a(i_0, i_1, \ldots, i_{m-1})\}$ and $\boldsymbol{B} = \{b(i_0, i_1, \ldots, i_{m-1})\}$ be two multi-dimensional arrays of same size, where $0 \le i_j \le n_j - 1$ and $0 \le j \le m-1$. The dot product of the arrays $\boldsymbol{A}$ and $\boldsymbol{B}$ is*

$$\boldsymbol{A} \cdot \boldsymbol{B} = \sum_{i_0=0}^{n_0-1} \sum_{i_1=0}^{n_1-1} \cdots \sum_{i_{m-1}=0}^{n_{m-1}-1} a(i_0, i_1, \ldots i_{m-1}) b^*(i_0, i_1, \ldots, i_{m-1}) , \tag{2.7}$$

*where $b^*(i_0, i_1, \ldots, i_{m-1})$ denotes the complex conjugate of $b(i_0, i_1, \ldots, i_{m-1})$.*

**Definition 2.15.** *Periodic cross-correlation and autocorrelation of arrays.*

*For an m-tuple* $(\tau_0, \tau_1, \ldots, \tau_{m-1})$ *of integers, the* ***periodic cross-correlation*** *of two same-size arrays* $\boldsymbol{A} = \{a(i_0, i_1, \ldots, i_{m-1})\}$ *and* $\boldsymbol{B} = \{b(i_0, i_1, \ldots, i_{m-1})\}$*, for the shift* $(\tau_0, \tau_1, \ldots, \tau_{m-1})$ *is*

$$CC_{\boldsymbol{A},\boldsymbol{B}}(\tau_0, \tau_1, \ldots, \tau_{m-1}) =$$
$$\sum_{i_0=0}^{n_0-1} \sum_{i_1=0}^{n_1-1} \cdots \sum_{i_{m-1}=0}^{n_{m-1}-1} a(i_0, i_1, \ldots i_{m-1}) b^*(i_0 + \tau_0, i_1 + \tau_1, \ldots, i_{m-1} + \tau_{m-1}) \ , \tag{2.8}$$

*where* $i_j + \tau_j$ *is calculated modulo* $n_j$*. When* $\boldsymbol{A} = \boldsymbol{B}$*, we denote* $CC_{\boldsymbol{A},\boldsymbol{A}}(\tau_0, \tau_1, \ldots, \tau_{m-1})$ *by* $AC_{\boldsymbol{A}}(\tau_0, \tau_1, \ldots, \tau_{m-1})$*, which is called the* ***periodic autocorrelation*** *value of the array* $\boldsymbol{A}$*, for the shift* $(\tau_0, \tau_1, \ldots, \tau_{m-1})$*. In terms of the dot product, the* $(\tau_0, \tau_1, \ldots, \tau_{m-1})$ *autocorrelation value is*

$$AC_{\boldsymbol{A}}(\tau_0, \tau_1, \ldots, \tau_{m-1}) =$$
$$\boldsymbol{A} \cdot \boldsymbol{A}^{(\tau_0, \tau_1, \ldots, \tau_{m-1})} = \tag{2.9}$$
$$\sum_{i_0=0}^{n_0-1} \sum_{i_1=0}^{n_1-1} \cdots \sum_{i_{m-1}=0}^{n_{m-1}-1} a(i_0, i_1, \ldots i_{m-1}) b^*(i_0 + \tau_0, i_1 + \tau_1, \ldots, i_{m-1} + \tau_{m-1}).$$

**Definition 2.16.** *Peak and off-peak values of an array.*

*Let* $\boldsymbol{A} = \{a(i_0, i_1, \ldots, i_{m-1})\}$ *be an array over an alphabet* $\mathcal{A}$*, where* $0 \leq i_j \leq n_j - 1$ *and* $0 \leq j \leq m - 1$*. The autocorrelation value of A, for the shift* $(0, \ldots, 0)$*, is called the* ***peak value****. The autocorrelation values of S, for all shifts* $(\tau_1, \ldots, \tau_{m-1}) \neq (0, \ldots, 0)$ *are called* ***off-peak values****.*

**Definition 2.17.** *Perfect array.*

*An array* $\boldsymbol{A} = \{a(i_0, i_1, \ldots, i_{m-1})\}$ *over an alphabet* $\mathcal{A}$ *is called* ***perfect*** *if all the off-peak values are zero, that is, for all shifts* $(\tau_0, \tau_1, \ldots, \tau_{m-1}) \neq (0, 0, \ldots, 0)$*, we have*

$AC_{\boldsymbol{A}}(\tau_0, \tau_1, \ldots, \tau_{m-1}) = 0$.

**Example 2.2.** *Let i be a fourth root of unity. Consider the array*

$$\boldsymbol{A} = \begin{pmatrix} 1 & i & 1 & i \\ i & 1 & -i & -1 \\ 1 & -i & 1 & -i \\ i & -1 & -i & 1 \end{pmatrix} \tag{2.10}$$

*Then* $AC_{\boldsymbol{A}}(\tau_0, \tau_1) = 0$, *for* $(\tau_0, \tau_1) \neq (0, 0)$ *mod*$(4, 4)$, *that is,* $\boldsymbol{A}$ *is a perfect array.*

**Definition 2.18.** *Decimation of an Array.*

*Let* $\boldsymbol{A} = \{a(i_0, i_1, \ldots, i_{m-1})\}$ *be an m-dimensional array, where* $0 \leq i_j \leq n_j - 1$ *and* $0 \leq j \leq m-1$, *over an alphabet* $\mathcal{A}$. *For* $k_j > 0$, *with* $0 \leq j \leq m-1$, *consider the array defined by* $\boldsymbol{B} = \{a(i_0k_0, i_1k_1, \ldots, i_{m-1}k_{m-1})\}$, *where* $0 \leq i_j \leq n_j - 1$ *and* $0 \leq j \leq m-1$ *and* $i_jk_j$ *is calculated mod* $n_j$. *The array* $\boldsymbol{B}$ *is said to be the* ***decimation*** *by* $(k_0, \ldots, k_{m-1})$ *of the array* $\boldsymbol{A}$. *If* $gcd(n_j, k_j) = 1$, *for* $0 \leq j \leq m-1$, *then the decimation is said to be* ***proper***.

## 2.3 Algebra

The following definitions are taken from Lang [48].

**Definition 2.19.** *Rule of composition.*

*Let G be a set. A mapping* $G \times G \to G$ *is called a* ***rule of composition*** *(of G into itself). If x and y are elements of G, the image of the pair* $(x, y)$ *under this mapping is also called their* ***product*** *under the rule of composition, and will be denoted by xy (in many cases it will be convenient to use an additive notation* $x + y$, *and in that case we call this element the sum of x and y).*

**Definition 2.20.** *Group.*

*Let G be a set with a rule of composition. If $x, y$ and z are elements of S, then we may form their product in two ways $(xy)z$ and $x(yz)$. If $(xy)z = x(yz)$, for all $x, y$ and z in G, then we say that the rule of composition is* ***associative****. An element e of G such that $ex = x = xe$, for all e in G is called a* ***unit element*** *(when the rule of composition is written additively, the unit element is denoted by* 0*, and is called a* ***zero element****). A unit element is unique. A* ***monoid*** *is a set G, with a rule of composition which is associative, and having a unit element (so that in particular, G is not empty). A* ***group*** *G is a monoid, such that for every element $x \in G$, there exists an element $y \in G$ such that $xy = yx = e$. Such an element is called an* ***inverse*** *of x. Such an inverse is unique. A group G is called commutative if $xy = yx$, for all x and $y \in G$, and in this case the rule of composition can be written additively.*

**Definition 2.21.** *Ring.*

*A* ***ring*** *R is a set, together with two rules of composition called multiplication and addition respectively, and written as a product and as a sum respectively, satisfying the following conditions: With respect to addition, R is a commutative group, the multiplication is associative, and has a unit element, and for all $x, y$ and $z \in R$ we have $(x + y)z = xz + yz$ and $z(x + y) = zx + zy$. We denote the unit element for addition by* 0*, and the unit element for multiplication by* 1*. A ring R is called commutative if $xy = yx$, for all x and $y \in R$.*

**Definition 2.22.** *Field.*

*Let R be a ring and let U be the set of elements of R which have both left and right inverses with respect to the multiplication. Then U is a multiplicative group and it is called the group of units of R or group of invertible elements of R. A ring such that $0 \neq 1$ and such that every non-zero element is invertible is called a* ***division ring****. A commutative division ring is called a* ***field****.*

**Definition 2.23.** *Galois field.*

*A field having a finite number of elements is called a* ***finite field*** *or a* ***Galois field****. Finite* *fields are classified by size: there is exactly one finite field up to isomorphism of size $p^n$ for a prime $p$ and positive integer $n$, and there are no fields of sizes other than $p^n$. Finite fields are denoted by $GF(p^n)$ and are isomorphic to the quotient ring $\frac{\mathbb{Z}}{<p^n>}$, where $p$ is a prime number and $n$ a positive integer.*

**Definition 2.24.** *Extension field.*
*The Galois field $GF(p^n)$ is known as a finite extension field of $GF(p)$.*

**Definition 2.25.** *Polynomial over a field.*
*Let $F$ be a field. A **polynomial** over $F$ is an expression of the form $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, where $n$ is a positive integer and the coefficients $a_i$, for $0 \leq i \leq n$, are elements of $F$. The symbol $x$, not belonging to $F$, is called an indeterminate over $F$. A polynomial $f(x)$ over a field $F$ having $1$ as the coefficient of the highest power of $x$ appearing is called a **monic** polynomial.*

**Definition 2.26.** *Algebraic element.*
*An element $\alpha$ of an extension field $E$ of a field $F$ is **algebraic** over $F$ if $f(\alpha) = 0$, for some non-zero polynomial $f(x)$ over $F$.*

**Definition 2.27.** *Irreducible polynomial.*
*Let $F$ denote a field. A polynomial $f(x)$ over $F$ is called **irreducible** over $F$ if $f$ has positive degree and $f = gh$, with $g, h$ polynomial over $F$, implies that either $g$ or $h$ is a constant polynomial. Otherwise $f$ is called **reducible** over $F$.*

**Definition 2.28.** *Minimal polynomial.*
*Let $E$ be an extension field of $F$ and $\alpha \in E$ be algebraic over $F$. Then the uniquely determined monic polynomial $f(x) \in F[x]$ generating the ideal $J = \{g(x) \in F[x] | g(\alpha) = 0\}$ is called the minimal polynomial of $\alpha$ over $F$.*

**Definition 2.29.** *Primitive polynomial.*
*The group $GF(p^n)^*$ is the group of units of $GF(p^n)$. A generator of the cyclic group $GF(p^n)^*$ is called a **primitive element** of $GF(p^n)$. An irreducible polynomial over*

*$GF(p)$ having a primitive element in $GF(p^n)$ as a root is called a primitive polynomial over $GF(p)$. The number of primitive polynomials of degree $n$ over $GF(p)$ is $\frac{\phi(p^n-1)}{n}$, where $\phi$ is the Euler-Totient function.*

**Definition 2.30.** *Module.*

*Let $R$ be a ring. A **left** $R$-**module** $M$ over the ring $R$ consists of an abelian group $(M, +)$ and an operation $R \times M \to M$ such that for all $r, s \in R$ and $x, y \in M$, we have*

1. $r(x+y) = rx + ry$.
2. $(r+s)x = rx + sx$.
3. $(rs)x = r(sx)$.
4. $1_R x = x$, *where $1_R$ is the multiplicative identity in $R$.*

*A **right** $R$-**module** $M$ is defined similarly, only the ring acts on the right. A **bimodule** is a module which is a left module and a right module, such that the two multiplications are compatible. When the ring $R$ is a field, an $R$-modulo is called $R$-**vector space**. This mean that the concept of a module over a ring is a generalisation of the notion of a vector space.*

**Definition 2.31.** *Algebra.*

*Let $R$ be a ring. An $R$-module $M$ that is also a ring is called an $R$-**Algebra**, provided all the operations are compatible, i.e., $(rm)n = m(rn)$, for $m, n \in M$ and $r \in R$. An algebra $A$ is called commutative, if as ring $xy = yx$, for all $x, y \in A$.*

## 2.4 Roots of Unity

**Definition 2.32.**

*A complex number $\omega$ is called an $n^{th}$ root of unity if $\omega^n = 1$. An $n^{th}$ root of unity $\omega$ is called primitive if $\omega^n = 1$ and $\omega^s \neq 1$, for all $1 \leq s < n$. The $n^{th}$ root of unity of the form $\omega = e^{\frac{2\pi i}{n}}$ is called the principal $n^{th}$ root of unity. If $w$ is a primitive $n^{th}$ root of* *unity, then the sum of all $n^{th}$ roots of unity is zero, that is,*

$$1 + w + w^2 + \cdots + w^{n-1} = \frac{w^n - 1}{w - 1} = 0. \tag{2.11}$$

CHAPTER

# 3

# PERFECT SEQUENCES AND ARRAYS OVER THE COMPLEX NUMBERS $\mathbb{C}$

We recall that a sequence $\boldsymbol{S} = (s_0, s_1, \ldots, s_{n-1})$ is said to be perfect, if all the off-peak autocorrelation values of the sequence are equal to zero, that is, for all shifts $\tau \neq 0$, we have $AC_{\boldsymbol{s}}(\tau) = 0$. Sequences over the $n$-th roots of unity are called **polyphase, unimodular** or **phase-shift keying** sequences.

## 3.1 Properties of perfect sequences over the complex numbers $\mathbb{C}$

### 3.1.1 Transformations preserving perfection

The next theorem explains some transformations of perfect sequences over roots of unity that preserve perfection. The first 5 properties are due to Fan and Darnell [29]. The fifth property is due to Gabidulin and Shorin [33].

**Theorem 3.1.** *If $\boldsymbol{S} = (s_t)$, where $0 \leq t \leq n-1$, is a perfect polyphase sequence, then so are the sequences obtained as follows.*

1. *Shift $m$ places to the left: $(s_{t+m})$, where $0 \leq t \leq n-1$ and $m$ is any integer and the subscript $t+m$ is calculated modulo $n$.*
2. *Multiplication by a constant: $(cs_t)$, where $0 \leq t \leq n-1$ and $c$ is any complex constant.*
3. *Conjugation: $(s_t^*)$, where $0 \leq t \leq n-1$ and $s_t^*$ denotes the complex conjugate.*
4. *Multiplying entries by consecutive roots of unity: $(s_t w^{t \ (mod\ n)})$, where $0 \leq t \leq n-1$, and $w$ is a primitive $n$-th root of unity.*
5. *Proper decimation: A proper decimation of a perfect sequence is perfect.*

Properties 1 - 4 are valid for perfect sequences over arbitrary complex numbers. Proofs for properties 1 - 3 are not complicated and follow from the definition of perfection, and are therefore omitted here. Property 4 is valid for any sequence $\boldsymbol{S}$ of length $kn$.

*Proof.* 4. Let $\boldsymbol{S} = (s_t)$ be a perfect sequence over the complex numbers, where $0 \leq t \leq nk$. Let $w$ be a primitive $n$-th root of unity. We show the sequence $\boldsymbol{U} = (u_t)$, where $u_t = s_t w^{t \ (mod\ n)}$, is also perfect. Consider the autocorrelation of the sequence $\boldsymbol{U}$, for any nonzero shift $\tau$

$$\begin{aligned}
AC_{\boldsymbol{U}}(\tau) &= \sum_{t=0}^{nk-1} u_t u_{t+\tau}^{*} \\
&= \sum_{t=0}^{nk-1} s_t \left(w^{t\ (mod\ n)}\right) s_{t+\tau}^{*} \left(w^{t+\tau\ (mod\ n)}\right)^{*} \\
&= \sum_{t=0}^{nk-1} s_t s_{t+\tau}^{*} \left(w^{t\ (mod\ n)}\right) \left(w^{t\ (mod\ n)}\right)^{*} \left(w^{\tau\ (mod\ n)}\right)^{*} \\
&= \sum_{t=0}^{nk-1} s_t s_{t+\tau}^{*} 1 \left(w^{\tau\ (mod\ n)}\right)^{*} \\
&= \left(w^{\tau\ (mod\ n)}\right)^{*} \sum_{t=0}^{nk-1} s_t s_{t+\tau}^{*} 1 \\
&= \left(w^{\tau\ (mod\ n)}\right)^{*} AC_{\boldsymbol{S}}(\tau) = 0.
\end{aligned} \tag{3.1}$$

5. Let $\boldsymbol{S} = (s_t)$ be a sequence of length $n$ over the complex numbers. Let $r$ be a positive integer such that $GCD(r, n) = 1$. Let $\boldsymbol{U} = (u_t)$ be the decimation of the sequence $\boldsymbol{S}$ by $r$, that is, $u_t = s_{tr}$, for $0 \leq t \leq n-1$. We will show that for any shift $1 \leq \tau \leq n-1$, the $\tau$-autocorrelation value of $\boldsymbol{U}$ is the off-peak autocorrelation value of the sequence $\boldsymbol{S}^{*}$ for the shift $\sigma$, where $\sigma = (n - \tau)r$. This will show that a proper decimation of a sequence permutes the positions of the off-peak autocorrelation values of the conjugated sequence $\boldsymbol{S}^{*}$. For the sake of simplicity, let us put $\rho = (n - \tau)$. Since $r$ and $n$ are coprime numbers, we have $\{0r, 1r, \ldots, (n-1)r\}$ $(mod\ n)$ is a permutation of the set $\{0, 1, \ldots, n-1\}$.

Then

$$\begin{gathered}
AC_{\boldsymbol{U}}(\tau) = \\
\sum_{t=0}^{n-1} u_t u^*_{t+\tau} = \sum_{t=0}^{n-1} s_{tr} s^*_{(t+\tau)r} = \sum_{t=0}^{n-\tau-1} s_{tr} s^*_{(t+\tau)r} + \sum_{t=n-\tau}^{n-1} s_{tr} s^*_{(t+\tau)r} = \\
\sum_{t=n-\tau}^{n-1} s_{tr} s^*_{(t+\tau)r} + \sum_{t=0}^{n-\tau-1} s_{tr} s^*_{(t+\tau)r} = \sum_{t=n-\tau}^{n-1} s^*_{(t+\tau)r} s_{tr} + \sum_{t=0}^{n-\tau-1} s^*_{(t+\tau)r} s_{tr} = \\
s^*_{(n-\tau+\tau)r} s_{(n-\tau)r} + s^*_{(n-\tau+1+\tau)r} s_{(n-\tau+1)r} + \cdots + s^*_{(n-1+\tau)r} s_{(n-1)r} + \\
s^*_{\tau r} s_{0r} + s^*_{(\tau+1)r} s_{1r} + \cdots + s^*_{(n-\tau-1+\tau)r} s_{(n-\tau-1r)} = \\
s^*_0 s_\rho + s^*_r s_{\rho+r} + s^*_{2r} s_{\rho+2r} + \cdots + s^*_{(\tau-1)r} s_{\rho+(\tau-1)r} + \\
s^*_{\tau r} s_0 + s^*_{(\tau+1)r} s_r + \cdots + s^*_{(n-1)r} s_{\rho+(n-1)r} = \\
s^*_0 s_\rho + s^*_1 s_{1+\rho} + \cdots + s^*_{n-1} s_{n-1+\rho} = \\
AC_{\boldsymbol{S}^*}(\rho).
\end{gathered} \tag{3.2}$$

Since $\boldsymbol{S}^*$ is perfect by Theorem (3.1) - (3), it follows that $\boldsymbol{U}$ is perfect.

□

**Definition 3.1.** *Discrete Fourier transform.*

*Let $\boldsymbol{S} = (s_0, \ldots, s_{m-1})$ be a sequence over any alphabet of complex numbers. The sequence $DFT(\boldsymbol{S}) = \boldsymbol{U} = (u_0, \ldots, u_{n-1})$, where*

$$u_t = \sum_{r=0}^{n-1} s_t e^{-\frac{2\pi i}{n} tr}, \tag{3.3}$$

*and $e^{\frac{2\pi i}{n}}$ is the principal n-th complex root of unity, is called the **discrete Fourier transform** of the sequence **S**.*

**Theorem 3.2** (Gabidulin [31]). *If the elements in the sequence **S** have equal norm, then the sequence $DFT(\boldsymbol{S}) = (DFT(s_t))$ is perfect, where $0 \leq t \leq n-1$ and $DFT(s_t)$ denotes the discrete Fourier transform of $s_t$.*

*Proof.* (Kuznetsov [46]).
Let $\boldsymbol{S} = (s_t)$ be a sequence over the complex numbers with all elements of equal norm, that is, $\|s_1\| = \cdots = \|s_{n-1}\| = c$. Now, consider the autocorrelation of the sequence $DFT(\boldsymbol{S}) = (DFT(s_t)) = (a_t)$, where $0 \leq t \leq n-1$, for some nonzero shift $\tau$

$$\begin{aligned} AC_{DFT(\boldsymbol{S})}(\tau) = & \sum_{t=0}^{n-1} a_t a^*_{t+\tau} = \sum_{i=0}^{n-1} \left( \sum_{t_1=0}^{n-1} s_{t_1} e^{\frac{-2\pi i}{n} t t_1} \right) \left( \sum_{t_2=0}^{n-1} s_{t_2} e^{\frac{-2\pi i}{n}(t+\tau) t_2} \right)^* \\ = & \sum_{t=0}^{n-1} \sum_{t_1=0}^{n-1} \sum_{t_2=0}^{n-1} s_{t_1} e^{\frac{-2\pi i}{n} t t_1} s^*_{t_2} e^{\frac{2\pi i}{n}(t+\tau) t_2} \\ = & \sum_{t=0}^{n-1} \sum_{t_1=0}^{n-1} \sum_{t_2=0}^{n-1} s_{t_1} s^*_{t_2} e^{\frac{-2\pi i}{n}(t(t_1-t_2)-\tau t_2)} \\ = & \sum_{t_1=0}^{n-1} s_{t_1} \sum_{t_2=0}^{n-1} s^*_{t_2} e^{\frac{2\pi i}{n}\tau t_2} \sum_{t=0}^{n-1} e^{\frac{-2\pi i}{n} t(t_1-t_2)}. \end{aligned} \tag{3.4}$$

The last summation $\sum_{t=0}^{n-1} e^{\frac{-2\pi i}{n} t(t_1-t_2)}$ represents a sum of a complete set of $n$-th roots of unity, which is equal to 0, for all $t_1 - t_2$ except for $t_1 = t_2$, for which the sum is equal to $n$. Therefore, the last term above is

$$= n \sum_{t_1=0}^{n-1} s_{t_1} s^*_{t_1} e^{\frac{2\pi i}{n}\tau t_1} = n \sum_{t_1=0}^{n-1} \|s_{t_1}\| e^{\frac{2\pi i}{n}\tau t_1} = nc \sum_{t_1=0}^{n-1} e^{\frac{2\pi i}{n}\tau t_1} = 0\,, \tag{3.5}$$

since $\sum_{t_1=0}^{n-1} e^{\frac{2\pi i}{n}\tau t_1}$ is a sum of all $n$-roots of unity. Since $AC_{DFT(S)}(\tau) = 0$, for $m = 1, \ldots, n-1$, we have $DFT(S)$ is perfect. □

**Corollary 3.1.** *The discrete Fourier transform of a perfect sequence is perfect.*

### 3.1.2 Balance Theorem

The Balance Theorem gives a necessary condition for perfection of sequences over the complex numbers, ℂ, by equating the balance of a perfect sequence to the norm of the sum of all elements in the sequence. Bomer and Antweiler introduced the Balance Theorem for two-dimensional perfect arrays [17]. Since perfect sequences are also two-dimensional arrays of size 1 × $n$, this result holds for perfect sequences.

**Theorem 3.3** (Balance Theorem)**.** *Let* $\mathbf{S} = (s_0, \ldots, s_{n-1})$ *be a sequence with entries from the complex numbers* ℂ*. If the sequence* $\mathbf{S}$ *is perfect, then*

$$\|s_0 + \cdots + s_{n-1}\| = \|s_0\| + \cdots + \|s_{n-1}\|. \tag{3.6}$$

*Proof.* Since $\mathbf{S}$ is perfect, we have

$$\sum_{t=0}^{n-1} s_t s_{t+\tau}^* = 0\,, \tag{3.7}$$

for $1 \leq \tau \leq n-1$. Summing up Equations (3.7) for $1 \leq \tau \leq n-1$ and adding the equation

$$\sum_{t=0}^{n-1} s_t s_t^* = \sum_{t=0}^{n-1} \|s_t\|\,, \tag{3.8}$$

we have

$$\begin{aligned}\sum_{\tau=0}^{n-1}\sum_{t=0}^{n-1} s_t s_{t+\tau}^* &= \sum_{t=0}^{n-1}\left(s_t \sum_{\tau=0}^{n-1} s_{t+\tau}^*\right) = \sum_{t=0}^{n-1}\left(s_t \sum_{t_1=0}^{n-1} s_{t_1}^*\right) \\ &= \left(\sum_{t=0}^{n-1} s_t\right)\left(\sum_{t=0}^{n-1} s_t^*\right) = \left(\sum_{t=0}^{n-1} s_t\right)\left(\sum_{t=0}^{n-1} s_t\right)^* \qquad (3.9) \\ &= \left\|\sum_{t=0}^{n-1} s_t\right\|.\end{aligned}$$

Since the off-peak autocorrelation values of the sequence $\boldsymbol{S}$ are zero, the only summand in the sum above not equal to zero is when $\tau = 0$. Hence

$$\sum_{\tau=0}^{n-1}\sum_{t=0}^{n-1} s_t s_{t+\tau}^* = \sum_{t=0}^{n-1} s_t s_t^* = \sum_{t-0}^{n-1} \|s_t\|. \qquad (3.10)$$

Therefore,

$$\left\|\sum_{t=0}^{n-1} s_t\right\| = \sum_{t-0}^{n-1} \|s_t\|. \qquad (3.11)$$

□

### 3.1.3 Composition of sequences

Let $\boldsymbol{S} = (s_0, \ldots, s_{n-1})$ and $\boldsymbol{U} = (u_0, \ldots, u_{m-1})$ be two sequences over the complex numbers $\mathbb{C}$, such that the lengths $n$ and $m$ are coprime numbers. We define the composition of $\boldsymbol{S}$ and $\boldsymbol{U}$, denoted by $\boldsymbol{V} = \boldsymbol{S} \circ \boldsymbol{U}$, by the rule

$$v_t = \left(s_{t \ (mod\ n)}\right)\left(u_{t \ (mod\ m)}\right)\ , \qquad (3.12)$$

for $t = 0, 1, \ldots, mn-1$.

### 3.1.4 Product Theorem

This theorem, introduced by Luke, states that each autocorrelation value of the composition of two perfect sequences of coprime lengths is the product of the two individual autocorrelation values for that shift [53].

**Theorem 3.4** (Luke [53]). *Let $\boldsymbol{S} = (s_0, \ldots, s_{n-1})$ and $\boldsymbol{U} = (u_0, \ldots, u_{m-1})$ be two sequences over the complex numbers $\mathbb{C}$, of coprime lengths $n$ and $m$. The autocorrelation function of the composition sequence $\boldsymbol{S} \circ \boldsymbol{U}$, for $0 \leq \tau \leq mn-1$ is*

$$AC_{\boldsymbol{S}\circ\boldsymbol{U}}(\tau) = AC_{\boldsymbol{S}}(\tau)AC_{\boldsymbol{U}}(\tau). \tag{3.13}$$

*Proof.* Let $\boldsymbol{S} = (s_t)$ and $\boldsymbol{U} = (u_t)$ be two sequences of coprime lengths $m$ and $n$. Let $\boldsymbol{V}$ be the product of $\boldsymbol{S}$ and $\boldsymbol{U}$. For $0 \leq \tau \leq mn-1$, we have

$$\begin{aligned} AC_{\boldsymbol{V}}(\tau) = \; & \sum_{t=0}^{mn-1} v_t v_{t+\tau}^* = \sum_{t=0}^{mn-1} s_{t\ (mod\ n)} u_{t\ (mod\ m)} s^*_{t+\tau\ (mod\ n)} u^*_{t+\tau\ (mod\ n)} \\ = \; & \sum_{t_1=0}^{n-1} \sum_{t_2=0}^{m-1} s_{t_1\ (mod\ n)} s^*_{t_1+\tau\ (mod\ n)} u_{t_2\ (mod\ m)} u^*_{t_2+\tau\ (mod\ n)} \\ & \left( \sum_{t_1=0}^{n-1} s_{t_1\ (mod\ n)} s^*_{t_1+\tau\ (mod\ n)} \right) \left( \sum_{t_2=0}^{m-1} u_{t_2\ (mod\ m)} u^*_{t_2+\tau\ (mod\ n)} \right) \\ = \; & AC_{\boldsymbol{S}}(\tau) AC_{\boldsymbol{U}}(\tau). \end{aligned} \tag{3.14}$$

□

The following corollary was proved, independently from Theorem (3.4), by Fan and Darnell [29],

**Corollary 3.2.** *The composition of two perfect sequences of coprime lengths is perfect.*

**Example 3.1.** *Let $w$ be a primitive third root of unity. The perfect sequences $(1,1,1,-1)$ and $(1,w,w)$, when multiplied, give the perfect sequence*

$$(1,w,w,-1,w,w,1,-w,w,1,w,-w)\,, \tag{3.15}$$

*over six roots of unity.*

## 3.2 Necessary and sufficient conditions for perfection over the complex numbers $\mathbb{C}$

In 1993, Mow noted in his PhD thesis that a polyphase sequence $S=(s_0,\ldots,s_{n-1})$ is perfect if and only if the norm of each discrete Fourier transform coefficient of the sequence $S$ is equal to one, that is, $\|DFT(S)_t\|=1$, for $0\le t\le n-1$ [62].

In 1995, Fan and Darnell stated the following necessary and sufficient condition for a sequence, over the complex numbers, to be perfect: A sequence $S=(s_0,\ldots,s_{n-1})$ over the complex numbers is perfect if and only if all discrete Fourier transform coefficients of the sequence $S=(s_0,\ldots,s_{n-1})$, have equal norm, that is, $\|DFT(S)_0\|=\cdots=\|DFT(S)_{n-1}\|$ [29].

In 1993 and 1995, Gabidulin used this necessary and sufficient condition in his work to construct perfect sequences over the complex numbers [31], [32].

None of these authors presented a formal proof of the necessity and sufficiency of this condition for perfection. However, Kuznetsov presented a proof in his PhD thesis [46], which we now present.

**Theorem 3.5.** *Let $S=(s_0,\ldots,s_{n-1})$ be a sequence over the complex numbers $\mathbb{C}$. The sequence $S$ is perfect if and only if the discrete Fourier transform coefficients $DFT(S)_t=\sum_{t=0}^{n-1}s_te^{-\frac{2\pi i}{n}rt}$, where $0\le r\le n-1$, are of equal norm.*

*Proof.* (Kuznetsov [46]).

1. First, assume that $\boldsymbol{S}$ is perfect. We prove that all the discrete Fourier transform coefficients of $\boldsymbol{S}$ have equal norm. For $0 \leq t \leq n-1$, we have

$$\begin{aligned}
\|DFT(\boldsymbol{S})_t\| &= DFT(\boldsymbol{S})DFT(\boldsymbol{S})^* \\
&= \left(\sum_{t_1=0}^{n-1} s_{t_1} e^{-\frac{2\pi i}{n}tt_1}\right)\left(\sum_{t_2=0}^{n-1} s_{t_2} e^{-\frac{2\pi i}{n}tt_2}\right)^* \\
&= \left(\sum_{t_1=0}^{n-1} s_{t_1} e^{-\frac{2\pi i}{n}tt_1}\right)\left(\sum_{t_2=0}^{n-1} s_{t_2}^* e^{\frac{2\pi i}{n}tt_2}\right) \\
&= \sum_{t_1=0}^{n-1}\sum_{t_2=0}^{n-1} s_{t_1} s_{t_2}^* e^{-\frac{2\pi i}{n}t(t_1-t_2)} \\
&= \sum_{t_1=0}^{n-1}\sum_{r=0}^{n-1} s_{t_1} s_{t_1-r}^* e^{-\frac{2\pi i}{n}tr} \qquad (3.16) \\
&= \sum_{r=0}^{n-1} e^{-\frac{2\pi i}{n}tr} \sum_{t_1=0}^{n-1} s_{t_1} s_{t_1-r}^* \\
&= \sum_{r=0}^{n-1} e^{-\frac{2\pi i}{n}tr} AC_{\boldsymbol{S}}(-r) \\
&= \sum_{r=0}^{n-1} e^{-\frac{2\pi i}{n}tr} (AC_{\boldsymbol{S}}(r))^* \\
&= (AC_{\boldsymbol{S}}(0))^* = \|\boldsymbol{S}\|.
\end{aligned}$$

Thus, all Fourier transform coefficients of a perfect sequence have equal norm.

2. Let $\boldsymbol{U} = (DFT(\boldsymbol{S})_0, \ldots, DFT(\boldsymbol{S})_{n-1})$ be the Discrete Fourier Transform of

$\boldsymbol{S}$. Assume that $\|DFT(\boldsymbol{S})_t\| = c$, for $0 \leq t \leq n-1$. We show that the sequence $\boldsymbol{S}$ is perfect. For some non-zero shift $\tau$, with $1 \leq \tau \leq n-1$

$$\begin{aligned}
AC_{\boldsymbol{S}}(\tau) = & \sum_{t=0}^{n-1} s_t s_{t+\tau}^* = \sum_{t=0}^{n-1} DFT^{-1}(\boldsymbol{U})_t \left(DFT^{-1}(\boldsymbol{U})_{t+\tau}\right)^* \\
= & \sum_{t=0}^{n-1} \left(\sum_{t_1=0}^{n-1} u_{t_1} e^{\frac{2\pi i}{n} t t_1}\right) \left(\sum_{t_2}^{n-1} u_{t_2} e^{\frac{2\pi i}{n}(t+\tau)t_2}\right)^* \\
= & \sum_{t=0}^{n-1} \sum_{t_1=0}^{n-1} \sum_{t_2=0}^{n-1} u_{t_1} e^{\frac{2\pi i}{n} t t_1} u_{t_2}^* e^{-\frac{2\pi i}{n}(t+\tau)t_2} \qquad (3.17) \\
= & \sum_{t=0}^{n-1} \sum_{t_1=0}^{n-1} \sum_{t_2=0}^{n-1} u_{t_1} u_{t_2}^* e^{\frac{2\pi i}{n}(t(t_1-t_2)-\tau t_2)} \\
= & \sum_{t_1=0}^{n-1} u_{t_1} \sum_{t_2=0}^{n-1} u_{t_2}^* e^{-\frac{2\pi i}{n}\tau t_2} \sum_{t=0}^{n-1} e^{\frac{2\pi i}{n} t(t_1-t_2)}.
\end{aligned}$$

The last summation, $\sum_{t=0}^{n-1} e^{\frac{2\pi i}{n} t(t_1-t_2)}$, is the sum of the $n$-th roots of unity, which is equal to 0, for all $t_1 - t_2$, except for $t_1 = t_2$, for which it is equal to $n$. Therefore, the equality above continues to

$$\sum_{t_1=0}^{n-1} u_{t_1} u_{t_1}^* e^{-\frac{2\pi i}{n}\tau t_1} = \sum_{t_1=0}^{n-1} \|u_{t_1}\| e^{-\frac{2\pi i}{n}\tau t_1} = c \sum_{t_1=0}^{n-1} e^{-\frac{2\pi i}{n}\tau t_1} = 0. \qquad (3.18)$$

So, $AC_{\boldsymbol{S}}(\tau) = 0$, for $1 \leq \tau \leq n-1$, that is, the sequence $\boldsymbol{S}$ is perfect.

As required. □

## 3.3 Known perfect sequences over the complex numbers $\mathbb{C}$

### 3.3.1 Binary perfect sequences

**Definition 3.2.** *Binary sequence.*
*A sequence* $\boldsymbol{S}$ *over the binary set* $\{-1, 1\}$ *is called a* ***binary sequence****.*

Up to equivalence, the only known perfect binary sequence has length 4, namely $\{1, 1, 1, -1\}$. Equivalent sequences are the 3 shifts, the negation $(-1, -1, -1, 1)$ and its shifts. By computer search, it has been shown that there are no perfect sequences of length greater than 4, and less than 12,100. It is conjectured that there are no binary perfect sequences of length $n > 4$.

### 3.3.2 Ternary perfect sequences

**Definition 3.3.** *Ternary sequence.*
*A sequence* $\boldsymbol{S}$ *over the ternary set* $\{-1, 0, 1\}$ *is called a* ***ternary sequence****.*

**Example 3.2.** *The sequences* $(0, 1, 1, 0, 1, -1)$ *and* $(0, 1, 1, 1, 1, -1, 0, 1, 0, 0, -1, 1, -1)$ *are perfect ternary sequences of length 6 and 13, respectively.*

Based on what is now known as the Balance Theorem, Chang presented in 1967, a necessary condition for perfection of a ternary sequence [20]. Let $\boldsymbol{S} = (s_0, \ldots, s_{n-1})$ be a ternary sequence. If the number of 1's, $-1$'s and 0's in the sequence are denoted by $a, b$ and $c$, respectively, then the following equation holds

$$a + b = \sum_{t=0}^{n-1} \|s_t\| = \left\| \sum_{t=0}^{n-1} s_t \right\| = (a - b)^2. \tag{3.19}$$

Chang generated some perfect ternary sequences of lengths $(3^n - 1)/2$, for some $n$'s, by a linear recursion relation over $GF(3)$, after replacing 2 by $-1$ in their entries. Chang constructed examples of perfect ternary sequences of lengths $13, 121$ and 1093. In his paper, Chang credited Tompkins [71] with listing all perfect ternary sequences up to length 18.

**Example 3.3.** *We use the minimal polynomial* $p(x) = x^3 + 2x + 1$ *over* $GF(3)$*, the initial condition* $(1, 1, 1)$ *and our code in Mathematica, shown below, to produce an m-sequence of length 13.*

```
The following linear recurrence produces an m−sequence
In[1]:=Mod[LinearRecurrence[{0, −2, −2}, {1, 1, 1}, 13], 3]
Out[1]={1, 1, 1, 2, 2, 0, 1, 2, 1, 0, 0, 1, 0}
```

*Since* $2 \equiv -1 \ (mod\ 3)$*, we convert the m-sequences in Out[1] to*

$$(1,1,1,-1,-1,0,1,-1,1,0,0,1,0), \tag{3.20}$$

*by changing* 2 *to* $-1$*. The autocorrelation of the altered sequence is*

$$(9,0,0,0,0,0,0,0,0,0,0,0,0). \tag{3.21}$$

Following Chang's necessary condition for perfection of ternary sequences, Moharir introduced more necessary conditions for perfection, called **combinatorial admissible conditions** [61]. Based on these conditions, Moharir suggested an algorithm that minimises the search space for exhaustive searches of perfect ternary sequences of longer lengths.

Shedd and Sarwate [69] presented in 1979, two constructions of perfect ternary sequences based on the Helleseth formula [38] for $m$-sequences over $GF(p)$ of lengths $p^n - 1$. One of the constructions works when $p = 2$, the other construction works when $p$ is an odd prime. Shedd and Sarwate presented examples of perfect ternary sequences of length 26 and 31 [69].

Ipatov [41] introduced in 1979 a family of perfect ternary sequences of lengths $\frac{q^n-1}{q-1}$, for $q \geq 3$ and $n$ an odd number. Ipatov constructed this family from linear shift register sequences over $GF(q^n)$, with $n$ an odd number and $q = p^s$, where $p$ is an odd prime.

Hoholdt and Justesen presented in 1983 a construction of perfect ternary sequences of length $\frac{q^{2m+1}-1}{q-1}$, where $q = 2^s$ and $m \geq 1$ and , using difference sets theory [39].

### 3.3.3 Multilevel perfect sequences over $\mathbb{R}$

Luke [53] showed in 1988 that, since the autocorrelation function of a binary $m$-sequence has value $-1$, for all non-zero shifts, then any binary $m$-sequence can be converted into a perfect two-level sequence, by changing all $-1$'s to a suitable rational number (refer also to Sarwate and Pursley [67]).

Luke also noticed that Legendre sequences can be modified in the same way by substituting all $-1$'s by a suitable rational number [53].

Legendre sequences $\boldsymbol{S} = (s_t)$, are three-level sequences defined for every prime number $p$ by

$$s_t = \begin{cases} 0, & \text{if } s_t \equiv 0 \ (mod\ p). \\ 1, & \text{if } t \text{ is a quadratic residue } mod\ p. \\ -1, & \text{if } t \text{ is not a quadratic residue } mod\ p. \end{cases} \tag{3.22}$$

Their autocorrelation off-peak values are $-1$.

Bomer and Antweiler [17], suggested, in 1991, another construction of three-level perfect sequences over the real numbers. This construction is based on any $m$-sequence $\boldsymbol{S} = (s_t)$ over $GF(q)$, of length $n = q^m - 1$, where $q = p^s$, and $p$ is a prime number. The new sequence $\boldsymbol{U} = (u_t)$ is defined by

$$u_t = \begin{cases} 1, & \text{if } s_t = 0. \\ b_1, & \text{if } s_t = 1. \\ b_2, & \text{otherwise.} \end{cases} \tag{3.23}$$

The sequence $\boldsymbol{U}$ is perfect if $b_1 = -\frac{c_2+(q-3)b_2^2}{2b_2}$ and $b_2$ is a real root of the equation

$$(4(q-2)+(q-3)^2)b_2^4 + 4(q-1)b_2^3 + (4c_1 - 2c_2(q-1))b_2^2 - 4c_2b_2 + c_2^2 = 0 \tag{3.24}$$

where $c_1 = \frac{q^{m-2}-1}{q^{m-2}}$ and $c_2 = \frac{q^{m-1}-1}{q^{m-1}}$.

The following theorem, that is known in the folklore, shows the existence of infinitely many perfect sequences over the rational numbers.

**Theorem 3.6.** *For each natural number $n > 0$, the sequence $\boldsymbol{S} = (1, \ldots, 1, -n/2)$ of length $n + 2$ is perfect.*

*Proof.* For $1 \leq \tau \leq n+1$, we compare the sequence $S$ against $S^\tau$, as follows

$$\begin{array}{c|ccccccc} & 0 & 1 & \ldots & \tau & \ldots & n+2 \\ \hline \boldsymbol{S} & 1 & 1 & \ldots & 1 & \ldots & -n/2 \\ \boldsymbol{S^\tau} & 1 & 1 & \ldots & -n/2 & \ldots & 1 \end{array} \tag{3.25}$$

From this table, the $\tau$ autocorrelation value of $\boldsymbol{S}$ is

$$\begin{aligned} AC_S(\tau) = {} & 1 \times 1 + \cdots + 1 \times 1 + (1)(-n/2) + \cdots + 1 \times 1 + (1)(-n/2) \\ = {} & n \times (1) + 2 \times (-n/2) = 0. \end{aligned} \tag{3.26}$$

That is, $S$ is perfect. □

### 3.3.4 Polyphase perfect sequences

**Frank sequence**

Heimiller [37] presented in 1961 a construction for producing polyphase perfect sequences of length $p^2$, where $p$ is a prime number. Let $w$ be a primitive $p$-th root of unity. We form a matrix consisting of powers of $w$, as follows

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & w & w^2 & \dots & w^{p-1} \\ 1 & w^2 & w^{2\times 2} & \dots & w^{(p-1)\times 2} \\ 1 & w^3 & w^{2\times 3} & \dots & w^{(p-1)\times 3} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & w^{p-1} & w^{2\times(p-1)} & \dots & w^{(p-1)\times(p-1)} \end{pmatrix} \tag{3.27}$$

The perfect sequence is form by concatenating, one by one, the rows of the Array (3.27), that is,

$$(1,1,1,\dots,1,1,w_1,w_1^2,\dots,w_1^{p-1},1,w_2,w_2^2,\dots,w_2^{p-1},1,w_{p-1},w_{p-1}^2,\dots,w_{p-1}^{p-1}). \tag{3.28}$$

The rows of the Array (3.27) are mutually orthogonal, so the order of the rows can be changed in any way, and any cyclic permutation of each row can be substituted for that row sequence, without altering perfection of the resulting sequence.

Frank noticed in 1952 (9 years before Heimiller) that this procedure also works for any natural number $n \geq 2$ (not necessarily a prime number), and so a perfect sequence of length $n^2$, over the $n$-th roots of unity was constructed. Being employed in the aircraft manufacturing industry, Frank could only publish his result in 1962 [30].

**Example 3.4.** *Let $i$ be a fourth root of unity. We form a matrix consisting of powers of $i$, as follows:*

$$\begin{pmatrix} i^{0\times0} & i^{0\times1} & i^{0\times2} & i^{0\times3} \\ i^{1\times0} & i^{1\times1} & i^{1\times2} & i^{1\times3} \\ i^{2\times0} & i^{2\times1} & i^{2\times2} & i^{2\times3} \\ i^{3\times0} & i^{3\times1} & i^{3\times2} & i^{3\times3} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \tag{3.29}$$

*We concatenate, one by one, the rows of the matrix in Equation (3.29) and obtain the following perfect sequence*

$$(1,1,1,1,i,-1,-i,1,-1,1,-1,1,-i,-1,i). \tag{3.30}$$

### Chu sequences

Chu gave in 1972 a construction of polyphase perfect sequences for every length $n \geq 2$ [22]. The lengths of Chu sequences are not restricted to perfect squares, like Frank sequences are. Let $n \geq 2$ be any natural number. Let $m$ be any other natural number co-prime to $n$. The Chu sequence $\boldsymbol{S}$, of length $n$, is given by

$$\begin{aligned} s_t &= e^{\frac{\pi m i}{n} t^2}, && \text{for even length } n. \\ s_t &= e^{\frac{\pi m i}{n} t(t+1)}, && \text{for odd length } n, \end{aligned} \tag{3.31}$$

for $0 \leq t \leq n-1$.

**Example 3.5.** *We use the following code in Mathematica to generate Chu sequences of any lengths.*

```
In[1]:= Chu[n_, m_] := Table[Re[#] + I Im[#] & /@
Simplify[ If[EvenQ[j] == True , E^{Pi*m*I*j^2/n},
```

*E^{Pi*m*I*j (j + 1)/n}]], {j, 0, n − 1}]*

*Now, for $n = 8$ and $m = 5$, we have the perfect sequence*

$$(1, -\frac{1+i}{\sqrt{2}}, i, -i, 1, -\frac{1-i}{\sqrt{2}}, i, -1)\,, \tag{3.32}$$

*and equivalently*

$$(w^0, w^1, w^2, w^6, w^0, w^1, w^2, w^4)\,, \tag{3.33}$$

*where $w = -\frac{1-i}{\sqrt{2}}$ is a primitive eighth root of unity.*

A linear phase shift of the form $e^{\frac{2\pi mqi}{n}t}$, where $q$ is any integer, when introduced into the sequence in Equation (3.31), will not affect perfection, by Theorem (3.1). So, a more general expression for a Chu sequence is

$$s_t = \begin{cases} e^{\frac{\pi mi}{n}(t^2+qt)}, & \text{if n is even.} \\ e^{\frac{\pi mi}{n}(t(t+1)+qt)}, & \text{if n is odd,} \end{cases} \tag{3.34}$$

for $0 \leq t \leq n-1$.

### Alltop sequences

Alltop presented in 1980 a family of quadratic phase sequences of odd length [1]. The construction is as follows, for $n$ an odd integer greater than 2 and any integer $m$ coprime to $n$. A quadratic phase sequence $\boldsymbol{U} = (u_0, \ldots, u_{n-1})$ is defined by

$$u_t = e^{\frac{2\pi mi}{n}t^2}, \tag{3.35}$$

for $0 \leq t \leq n-1$. Alltop sequences correspond to Chu sequences of odd length. If we take $M = 2m$, $q = -1$ and $N = n$ in the Equation (3.34), for $0 \leq t \leq N-1$, we have $s_t = e^{\frac{\pi Mi}{N}(t(t+1)+qt)} = e^{\frac{2\pi mi}{n^2}t^2} = u_t$.

### P3 and P4 codes

Lewis and Kretschmer [51] introduced in 1982, two other sequences. For any integer $n$, the sequences P3 and P4 are defined as follows

$$\begin{aligned} P3: \quad & s_t = e^{\frac{\pi i}{n}t^2}. \\ P4: \quad & s_t = e^{\frac{\pi i}{n}t^2 + \pi i t}, \end{aligned} \tag{3.36}$$

for $0 \leq t \leq n-1$. These two sequences are equivalent to Chu sequences (Fan and Darnell [29]).

### Golomb sequences

Zhang and Golomb introduced in 1993 another class of perfect polyphase sequences [75]. For any integer $n \geq 2$ and any integer $m$ co-prime with $n$, we define a Golomb Sequence $S = (s_0, \ldots, s_{n-1})$ as follows

$$s_t = e^{\frac{\pi m i}{n}t(t-1)}, \tag{3.37}$$

for $0 \leq t \leq n-1$.

### Milewski sequences

Milewski [60], in 1983, gave a construction of perfect sequences of length $n = m^{2l+1}$ over $m^{l+1}$-roots of unity, for any positive integer $m$ and $l \geq 1$. This construction concatenates a few copies of a Chu sequence, multiplied by roots of unity in a particular order, as follows:

Let $S = (s_0, \ldots, s_{m-1})$ be any Chu sequence of length $m$. Let $w$ be a primitive $m^{l+1}$ root of unity. We form a matrix of size $m^{l+1} \times m^l$, as follows,

$$\begin{pmatrix} s_0 w^{0\times 0} & \dots & s_{m-1} w^{(m-1)\times 0} & \dots & s_0 w^{(m^{l+1}-m)\times 0} & \dots & s_{m-1} w^{(m^{l+1}-1)\times 0} \\ s_0 w^{0\times 1} & \dots & s_{m-1} w^{(m-1)\times 1} & \dots & s_0 w^{(m^{l+1}-m)\times 1} & \dots & s_{m-1} w^{(m^{l+1}-1)\times 1} \\ \vdots & & \vdots & & \vdots & & \vdots \\ s_0 w^{0\times (m^l-1)} & \dots & s_{m-1} w^{(m-1)\times (m^l-1)} & \dots & s_0 w^{(m^{l+1}-m)\times (m^l-1)} & \dots & s_{m-1} w^{(m^{l+1}-1)\times (m^l-1)} \end{pmatrix} \tag{3.38}$$

We obtain a Milewski sequence by concatenating, one by one, the rows of the matrix in Equation (3.38).

### One-dimensional bent function sequences

**Definition 3.4.** *Chung and Kumar [23]*
*A general bent function $f : \mathbb{Z}_q^m \to \mathbb{Z}_q$, for a positive integer $q$, is a function having the property that all the discrete Fourier transform coefficients*

$$\mathcal{F}(\lambda) = \frac{1}{\sqrt{q^m}} \sum_{x \in \mathbb{Z}_q^m} w^{f(x)} w^{f(q-1)} \ , \tag{3.39}$$

*of $(w^{f(0)}, \dots, w^{f(q-1)})$, for $\lambda \in \mathbb{Z}_q^m$ and $w$ a primitive $q$-th root of unity, have magnitude one.*

In the case $m = 1$, $f : \mathbb{Z}_q^m \to \mathbb{Z}_q$ is called one dimensional bent function, see Mow [63]. This function generates the next sequence $(w^{f(0)}, \dots, w^{f(q-1)})$, whose elements all have norm equal to one. And so, this sequence is perfect, by Theorem (3.5). This type of sequence includes Frank and Chu sequences [29].

**Unified approach of Mow**

Mow presented in 1995, a unified construction of perfect polyphase sequences which contains all the classes of perfect polyphase sequences as special cases [64].

**Bomer and Antweiler construction**

Bomer and Antweiler presented a construction of a three-level perfect sequence of length $n = 3^m - 1$, where $m$ is any positive integer, by mapping elements of an $m$-sequence over $GF(3)$ to three complex values [16]. If $\boldsymbol{S} = (s_0, \ldots, s_{n-1})$ is an $m$-sequence over $GF(3)$, then, for $0 \leq t \leq n-1$, a three-level complex sequence $\boldsymbol{U} = (u_0, \ldots, u_{n-1})$ is constructed as follows

$$u_t = \begin{cases} 1, & \text{if } s_t = 0, \\ e^{i\theta_1}, & \text{if } s_t = 1, \\ e^{i\theta_2}, & \text{otherwise,} \end{cases} \tag{3.40}$$

where $\theta_1 = \theta_2 \pm cos^{-1}(\phi)$, $\theta_2 = \pm cos^{-1}\left(\phi\sqrt{\frac{2}{1+\phi}}\right) \pm \frac{1}{2}cos^{-1}(\phi)$ and $\phi = \frac{1-3^{m-1}}{2\cdot 3^{m-1}}$.

### 3.3.5 Multilevel perfect sequences over $\mathbb{C}$

Multilevel perfect sequences over the complex numbers have not been extensively studied in the literature.

**Darnell and Fan Sequences**

Darnell and Fan in 1995 presented a construction of multilevel perfect sequences over the complex numbers of length $n$, where n is a positive integer, $n = p^m - 1$, for some prime $p$ and some integer $m$ and $n = 4t$, for some odd $t$ [25].

**Example 3.6.** *Multilevel perfect sequence over complex numbers of length 31*

$$(-i,-i,1,-1,1,-i,-1,1,0,0,1,-i,0,-1,0,-1,1,i,1,1,1,0,i,i,-i,-i,-1,-i,1,0,-1). \tag{3.41}$$

**Lee Sequences**

Lee presented in 1999, a construction of perfect sequences over the alphabets $\{0, w_m^1, w_m^2, \ldots, 1\}$, where $w_m$ is a primitive $m$-th root of unity [50]. For the case $w = i$, where $i$ is the fourth root of unity, the alphabet is $\{0, 1, -1, i, -i\}$, and over this alphabet, Lee constructed a family of perfect sequences of unbounded lengths with only one zero occurrence, for all lengths $m = p + 1 \equiv 2 \ (mod\ 4)$, with $p$ a prime number, that is, for $m = 6, 14, 18, 30...$ [49].

**Example 3.7.** *Lee sequence of length 14*

$$(0, i, 1, -i, -1, -i, 1, -i, 1, -i, -1, -i, 1, i). \tag{3.42}$$

Luke presented in 2003, a generalisation of Lee's construction, for all lengths $m = p^k + 1 \equiv 2 \ (mod\ 4)$, where $k \in \mathbb{N}$ and $p$ is a prime number, that is for $m = 6, 10, 14, 18, 26, 30...$ [54]. The sequences constructed by Lee and generalised by Luke are called **Lee Sequences** and they have the following properties: They have one single zero occurrence, are palindromic about two centres, alternate from $\pm i$ to $\pm 1$, ignoring the zero, and have even length.

Lee presented in his Ph.D. Thesis [50], a construction of perfect sequences over the alphabet $PSK+$, that is, the set of $n$-roots of unity extended by adding 0. This construction uses $m$-sequences over $GF(q)$ of length $q^m - 1$, for $m \equiv -2 \ (mod\ q)$, and generates a perfect sequence over $PSK+$ of length $\frac{q^m-1}{q-1}$ (See Boztas and Parampalli [19]).

**Example 3.8.** *(Boztas and Parampalli [19])*
*The following perfect sequence over* $\{0, 1, -1, i, -i\}$ *was obtained from a maximal length sequence of period* $(5^3 - 1) = 124$

$$(-i, -i, 1, -1, 1, -i, -1, 1, 0, 0, 1, -i, 0, -1, 0, -1, 1, i, 1, 1, 1, 0, i, i, -i, -i, -1, -i, 1, 0, -1). \tag{3.43}$$

## 3.4 Non-existence of perfect sequences over the complex numbers ℂ, beyond certain lengths

Perfect sequences, over different alphabets of complex numbers, exist for unbounded lengths, for example, Lee sequences, sequences in Theorem (3.6) and some constructions of ternary sequences, based on *m*- or Legendre sequences. In this section we will discuss the non-existence, **beyond certain lengths**, of perfect sequences over some particular alphabets of complex numbers.

### 3.4.1 Non-existence of binary perfect sequences

**Difference set theory** is a combinatorial design tool that has been used to prove the non-existence of binary and polyphase perfect sequences.

**Definition 3.5.** *Jungnickel and Pott [43]*
*Let G be an additive group of order n, and D be an m-element subset of G. Then D is called a* $(n, m, \lambda)$-***difference set*** *if the set of all D differences, that is* $\delta D = \{d_1 - d_2 \,|d_1, d_2 \in D, d_1 \neq d_2\}$*, contains each non-zero element of G precisely* $\lambda$ *times. If G is a cyclic group, D is also called cyclic.*

In 1971, Baumert stated that there exists a one-to-one correspondence between binary sequences of length $n$ with two-level autocorrelation function, that is, constant off-peak autocorrelation value sequences, and cyclic difference sets in $\mathbb{Z}_n$ [12].

If $D$ is a $(n, m, \lambda)$-difference set in $\mathbb{Z}_n$, we construct a binary sequence $S = (s_0, \ldots, s_{n-1})$ by

$$s_t = \begin{cases} 1, & \text{if } t \in D, \\ -1, & \text{if } t \notin D. \end{cases} \tag{3.44}$$

The autocorrelation of $S$ is given by

$$AC_S = \begin{cases} n, & \text{if } m \equiv 0 \; (mod\; n). \\ n - 4(m - \lambda), & \text{if } m \not\equiv 0 \; (mod\; n), \end{cases} \tag{3.45}$$

for $0 \leq t \leq n - 1$.

Regarding perfect binary sequences, for a difference set $D$ to exist in $\mathbb{Z}_n$, the length $n$ has to be an even square, that is, $n = 4u^2$, for some $u$ and the parameters are in the form $(n, m, \lambda) = (4u^2, 2u^2 - u, u^2 - u)$. Difference sets of this type are called **Hadamard difference sets** [40]. The only Hadamard difference set known is the trivial $(4, 1, 0)$-difference set, corresponding to the sequence $(1, 1, 1, -1)$ [ref]. It has been conjectured that no other Hadamard difference sets exist. This conjecture is known as the **circular Hadamard matrix conjecture**.

### 3.4.2 Non-existence of quaternary perfect sequences

Sequences over the four roots of unity are commonly known as **quaternary sequences**. Here, we have some results on non-existence of quaternary perfect sequences.

In 1989, Chung and Kumar proved that there are no perfect quaternary sequences of length $2^n$, for $n > 4$ [23].

Arasu, de Launey and Ma stated in 2002 a relation between relative difference sets in the group $C_4 \times C_n$, where $C_4$ and $C_n$ are cyclic groups of order 4 and $n$, respectively, and quaternary perfect sequences [5]. They have proved that there are no perfect sequences for many orders. In fact, there are only 11 orders to be checked, up to 1000, namely 260, 340, 442, 520, 580, 680, 754, 820, 884, 890.

### 3.4.3 Non-existence of polyphase perfect sequences

Ma and Ng showed in 2009, that the existence of perfect sequences over the $p$-roots of unity, for $p$ an odd prime, is equivalent to the existence of a type of difference set [58]. Ma and Ng proved the non-existence of perfect sequences of many lengths, including

1. $p^m$, for $m \geq 3$.
2. $2p^m$, for $m \geq 1$.
3. $pq$, for $q$ a prime number and $q > p$.

### 3.4.4 Non-existence of almost polyphase perfect sequences

Chee et al [21] introduced in 2010, almost $p$-ary sequences of length $n + 1$. These are sequences of the form $(0, s_1, \ldots, s_n)$, where $s_1, \ldots, s_n$ are $p$-th roots of unity, for some $p$. Chee et al stated some results on non-existence of perfect almost $p$-ary sequences for certain combinations of $n$ and $p$.

In 2003 Luke proved that perfect almost binary sequences of length $n + 1$ do not exist for $n > 1$ [55].

### 3.4.5 Mow's conjecture on the non-existence of longer polyphase perfect sequences

Mow observed that all known constructions of perfect sequences over $n$-th roots of unity (polyphase perfect sequences), only produce sequences of length less than or equal to $n^2$. Based on this observation, he proposed the following conjecture [64].

**Conjecture 3.1** (Mow). *Let $L = mn^2$, for $m$ and $n$ positive integers, with $m$ square free. A perfect polyphase sequence of length $L$ exists if and only if its alphabet size $N$ is an integer multiple of $N_{min}$, where $N_{min}$ is the minimum alphabet size, given by*

$$N_{min} = \begin{cases} 2mn, & \textit{for even } m \textit{ and odd } n, \\ mn, & \textit{otherwise.} \end{cases} \tag{3.46}$$

This conjecture, if true, would imply that over the alphabet of $n$-roots of unity, there are no perfect sequences of length above $n^2$.

## 3.5 Properties of perfect arrays over the complex numbers $\mathbb{C}$

We recall that an array $\boldsymbol{A} = \{a(i_0, i_1, \ldots, i_{m-1})\}$, where $0 \le i_j \le n_j - 1$ and $0 \le j \le m - 1$, is said to be perfect, if all the off-peak autocorrelation values of the array are equal to zero, that is, for all shifts $(\tau_0, \tau_1, \ldots, \tau_{m-1}) \neq (0, 0, \ldots, 0)$, we have $AC_{\boldsymbol{A}}(\tau_0, \tau_1, \ldots, \tau_{m-1}) = 0$.

### 3.5.1 Transformations preserving perfection

Arrays over the roots of unity are known as polyphase arrays. The next theorem explains some transformations on perfect **polyphase arrays** that preserve perfection.

**Theorem 3.7.** *If $\boldsymbol{A} = \{a(i_0, i_1, \ldots, i_{m-1})\}$, where $0 \leq i_t \leq n_t - 1$ and $0 \leq t \leq m-1$, is a perfect polyphase array, then so are the arrays obtained as follows.*

1. *Shift $(j_0, \ldots, j_{m-1})$ places: $\boldsymbol{A}^{(j_0, j_1, \ldots, j_{m-1})} = \{a(i_0 + j_0, i_1 + j_1, \ldots, i_{m-1} + j_{m-1})\}$, where $0 \leq i_t \leq n_t - 1$ and $0 \leq t \leq m-1$ and the indices $i_t + j_t$, are calculated modulo $n_t$, for $0 \leq t \leq m-1$.*
2. *Multiplication by a constant: $c\boldsymbol{A} = \{ca(i_0, i_1, \ldots, i_{m-1})\}$, where $0 \leq i_t \leq n_t - 1$ and $0 \leq t \leq m-1$ and $c$ is any complex constant.*
3. *Conjugation: $\{a^*(i_0, i_1, \ldots, i_{m-1})\}$, where $0 \leq i_t \leq n_t - 1$ and $0 \leq t \leq m-1$, and $a^*(i_0, i_1, \ldots, i_{m-1})$ denotes the complex conjugate.*
4. *Multiplying entries by consecutive roots of unity: $\{w^{i_t \ (mod \ n_t)} a(i_0, i_1, \ldots, i_t, \ldots, i_{m-1})\}$, where $0 \leq i_t \leq n_t - 1$, and $w$ is a primitive $n$-th root of unity.*
5. *Proper decimation (See Definition 2.18, Chapter 2): A proper decimation of a perfect array is perfect.*

The proof of Theorem (3.7) is similar to the proof of Theorem (3.1), and therefore we omit this proof.

**Example 3.9.**

1. *Let $w$ be a primitive sixth root of unity, say $w = \frac{1}{2} + \frac{i\sqrt{3}}{2}$, and let $z$ be a primitive third root of unity, say $z = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$. We multiply the columns of the perfect array*

$$\begin{pmatrix} 1 & w & 1 & -1 & w^4 & -1 \\ 1 & 1 & w^2 & 1 & 1 & w^2 \end{pmatrix} \tag{3.47}$$

*by $z^0, z^1, z^2, z^0, z^1$ and $z^2$ respectively, and we obtain the perfect array*

$$\begin{pmatrix} 1 & wz^1 & 1z^2 & -1 & w^4z^1 & -1z^2 \\ 1 & 1z^1 & w^2z^2 & 1 & 1z^1 & w^2z^2 \end{pmatrix} \tag{3.48}$$

2. *A three-dimensional array can be viewed as a sequence of two-dimensional arrays. We decimate by $(3,1,3)$ (rows, columns and faces) the following three-dimensional perfect array*

$$\left( \begin{pmatrix} 1 & i & 1 & i \\ -i & -1 & i & 1 \\ 1 & -i & 1 & -i \\ i & -1 & -i & 1 \end{pmatrix}, \begin{pmatrix} i & 1 & -i & -1 \\ 1 & i & 1 & i \\ i & -1 & -i & 1 \\ -1 & i & -1 & i \end{pmatrix}, \begin{pmatrix} -1 & i & -1 & i \\ -i & 1 & i & -1 \\ -1 & -i & -1 & -i \\ i & 1 & -i & -1 \end{pmatrix}, \begin{pmatrix} -i & 1 & i & -1 \\ -1 & i & -1 & i \\ -i & -1 & i & 1 \\ 1 & i & 1 & i \end{pmatrix} \right) \tag{3.49}$$

*and we obtain this perfect array*

$$\left( \begin{pmatrix} 1 & i & 1 & i \\ i & -1 & -i & 1 \\ 1 & -i & 1 & -i \\ -i & -1 & i & 1 \end{pmatrix}, \begin{pmatrix} -i & 1 & i & -1 \\ 1 & i & 1 & i \\ -i & -1 & i & 1 \\ -1 & i & -1 & i \end{pmatrix}, \begin{pmatrix} -1 & i & -1 & i \\ i & 1 & -i & -1 \\ -1 & -i & -1 & -i \\ -i & 1 & i & -1 \end{pmatrix}, \begin{pmatrix} i & 1 & -i & -1 \\ -1 & i & -1 & i \\ i & -1 & -i & 1 \\ 1 & i & 1 & i \end{pmatrix} \right) \tag{3.50}$$

### 3.5.2 Balance Theorem for multi-dimensional perfect arrays

The Balance Theorem gives a necessary condition for perfection of sequences over the complex numbers, ℂ, by equating the balance of a perfect array to the norm of the sum of all elements in the sequence. Bomer and Antweiler introduced the Balance Theorem for two-dimensional perfect arrays [16]. This result can be extended routinely to perfect multi-dimensional arrays:

**Theorem 3.8** (Balance Theorem for multi-dimensional arrays)**.** *Let*

$$A = \{a(i_0, i_1, \ldots, i_{m-1})\} \tag{3.51}$$

*be an array with entries from the complex numbers* $\mathbb{C}$*, where* $0 \leq i_t \leq n_j - 1$ *and* $0 \leq t \leq m-1$*. If the array* $A$ *is perfect, then*

$$\sum_{i_0=0}^{n_0-1} \sum_{i_1=0}^{n_1-1} \cdots \sum_{i_{m-1}=0}^{n_{m-1}-1} \|a(i_0, i_1, \ldots i_{m-1})\| = \left\| \sum_{i_0=0}^{n_0-1} \sum_{i_1=0}^{n_1-1} \cdots \sum_{i_{m-1}=0}^{n_{m-1}-1} a(i_0, i_1, \ldots i_{m-1}) \right\| \tag{3.52}$$

Equation (3.52) is a necessary condition for the existence of perfect multi-dimensional arrays.

**Example 3.10.** *There are not perfect two-dimensional arrays of size* $3 \times 2$ *over the fourth roots of unity* $\{1, -1, i, -i\}$*. Let* $a, b, c$ *and* $d$ *be the number of* $1's$*,* $-1's$*,* $i's$ *and* $-i's$*, occurring in the array, respectively. By Equation (3.52) we have* $6 = (a-b)^2 + (c-d)^2$*, but the number 6 is not the sum of two squares, therefore there are not perfect two-dimensional arrays over* $\{1, -1, i, -i\}$ *of size* $3 \times 2$*.*

### 3.5.3 Composition of arrays

Let $A$ and $B$ be two perfect two-dimensional arrays of sizes $m_1 \times n_1$ and $m_2 \times n_2$, with $GCD(m_1, n_1) = 1$ and $GCD(m_2, n_2) = 1$. By repeating the array $A$ $m_2 \times n_2$ times and the array and $B$ $m_1 \times n_1$ times, and multiplying them together, we obtain the product array

$$A \circ B = \left(a_{i_1 \ (mod\ m_1), i_2\ (mod\ n_1)} b_{i_1\ (mod\ m_2), i_2\ (mod\ n_2)}\right), \tag{3.53}$$

of size $m_1 m_2 \times n_1 n_2$, which is also perfect. This result is a corollary of the following Product Theorem for autocorrelation functions, presented by Luke [53].

### 3.5.4 Product Theorem

**Theorem 3.9** (Luke [53]). *Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be two two-dimensional arrays of sizes $m_1 \times n_1$ and $m_2 \times n_2$, with $GCD(m_1, n_1) = GCD(m_2, n_2) = 1$. The autocorrelation function of the composition $\boldsymbol{A} \circ \boldsymbol{B}$ is the product of the autocorrelation functions of the arrays $\boldsymbol{A}$ and $\boldsymbol{B}$, that is, for $0 \leq \tau_1 \leq m_1m_2$ and $0 \leq \tau_2 \leq n_1n_2$*

$$AC_{\boldsymbol{A}\circ\boldsymbol{B}}(\tau_1, \tau_2) = AC_{\boldsymbol{A}}(\tau_1\ (mod\ m_1), \tau_2\ (mod\ n_1))AC_{\boldsymbol{B}}(\tau_1\ (mod\ m_2), \tau_2\ (mod\ n_2)). \tag{3.54}$$

*Proof.* Let $\boldsymbol{A} = \{a(i_1, i_2)\}$ and $\boldsymbol{B} = \{b(i_1, i_2)\}$ be two arrays of sizes $m_1 \times n_1$ and $m_2 \times n_2$, respectively, and let $\boldsymbol{C}$ the product of the arrays $\boldsymbol{A}$ and $\boldsymbol{B}$. For $0 \leq \tau_1 \leq m_1m_2$ and $0 \leq \tau_2 \leq n_1n_2$, we have

$$\begin{aligned} AC_{\boldsymbol{C}}(\tau_1, \tau_2) &= \sum_{r=0}^{m_1m_2-1} \sum_{s=0}^{n_1n_2-1} c(r,s)c^*(r+\tau_1, s+\tau_2) \\ &= \sum_{r=0}^{m_1m_2-1} \sum_{s=0}^{n_1n_2-1} a(r,s)b(r,s)a^*(r+\tau_1, s+\tau)b^*(r+\tau_1, s+\tau_2) \\ &= \sum_{k=0}^{m_1m_2-1} \left( \sum_{s=0}^{n_1n_2-1} a(r,s)b(r,s)a^*(r+\tau_1, s+\tau)b^*(r+\tau_1, s+\tau_2) \right). \end{aligned} \tag{3.55}$$

Now, for $r$ fixed, we have

$$\begin{gathered} \sum_{s=0}^{n_1n_2-1} a(r,s)b(r,s)a^*(r+\tau_1, s+\tau)b^*(r+\tau_1, s+\tau_2) = \\ \sum_{l_1=0}^{n_1-1} \sum_{l_2=0}^{n_2-1} a(r,l_1)a^*(r+\tau_1, l_1+\tau)b(r,l_2)b^*(r+\tau_1, l_2+\tau_2). \end{gathered} \tag{3.56}$$

From Equation (3.56), we have

$$AC^{(\tau,\sigma)}(C) =$$

$$\sum_{r=0}^{m_1m_2-1}\left(\sum_{l_1=0}^{n_1-1}\sum_{l_2=0}^{n_2-1} a(r,l_1)a^*(r+\tau_1,l_1+\tau)b(r,l_2)b^*(r+\tau_1,l_2+\tau_2)\right) =$$

$$\sum_{l_1=0}^{m_1-1}\sum_{l_2=0}^{m_2-1}\left(\sum_{r=0}^{m_1m_2-1} a(r,l_1)a^*(r+\tau_1,l_1+\tau)b(r,l_2)b^*(r+\tau_1,l_2+\tau_2)\right) =$$

$$\sum_{l_1=0}^{m_1-1}\sum_{l_2=0}^{m_2-1}\sum_{l_3=0}^{n_1-1}\sum_{l_4=0}^{n_2-1} a(l_3,l_1)a^*(l_3+\tau_1,l_1+\tau)b(l_4,l_2)b^*(l_4+\tau_1,l_2+\tau_2) =$$

$$\left(\sum_{l_1=0}^{m_1-1}\sum_{l_3=0}^{n_1-1} a(l_3,l_1)a^*(l_3+\tau_1,l_1+\tau_2)\right)\left(\sum_{l_2=0}^{m_1-1}\sum_{l_4=0}^{n_1-1} b(l_4,l_2)b^*(l_4+\tau_1,l_2+\tau_2)\right) =$$

$$AC_{\boldsymbol{A}}(\tau_1,\tau_2)AC_{\boldsymbol{B}}(\tau_1,\tau_2). \tag{3.57}$$

□

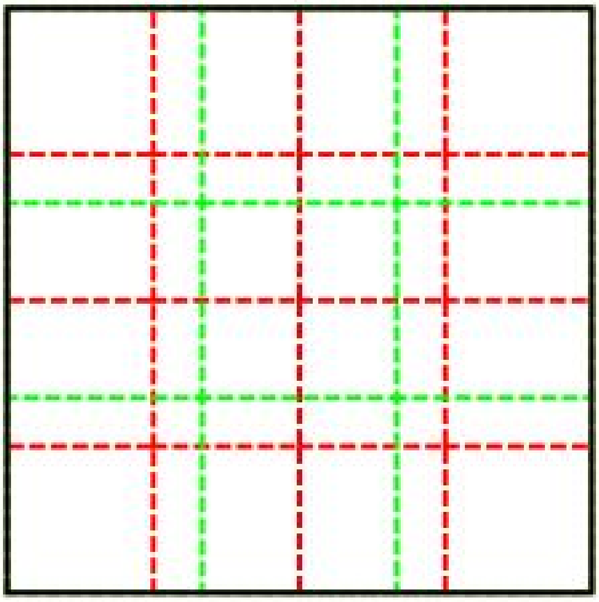
**Corollary 3.3.** *If* $\boldsymbol{A}$ *and* $\boldsymbol{B}$ *are two perfect arrays of sizes* $m_1 \times n_1$ *and* $m_2 \times n_2$*, with* $GCD(m_1, m_1) = GCD(n_2, n_2) = 1$*, then the composition* $\boldsymbol{A} \circ \boldsymbol{B}$ *of* $\boldsymbol{A}$ *and* $\boldsymbol{B}$ *is perfect.*

**Example 3.11.**

1. *Let* $w$ *be a primitive third root of unity. The perfect arrays*

$$A_{3\times 3} = \begin{pmatrix} 1 & w^2 & w^2 \\ w & w & w^2 \\ w & w^2 & 1 \end{pmatrix} \text{ and } B_{4\times 4} = \begin{pmatrix} 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 \end{pmatrix} \tag{3.58}$$

*are repeated* $4 \times 4$ *and* $3 \times 3$ *times, respectively, as shown in the template below. We call to this underlying template by the name* ***Kilt****.*



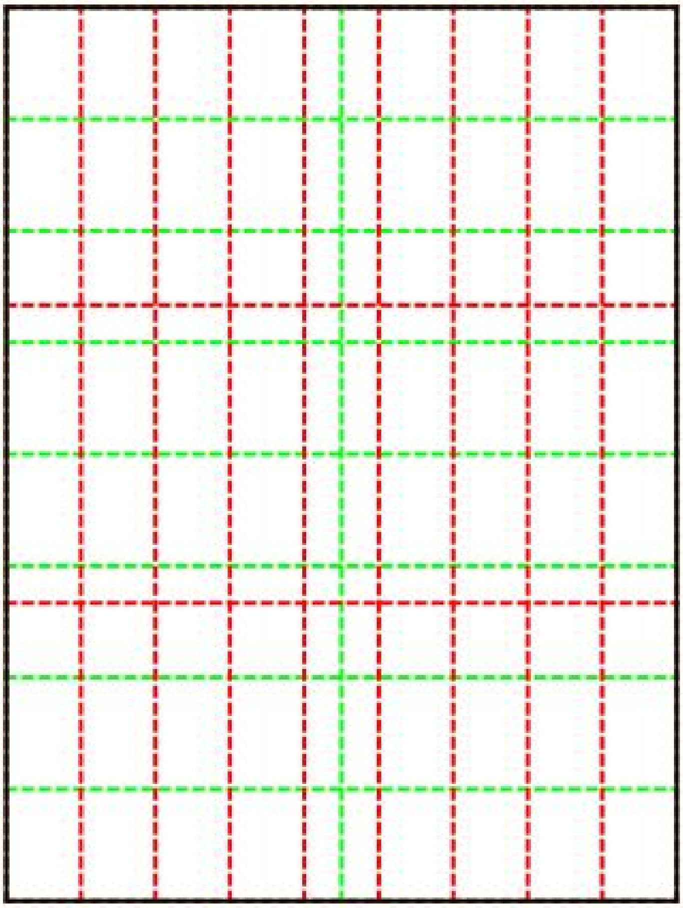
*Corresponding entries are then multiplied together to produce the* $12 \times 12$ *perfect array*

$$\begin{pmatrix} 1 & -w^2 & w^2 & -1 & w^2 & -w^2 & 1 & -w^2 & w^2 & -1 & w^2 & -w^2 \\ w & w & -w^2 & -w & w & w^2 & -w & -w & w^2 & w & -w & -w^2 \\ w & w^2 & w & w & w^2 & w & w & w^2 & w & w & w^2 & w \\ -1 & w^2 & w^2 & -1 & -w^2 & w^2 & 1 & -w^2 & -w^2 & 1 & w^2 & -w^2 \\ w & -w & w^2 & -w & w & -w^2 & w & -w & w^2 & -w & w & -w^2 \\ w & w^2 & -w & -w & w^2 & w & -w & -w^2 & w & w & -w^2 & -w \\ 1 & w^2 & w^2 & 1 & w^2 & w^2 & 1 & w^2 & w^2 & 1 & w^2 & w^2 \\ -w & w & w^2 & -w & -w & w^2 & w & -w & -w^2 & w & w & -w^2 \\ w & -w^2 & w & -w & w^2 & -w & w & -w^2 & w & -w & w^2 & -w \\ 1 & w^2 & -w^2 & -1 & w^2 & w^2 & -1 & -w^2 & w^2 & 1 & -w^2 & -w^2 \\ w & w & w^2 & w & w & w^2 & w & w & w^2 & w & w & w^2 \\ -w & w^2 & w & -w & -w^2 & w & w & -w^2 & -w & w & w^2 & -w \end{pmatrix} \tag{3.59}$$

2. *Let $w$ be a primitive third root of unity. The perfect arrays*

$$A_{3\times 9} = \begin{pmatrix} 1 & w & w & 1 & w^2 & 1 & 1 & 1 & w^2 \\ w & 1 & w & w & w & 1 & w & w^2 & w^2 \\ w & w & 1 & w & w^2 & w^2 & w & w & w \end{pmatrix} \text{ and } B_{8\times 2} = \begin{pmatrix} -1 & -1 \\ -1 & 1 \\ -1 & -1 \\ -1 & 1 \\ -1 & -1 \\ -1 & 1 \\ 1 & 1 \\ 1 & -1 \end{pmatrix}$$

*are repeated $8 \times 2$ times and $3 \times 9$ times, respectively, as shown in the template below*



*Corresponding entries are multiplied together to produce the* $24 \times 18$ *perfect array*

$$\left(\begin{array}{cccccccccccccccccc}
1 & w & w & 1 & w^2 & 1 & 1 & 1 & w^2 & 1 & w & w & 1 & w^2 & 1 & 1 & 1 & w^2 \\
w & 1 & w & w & w & 1 & w & w^2 & w^2 & w & 1 & w & w & w & 1 & w & w^2 & w^2 \\
w & w & 1 & w & w^2 & w^2 & w & 1 & w & w & w & 1 & w & w^2 & w^2 & w & 1 & w \\
1 & w & w & 1 & w^2 & 1 & 1 & 1 & w^2 & 1 & w & w & 1 & w^2 & 1 & 1 & 1 & w^2 \\
w & 1 & w & w & w & 1 & w & w^2 & w^2 & w & 1 & w & w & w & 1 & w & w^2 & w^2 \\
w & w & 1 & w & w^2 & w^2 & w & 1 & w & w & w & 1 & w & w^2 & w^2 & w & 1 & w \\
1 & w & w & 1 & w^2 & 1 & 1 & 1 & w^2 & 1 & w & w & 1 & w^2 & 1 & 1 & 1 & w^2 \\
w & 1 & w & w & w & 1 & w & w^2 & w^2 & w & 1 & w & w & w & 1 & w & w^2 & w^2 \\
w & w & 1 & w & w^2 & w^2 & w & 1 & w & w & w & 1 & w & w^2 & w^2 & w & 1 & w \\
1 & w & w & 1 & w^2 & 1 & 1 & 1 & w^2 & 1 & w & w & 1 & w^2 & 1 & 1 & 1 & w^2 \\
w & 1 & w & w & w & 1 & w & w^2 & w^2 & w & 1 & w & w & w & 1 & w & w^2 & w^2 \\
w & w & 1 & w & w^2 & w^2 & w & 1 & w & w & w & 1 & w & w^2 & w^2 & w & 1 & w \\
1 & w & w & 1 & w^2 & 1 & 1 & 1 & w^2 & 1 & w & w & 1 & w^2 & 1 & 1 & 1 & w^2 \\
w & 1 & w & w & w & 1 & w & w^2 & w^2 & w & 1 & w & w & w & 1 & w & w^2 & w^2 \\
w & w & 1 & w & w^2 & w^2 & w & 1 & w & w & w & 1 & w & w^2 & w^2 & w & 1 & w \\
1 & w & w & 1 & w^2 & 1 & 1 & 1 & w^2 & 1 & w & w & 1 & w^2 & 1 & 1 & 1 & w^2 \\
w & 1 & w & w & w & 1 & w & w^2 & w^2 & w & 1 & w & w & w & 1 & w & w^2 & w^2 \\
w & w & 1 & w & w^2 & w^2 & w & 1 & w & w & w & 1 & w & w^2 & w^2 & w & 1 & w \\
1 & w & w & 1 & w^2 & 1 & 1 & 1 & w^2 & 1 & w & w & 1 & w^2 & 1 & 1 & 1 & w^2 \\
w & 1 & w & w & w & 1 & w & w^2 & w^2 & w & 1 & w & w & w & 1 & w & w^2 & w^2 \\
w & w & 1 & w & w^2 & w^2 & w & 1 & w & w & w & 1 & w & w^2 & w^2 & w & 1 & w \\
1 & w & w & 1 & w^2 & 1 & 1 & 1 & w^2 & 1 & w & w & 1 & w^2 & 1 & 1 & 1 & w^2 \\
w & 1 & w & w & w & 1 & w & w^2 & w^2 & w & 1 & w & w & w & 1 & w & w^2 & w^2 \\
w & w & 1 & w & w^2 & w^2 & w & 1 & w & w & w & 1 & w & w^2 & w^2 & w & 1 & w
\end{array}\right) \tag{3.60}$$

Theorem (3.9) and Corollary (3.3) can be generalised to higher-dimensional arrays.

### 3.5.5 From sequences to two and higher dimensional arrays

Let $\boldsymbol{S}$ and $\boldsymbol{U}$ be two perfect sequences of length $n$. We regard $\boldsymbol{S}$ and $\boldsymbol{U}$ as $n \times 1$ and $1 \times n$ matrices. We can deduce from Theorem (3.9) that the following array $\boldsymbol{A}$ is perfect:

$$\boldsymbol{A} = \begin{pmatrix} s_0u_0 & s_1u_{n-1} & \dots & s_{n-1}u_1 \\ s_0u_1 & s_1u_0 & \dots & s_{n-1}u_2 \\ \vdots & \vdots & & \vdots \\ s_0u_{n-1} & s_1u_{n-2} & \dots & s_{n-1}u_0 \end{pmatrix} \tag{3.61}$$

From the Product Theorem (3.9), the autocorrelation function of the new array $\boldsymbol{A}$ is the product of the autocorrelation functions of the two sequences $\boldsymbol{S}$ and $\boldsymbol{U}$. Now, since the sequences $\boldsymbol{S}$ and $\boldsymbol{U}$ are perfect, all the off-peak autocorrelation values of the array $\boldsymbol{A}$ are zero, and so the array $\boldsymbol{A}$ is perfect.

**Example 3.12.** *Let $w$ be a third primitive root of unity, say $w = -\frac{1}{2} - \frac{i\sqrt{3}}{2}$. We use the perfect sequence $(1, w, w)$ to produce the following perfect two-dimensional array, by taking the product of $(1, w, w)$ with its transpose $(1, w, w)^T$*

$$\begin{pmatrix} 1 \times 1 & w \times w & w \times w \\ 1 \times w & w \times 1 & w \times w \\ 1 \times w & w \times w & w \times 1 \end{pmatrix} = \begin{pmatrix} 1 & w^2 & w^2 \\ w & w & w^2 \\ w & w^2 & w \end{pmatrix} \tag{3.62}$$

### 3.5.6 Folding perfect sequences to produce higher dimensional array

Let $S$ be a perfect sequence of length $n = m_1m_2$, with $GCD(m_1, m_2) = 1$. The sequence $\boldsymbol{S}$ can be folded into a two-dimensional array $\boldsymbol{A}$ of size $m_1 \times m_2$, preserving perfection [59], as follows:

$$\begin{array}{|c|c|c|c|c|c|c|} \hline s_0 & & & & s_{m_1} & & \\ \hline & s_1 & & & & s_{m_1+1} & \\ \hline & & \ddots & & & & \ddots \\ \hline & & & s_{m_1-1} & & & \\ \hline \end{array} \tag{3.63}$$

**Example 3.13.** *The perfect sequence* $(1, 0, -1, 1, 0, 1)$ *of length* 6 *is folded into a two-dimensional perfect array of size* $2 \times 3$

$$\begin{pmatrix} 1 & 0 & -1 \\ 1 & 0 & 1 \end{pmatrix} \tag{3.64}$$

## 3.6 Known perfect arrays over the complex numbers $\mathbb{C}$

### 3.6.1 Binary perfect arrays

**Definition 3.6.** *Binary array.*

*An array* $\boldsymbol{A}$ *over the binary set* $\{-1, 1\}$ *is called a* ***binary array***.

**Example 3.14.** *Perfect binary array of size* $4 \times 4$

$$\begin{pmatrix} 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 \end{pmatrix} \tag{3.65}$$

In 1992 Jedwab [42] studied a relation between the existence of perfect binary arrays and the existence of combinatorial objects, called **Hadamard Difference Sets**.

Dillion presented in 2010 several perfect multi-dimensional arrays and synchronization patterns with colourful pictures [28]. For more literature on Hadamard difference sets we refer to Beth, Jungnickel and Lenz [14] and Horadam [40].

In 2011 Arasu [3] summarised the state of art of Hadamard Difference Sets and Matrices. Horadam [40] gives a detailed introduction to **Hadamard Matrices**.

### 3.6.2 Ternary perfect arrays

**Definition 3.7.** *Ternary array.*
*An array* $\boldsymbol{A}$ *over the ternary set* $\{-1, 0, 1\}$ *is called a* ***ternary array****.*

**Example 3.15.**

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & -1 & 0 & -1 \\ 1 & 0 & -1 & 1 & 0 & -1 & 1 & 0 & -1 & -1 & 0 & 1 \end{pmatrix} \tag{3.66}$$

In 1990 Antweiler, Bomer and Luke [2] first introduced the term perfect ternary array.

In 1992 Jedwab published some results on generalised perfect arrays that apply to the ternary case as well [42].

In 1999, Arasu and Dillon presented a survey on perfect ternary arrays [6].

In 2011 Arasu summarised the state of art of a known connection between perfect ternary arrays and a group invariant, called a developed matrix. For a detailed literature on perfect ternary arrays, see Arasu [3].

### 3.6.3 Quaternary Perfect arrays

**Definition 3.8.** *Quaternary array.*
*An array* $\boldsymbol{A}$ *over the four roots of unity* $\{1, i, -1, -i\}$ *is called a* ***quaternary array****.*

**Example 3.16.** *Perfect quaternary array of size* $2 \times 2$

$$\begin{pmatrix} 1 & i & -1 & -i \\ i & 1 & i & 1 \\ -1 & i & 1 & -i \\ i & -1 & i & -1 \end{pmatrix} \tag{3.67}$$

Arasu and de Launey [5], and Arasu and Ma [7], have investigated relationships between Hadamard matrices (equivalently Hadamard difference sets) and some perfect quaternary arrays.

In 2001, Arasu and de Launey showed that perfect quaternary arrays are equivalent to relative difference sets. From this connection several new families of perfect quaternary arrays have been constructed [5].

**Example 3.17.** *Perfect quaternary array of size* $6 \times 3$.

$$\begin{pmatrix} -i & i & -1 & 1 & 1 & 1 \\ -1 & -i & -i & -1 & 1 & -i \\ -i & 1 & -i & 1 & i & i \end{pmatrix} \tag{3.68}$$

**Theorem 3.10** (Arasu and de Launey [5]). *Let $l$ be any nonnegative integer. There exist perfect quaternary arrays of size $2^n3^l \times 2^m3^l$, for all nonnegative integers $n$ and $m$ such that $-4 \leq n - m \leq 4$ and $n + m \geq 1$.*

**Theorem 3.11** (Arasu and de Launey [5]). *Let $l$ be any nonnegative integer. Let*

$$p_0, p_1, \ldots, p_k \equiv 3 \ (mod\ 4)\ , \tag{3.69}$$

*be a sequence of primes, and let $g_0, g_1, \ldots, g_k$ be a nondecreasing sequence of positive* *integers such that*

$$p_i = \begin{cases} 2^{g_0}3^{2l} - 1 & \text{if } i = 0, \\ 2^{g_i}3^{2l}p_0^2p_1^2 \dots p_{i-1}^2 - 1 & \text{if } i > 0. \end{cases} \tag{3.70}$$

*Then there exist perfect quaternary arrays of size* $(2^n3^lp_0p_0 \dots p_k) \times (2^m3^lp_0p_1 \dots p_k)$, *for all positive integers n and m such that* $-4 \leq n - m \leq 4$ *and* $n + m \geq g_k - 1$.

**Theorem 3.12** (Arasu and de Launey [5]). *Let l be a positive integer. Let* $p_0, p_1, \dots, p_k$ *be a sequence of odd primes where*

$$p_0 \equiv 1 \ (mod\ 4), \tag{3.71}$$

*and let* $g_0, g_1, \dots, g_k$ *be a nondecreasing sequence of positive integers such that*

$$p_i = \begin{cases} 2^{g_0}3^{2l} - 1 & \text{if } i = 0, \\ 2^{g_i}3^{2l}p_0^2p_1^2 \dots p_{i-1}^2 - 1 & \text{if } i > 0. \end{cases} \tag{3.72}$$

*Then there exist perfect quaternary arrays of size* $(2^n3^lp_0p_0 \dots p_k) \times (2^m3^lp_0p_1 \dots p_k)$, *for all positive integers n and m such that* $-3 \leq n - m \leq 3$ *and* $n + m \geq max(1, g_k - 1)$, *except possibly for* $(m, n) = (0, 2), (2, 0)$.

In Chapter 8, we use the Arasu and de Launey construction, for inflating perfect quaternary arrays, to produce new perfect arrays over the basic quaternions $\{1, -1, i, -i, j, -j, k, -k\}$ of larger sizes.

CHAPTER

4

# PERFECT SEQUENCES OVER THE QUATERNIONS $\mathbb{H}$

PERFECT sequences, over the algebra of quaternions $\mathbb{H}$, were first introduced by Kuznetsov in 2009 [45]. This insight provided a new research field regarding sequences and their correlation. The algebra of quaternions is associative but not commutative, and so the concepts of right and left autocorrelation were introduced. Likewise, the concepts of right and left perfection of sequences over the quaternions were introduced. Moreover, it was shown that these two concepts are equivalent [45, 46]. One year later, Kuznetsov and Hall showed a construction of a perfect sequence of length $5,354,228,880$ over a quaternion alphabet with 24 elements, namely the double-tetrahedron group $\mathbb{H}_{24} \subset \mathbb{H}$ [47].

Kuznetsov and Hall [47] conjectured there are perfect sequences of unbounded lengths over the double-tetrahedron group $\mathbb{H}_{24}$.

The author and T. E. Hall worked on Kuznetsov and Hall's problem and found a family of perfect sequences of **unbounded lengths** over $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, which is an alphabet more likely to be implemented in Electronic Communication, smaller than $\mathbb{H}_{24}$ and easier to handle, as we shall see in Chapter 6.

We found that the smaller alphabet, $\{\pm 1, \pm i, j\}$ is sufficient. Kuznetsov published in [46] a sequence of length 10, equivalent to one of ours, and S. Blake found sequences up to length 98 equivalent to ours, by computer search (unpublished).

In this chapter, we introduce the basic definitions and the main results regarding perfect sequences over the quaternion algebra.

## 4.1 Algebra of Quaternions

The quaternions were discovered by Sir William Rowan Hamilton in 1843 (Van der Waerden [72]). Quaternions are an algebraic structure similar to a field, except for the commutativity of the product. This kind of structure is called a **skew field**. Getting excited by the way the complex numbers are applied in the Euclidean plane geometry, Hamilton had spent a number of years trying to invent a bigger structure which can be similarly applied in three-dimensional geometry. By analogy with the complex numbers, Hamilton attempted to construct the new numbers by means of attaching the second imaginary unit to the well known, by that time, complex numbers [46]. So he introduced a new imaginary unit $j$, with $j^2 = -1$, and studied the numbers of the form $a + bi + cj$, where $a, b, \in \mathbb{R}$. Hamilton found an inconsistency as follows. Since the new number system is required to be closed under multiplication, the product of the two imaginary units $i$ and $j$

is of the form

$$ij = a + bi + cj, \tag{4.1}$$

with $a, b, c$ real numbers. Hamilton found that

$$\begin{aligned} -j = \;& i^2 j = i(ij) = i(a + bi + cj) = ai + bi^2 + cij = ai - b + c(a + bi + cj) \\ = \;& (ac - b) + (a + bc)i + c^2 j, \end{aligned} \tag{4.2}$$

which implies an inconsistent equation $c^2 = -1$, with $c \in \mathbb{R}$.

In modern terms, Hamilton tried to construct a three-dimensional field, which is impossible, according to Frobenius's result: For $n > 2$, $\mathbb{R}^n$ can not be made into a field [74].

Years later, Hamilton realised, in a famous moment of inspiration, that the solution was a higher dimensional space: it was not in $\mathbb{R}^3$, but in $\mathbb{R}^4$ that one could introduce a meaningful multiplication, connected to rotations in $\mathbb{R}^3$ [8]. The third imaginary number $k$ was introduced. Numbers of the form $a + bi + cj + dk$, where $a, b, c, d \in \mathbb{R}$ have been called (real) quaternions [26].

**Definition 4.1.** *Algebra of Quaternions.*
*The algebra of quaternions $\mathbb{H}$ is defined as follows: it is an algebra generated by the elements $i$ and $j$, over the real number field $\mathbb{R}$, with the following multiplication rules*

$$i^2 = -1, \quad j^2 = -1 \quad \textit{and} \quad ij = -ji. \tag{4.3}$$

*This last equation makes the algebra non-commutative. For the sake of simplicity the product $ij$ is denoted by $k$. Then*

$$ij = k, \quad jk = i, \quad ki = j. \tag{4.4}$$

*and*

$$ji = -k, \quad kj = -i, \quad ik = -j. \tag{4.5}$$

*The quaternion algebra can be regarded as a 4-dimensional* $\mathbb{R}$*-vector space with basis vectors*

$$1 = (1,0,0,0), \quad i = (0,1,0,0), \quad j = (0,0,1,0) \quad \textit{and} \quad k = (0,0,0,1). \tag{4.6}$$

*Every quaternion $q$ can be written as*

$$q = a1 + bi + cj + dk, \tag{4.7}$$

*for $a, b, c, d \in \mathbb{R}$.*

The real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$ are special cases of quaternion numbers.

**Definition 4.2.** *Addition of Quaternions.*
*For any quaternions $p = p_0 + p_1 i + p_2 j + p_3 k$ and $q = q_0 + q_1 i + q_2 j + q_3 k$, addition of $p$ and $q$ is given by the rule*

$$p + q = (p_0 + q_0) + (p_1 + q_1)i + (p_2 + q_2)j + (p_3 + q_3)k. \tag{4.8}$$

**Definition 4.3.** *Multiplication of Quaternions.*
*For any quaternions $p = p_0 + p_1 i + p_2 j + p_3 k$ and $q = q_0 + q_1 i + q_2 j + q_3 k$, multiplication of $p$ and $q$ is given by the rule*

$$\begin{aligned} pq = \; & (p_0q_0 - p_1q_1 - p_2q_2 - p_3q_3) + (p_0q_1 + p_1q_0 + p_2q_3 - p_3q_2)i + \\ & (p_0q_2 + p_2q_0 + p_3q_1 - p_1q_3)j + (p_0q_3 + p_3q_0 + p_1q_2 - p_2q_1)k. \end{aligned} \tag{4.9}$$

*The multiplication of two quaternions can commute, anti-commute, or neither of the two.*

**Example 4.1.**

1. *Commutative case:* $(1+k)(1-k) = 2 = (1-k)(1+k)$.
2. *Anti-commutative case:* $ij = k$ *and* $ji = -k$.
3. *Neither commutative, nor anti-commutative* $(1+i)(j+k) = 2k$ *and* $(j+k)(1+i) = 2j$.

**Definition 4.4.** *Conjugation.*

*The quaternion algebra has conjugation, given by*

$$i^* = -i, \quad j^* = -j \quad \textit{and} \quad k^* = -k. \tag{4.10}$$

*In general, for any quaternion* $q = q_0 + q_1 i + q_2 j + q_3 k$*, its conjugate is* $q^* = q_0 - q_1 i - q_2 j - q_3 k$.

**Definition 4.5.** *Norm of a quaternion.*

*For any quaternion* $q = q_0 + q_1 i + q_2 j + q_3 k$*, the norm of* $q$ *is*

$$\|q\| = qq^* = q_0^2 + q_1^2 + q_2^2 + q_3^2. \tag{4.11}$$

*A quaternion of norm 1 is called a unit quaternion.*

**Definition 4.6.** *Basic quaternions group.*

*The set* $\mathbb{H}_8 = \{1, -1, i, -i, j, -j, k, -k\}$ *in* $\mathbb{H}$ *forms a group under the multiplication operation. We refer to this group as the basic quaternions group.*

**Definition 4.7.** *Double-tetrahedron group.*

*The set* $\mathbb{H}_{24} = \{\pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2}\}$ *in* $\mathbb{H}$ *forms a group under the multiplication operation. We refer to this group as the double-tetrahedron group. Notice that* $\mathbb{H}_8 \subset \mathbb{H}_{24} \subset \mathbb{H}$.

## 4.2 Autocorrelation of sequences over quaternions

**Definition 4.8.** *[45,46]. Right and left autocorrelation.*

*Let* $\mathbf{S} = (s_0, s_1, \ldots, s_{n-1})$ *be a sequence over any quaternion alphabet. For an integer* $\tau \geq 0$*, the* ***right*** *and* ***left periodic autocorrelation*** *of the sequence* $\mathbf{S}$*, for the shift* $\tau$ *are*

$$AC^R_{\mathbf{S}}(\tau) = \sum_{i=0}^{n-1} s_i s^*_{i+\tau}\,, \tag{4.12}$$

$$AC^L_{\mathbf{S}}(\tau) = \sum_{i=0}^{n-1} s^*_i s_{i+\tau}. \tag{4.13}$$

We wrote the following two codes in *Mathematica* to compute the left and right cross-correlation functions of a sequence over any quaternion alphabet.

```
In[1]:= << Quaternions'
In[2]:= i = Quaternion[0, 1, 0, 0]
Out[2]= Quaternion[0, 1, 0, 0]
In[3]:= j = Quaternion[0, 0, 1, 0]
Out[3]= Quaternion[0, 0, 1, 0]
In[4]:= k = Quaternion[0, 0, 0, 1]
Out[4]= Quaternion[0, 0, 0, 1]
```

```
In[5]:= LCCVS[n_, m_ ] := Table[Simplify[Sum[n[[r]] **
        Conjugate[ m[[If[0 < Mod[r + s - 1, Length[m]] <
        Length[m], Mod[r + s - 1, Length[m]], If[Mod
        [r + s - 1, Length[m]] > Length[m], Mod[r + s - 1,
        Length[m]] + 1, Length[m]]]]]], {r, 1,Length[m]}]],
        {s, Length[m]}]
```

```
In[6]:= RCCVS[n_, m_ ] := Table[Simplify[Sum[
     Conjugate[n[[r]]] ** m[[If[0 < Mod[r + s - 1,
     Length[m]] < Length[m], Mod[r + s - 1, Length[m]],
     If[Mod[r + s - 1, Length[m]] > Length[m],Mod[r + s
     - 1, Length[m]] + 1, Length[m]]]]], {r, 1,
     Length[m]}]], {s, Length[m]}]
```

We also wrote the following two codes in *Mathematica* to compute the left and right autocorrelation functions of a sequence over any quaternion alphabet.

```
In[7]:= LACVS[m_ ] := Table[Simplify[Sum[m[[r]] **
     Conjugate[m[[If[0 < Mod[r + s - 1, Length[m]] <
     Length[m], Mod[r + s - 1, Length[m]], If[Mod[
     r + s - 1, Length[m]] > Length[m], Mod[r + s - 1,
     Length[m]] + 1, Length[m]]]]]],
     {r, 1, Length[m]}]], {s, Length[m]}]
```

```
In[8]:= RACVS[m_ ] := Table[Simplify[Sum[Conjugate[m[[r]]]
     ** m[[If[0 < Mod[r + s - 1, Length[m]] < Length[m],
     Mod[r + s - 1, Length[m]], If[Mod[r + s - 1, Length
     [m]] > Length[m], Mod[r + s - 1, Length[m]] + 1,
     Length[m]]]]], {r, 1,  Length[m]}]], {s, Length[m]}]
```

**Example 4.2.** *In this example we find left and right autocorrelation values for the sequence* $(j, j, -1, -k, i, -j)$.

| *Left and Right AC values of $(j, j, -1, -k, i, -j)$* | | |
|---|---|---|
| *Shift* | $AC_S^L$ | $AC_S^R$ |
| *0* | *6* | *6* |
| *1* | *0* | *2j+2k* |
| *2* | *-1+3i-j-k* | *-1+i+j-k* |
| *3* | *0* | *0* |
| *4* | *-1-3i+j+k* | *-1-i-j+k* |
| *5* | *0* | *-2j-2k* |

(4.14)

**Definition 4.9.** *Right and left perfection.*

*Let* $\mathbf{S} = (s_0, s_1, \ldots, s_{n-1})$ *be a sequence over any quaternion alphabet. The sequence* $\mathbf{S}$ *is called right (left) perfect if its right (left) periodic autocorrelation function* $AC_{\mathbf{S}}^R(\tau)$ $\big(AC_{\mathbf{S}}^L(\tau)$*, respectively*$\big)$ *is zero, for each non-zero shift* $\tau$*.*

## 4.3 Equivalence of right and left perfection

In 2009, Kuznetsov proved that the concepts of right and left perfection over the quaternions are equivalent [45]. This equivalence allows us to call any right or left perfect sequence over quaternions, a perfect sequence over quaternions.

**Theorem 4.1** (Kuznetsov [45])**.** *Let* $\mathbf{S}$ *be any sequence over any quaternion alphabet. The sequence* $\mathbf{S}$ *is right perfect if and only if it is left perfect.*

**Example 4.3.** *A perfect sequence of length 26 over the basic quaternions* $\{\pm 1, \pm i, \pm j, \pm k\}$

$$(1, i, j, -i, -1, i, -1, -k, j, -k, -j, -i, -j, i, -j, -i, -j, -k, j, -k, -1, i, -1, -i, j, i). \tag{4.15}$$

## 4.4 Transformations preserving perfection over quaternions

The next theorem explains some transformations on perfect sequences over quaternions that preserve perfection.

**Theorem 4.2** (Kuznetsov [46]). *If $\mathbf{S} = (s_t)$, where $0 \leq t \leq n-1$, is a perfect sequence over any quaternion alphabet, then so are the sequences obtained as follows.*

1. *Shift $m$ places to the right: $(s_{t+m})$, where $0 \leq t \leq n-1$ and $m$ is any integer and the subscript is calculated modulo $n$.*
2. *Left and right multiplication by constants: $(ps_tq)$, where $0 \leq t \leq n-1$ and $p$ and $q$ are any quaternion numbers.*
3. *Conjugation: $(s_t^*)$, where $0 \leq t \leq n-1$ and $s_t^*$ denotes the conjugate of $s_t$.*
4. *Multiplying entries by consecutive roots of unity: If all the entries of $\mathbf{S}$ commute with the $n$-th roots of unity $w = e^{\frac{2\pi si}{n}}$, for $1 \leq s \leq n-1$, then $(s_t w^t)$, where $0 \leq t \leq n-1$, is perfect. This property is still valid for length $kn$.*
5. *Proper decimation: A proper decimation of a perfect sequence is perfect, i.e., if $p$ is a positive integer coprime with $n$, then the sequence $Dec_p(\mathbf{S})$, obtained by decimating the sequence $\mathbf{S}$ by $p$, is perfect.*

**Example 4.4.** *Given the perfect sequence*

$$\mathbf{S} = (1, k, -j, -i, j, i, 1, i, 1, i, j, -i, -j, k). \tag{4.16}$$

*of length 14 over the basic quaternions $\{\pm 1, \pm i, \pm j, \pm k\}$, we have the following transformations*

1. *Shifting the perfect sequence $\mathbf{S}$ by 7, produces the perfect sequence*

$$\mathbf{S}^7 = (i, 1, i, j, -i, -j, k, 1, k, -j, -i, j, i, 1). \tag{4.17}$$

2. *Multiplying the perfect sequence* $\boldsymbol{S}$ *by the quaternions* $j$ *and* $k$ *by the left and right, respectively, produces the perfect sequence*

$$jSk = (i,-j,k,-1,-k,1,i,1,i,1,-k,-1,k,-j). \tag{4.18}$$

3. *Conjugating the perfect sequence* $\boldsymbol{S}$ *produces the perfect sequence*

$$\boldsymbol{S}^* = (1,-k,j,i,-j,-i,1,-i,1,-i,-j,i,j,-k). \tag{4.19}$$

4. *Decimating the perfect sequence* $\boldsymbol{S}$ *by 3, produces the perfect sequence*

$$Dec_3(\boldsymbol{S}) = (1,-i,1,i,-j,k,j,i,j,k,-j,i,1,-i). \tag{4.20}$$

Let us recall that the sum of all elements in a sequence is called the balance of the sequence. The next theorem explains the perfection of a sequence of balances of decimations of a perfect sequence.

**Theorem 4.3** (Kuznetsov [46]). *Let* $\boldsymbol{S} = (s_0,\ldots,s_{n-1})$ *be a perfect sequence over an alphabet of complex numbers, and* $n_1$ *and* $n_2$ *two integers such that* $n_1, n_2 \geq 2$ *and* $n = n_1 n_2$*. The sequence*

$$\left(\sum_{i=0}^{n_1-1} s_{in_2}, \sum_{i=0}^{n_1-1} s_{1+in_2}, \sum_{i=0}^{n_1-1} s_{2+in_2}, \ldots, \sum_{i=0}^{n_1-1} s_{n_2-1+in_2}\right), \tag{4.21}$$

*of length* $n_2$ *is perfect.*

We wrote the following codes in *Mathematica* to compute the sequence of decimations of any sequence over any quaternion alphabet.

```
In[1]:= << Quaternions'
In[2]:= i = Quaternion[0, 1, 0, 0]
Out[2]= Quaternion[0, 1, 0, 0]
```

```
In[3]:= j = Quaternion[0, 0, 1, 0]
Out[3]= Quaternion[0, 0, 1, 0]
In[4]:= k = Quaternion[0, 0, 0, 1]
Out[4]= Quaternion[0, 0, 0, 1]
In[5]:= Reductor[list_, d_] := (m = Length[list]/d;
   Table[Sum[list[[j + i*m]], {i, 0, d - 1}], {j, 1, m}])
```

**Example 4.5.** *Consider the perfect sequence*

$$\boldsymbol{S} = (1, k, -j, -i, j, i, 1, i, 1, i, j, -i, -j, k), \tag{4.22}$$

*of length 14. By Theorem (4.3), for $n_1 = 2$ and $n_2 = 7$, we obtain the perfect sequence $\boldsymbol{T}$ of length 7, by adding together the pairs of entries 7 apart*

$$\boldsymbol{T} = (1 + i, 1 + k, i - j, -i + j, -i + j, i - j, 1 + k). \tag{4.23}$$

## 4.5 Composition of sequences over quaternions

**Theorem 4.4** (Luke [53]). *Let $\boldsymbol{S} = (s_0, \ldots, s_{m-1})$ and $\boldsymbol{U} = (u_0, \ldots, u_{n-1})$ be two sequences over complex numbers, such that their lengths $m$ and $n$ are relatively prime numbers. The autocorrelation values of the composition of $\boldsymbol{S}$ and $\boldsymbol{U}$, are the products of their individual autocorrelation values, that is, for $0 \leq \tau \leq mn - 1$*

$$AC_{\boldsymbol{S} \circ \boldsymbol{U}}(\tau) = AC_{\boldsymbol{S}}(\tau \ (mod\ m)) AC_{\boldsymbol{U}}(\tau \ (mod\ n)). \tag{4.24}$$

**Corollary 4.1.** *Let $\boldsymbol{S} = (s_0, \ldots, s_{m-1})$ and $\boldsymbol{U} = (u_0, \ldots, u_{n-1})$ be two perfect sequences over the complex numbers, such that their lengths $m$ and $n$ are relatively prime* *numbers. Then their composition*

$$\boldsymbol{S} \circ \boldsymbol{U} = (s_{t \ (mod \ m)} u_{t \ (mod \ n)}), \tag{4.25}$$

*for $t = 0, \dots, mn-1$, is perfect.*

Theorem (4.4) does not necessarily hold for sequences over any quaternion alphabet, as we can see in the next example. However, Corollary (4.1) holds for sequences over any quaternion alphabet [46].

**Example 4.6.** *Consider the sequences $\boldsymbol{S} = (1, 1, i)$ and $\boldsymbol{U} = (1, j)$. When we calculate the autocorrelation values for shift 4, we have*

$$\begin{aligned} &AC^L_{\boldsymbol{S}\circ\boldsymbol{U}}(4) = -i, \\ &AC^L_{\boldsymbol{S}}(4) = AC^L_{\boldsymbol{S}}(1) = 1, \\ &AC^L_{\boldsymbol{U}}(4) = AC^L_{\boldsymbol{U}}(0) = 2. \end{aligned} \tag{4.26}$$

*Therefore*

$$AC^L_{\boldsymbol{S}\circ\boldsymbol{U}}(4) \neq AC^L_{\boldsymbol{S}}(4) AC^L_{\boldsymbol{U}}(4). \tag{4.27}$$

**Theorem 4.5** (Kuznetsov [46]). *Let $\boldsymbol{S} = (s_0, \dots, s_{m-1})$ and $\boldsymbol{U} = (u_0, \dots, u_{n-1})$ be two perfect sequences over the quaternions, such that their lengths m and n are relatively prime numbers. Then their composition*

$$\boldsymbol{S} \circ \boldsymbol{U} = (s_{t \ (mod \ m)} u_{t \ (mod \ n)}), \tag{4.28}$$

*for $t = 0, \dots, mn-1$, is perfect.*

**Example 4.7.** *Given the perfect sequences $(1+i, 1+k, i-j, -i+j, -i+j, i-j, 1+k)$*

*and* $(1, i, -1, i)$*, we take their composition, to produce the length-28 perfect sequence*

$$\begin{aligned}&(1+i, i-j, -i+j, 1+k, -i+j, -1-k, -1-k, -1+i, 1+k, -1-k, i-j, 1+k,\\ &i-j, i-j, -1-i, i-j, i-j, 1+k, i-j, -1-k, 1+k, -1+i, -1-k, -1-k,\\ &-i+j, 1+k, -i+j, i-j).\end{aligned} \tag{4.29}$$

Based on Theorem (4.5), Kuznetsov and Hall showed the existence of a perfect sequence of length 5,354,228,880, over the alphabet $\mathbb{H}_{24} = \{\pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2}\}$ [47]. From this idea, Kuznetsov and Hall posed the question: Are there perfect sequences of unbounded lengths over the alphabet $\mathbb{H}_{24}$? An affirmative answer to this question will be given in the present work in Chapter 6.

**Theorem 4.6** (Kuznetsov [45]). *Let* $\boldsymbol{S} = (s_0, \ldots, s_{m-1})$ *and* $\boldsymbol{U} = (u_0, \ldots, u_{n-1})$ *be two perfect sequences over unit quaternions with even lengths m and n, so that the following conditions are satisfied:*

1. *m is not a multiple or a divisor of n.*
2. *Sequence* $\boldsymbol{S}$ *is perfect.*
3. *Sequence* $Dec_2(\boldsymbol{U})$*, and hence sequence* $Dec_2(\boldsymbol{U})^1$*, is perfect, where* $Dec_2(\boldsymbol{U})^1$ *means the rotation by 1 of the sequence* $Dec_2(\boldsymbol{U})$*.*
4. $CC^R_{Dec_2(\boldsymbol{U}),Dec_2(\boldsymbol{U})^1}(t-1) = CC^R_{Dec_2(\boldsymbol{U})^1,Dec_2(\boldsymbol{U})}(t)$*, for* $1 \leq t \leq \lceil \frac{n}{4} \rceil$.
5. $CC^R_{Dec_2(\boldsymbol{U})^1,Dec_2(\boldsymbol{U})}(t)$ *are real numbers for* $1 \leq t \leq \lfloor \frac{n}{4} \rfloor$.

*Then, the composition sequence*

$$\boldsymbol{S} \circ \boldsymbol{U} = (s_{t \ (mod \ m)} u_{t \ (mod \ n)}), \tag{4.30}$$

*with* $0 \leq t \leq LCM(m, n) - 1$*, is perfect.*

**Example 4.8.** *The sequence*

$$\boldsymbol{U} = \left(1, \frac{-1+i+j+k}{2}, 1, 1, \frac{-1+i+j+k}{2}, 1\right), \tag{4.31}$$

*of length 6, has properties 3-5 of Theorem (4.6). For the perfect sequence* $\boldsymbol{S} = (1, i, -1, i)$ *of length 4, we have that* $m = 4$ *is not a multiple or divisor of* $n = 6$*. Therefore we can compose the sequences* **S** *and* **U** *to produce the length-12 perfect sequence*

$$\left(1, \frac{-1+i+j+k}{2}, 1, -1, \frac{-1+i+j+k}{2}, 1, 1, \frac{1-i-j-k}{2}, 1, 1, \frac{-1+i+j+k}{2}, -1\right). \tag{4.32}$$

## 4.6 Balance theorem over quaternions

The Balance Theorem, by Bomer and Antweiler [17], is also valid for perfect sequences over any quaternion alphabet.

**Theorem 4.7.** *Let* $S = (s_0, \ldots, s_{m-1})$ *be a perfect sequence over any quaternion alphabet. Then*

$$\left\|\sum_{t=0}^{n-1} s_t\right\| = \sum_{t=0}^{n-1} \|s_t\|. \tag{4.33}$$

**Example 4.9.** *Consider the perfect sequence of length 24 over the basic quaternions* $\{\pm 1, \pm i, \pm j, \pm k\}$

$$\boldsymbol{S} = (1, -1, i, -i, k, -j, -i, j, k, i, i, 1, 1, 1, i, i, k, j, -i, -j, k, -i, i, -1). \tag{4.34}$$

*Since all elements of* **S** *have norm equal to 1, we have*

$$\begin{aligned} \left\|\textstyle\sum_{t=0}^{n-1} s_t\right\| &= ||4(1) + 2(-1) + 6(i) + 4(-i) + 2(j) + 2(-j) + 4(k)|| \\ &= ||2(1) + 2(i) + 4(k)|| = 2^2 + 2^2 + 4^2 = 24 \\ &= \textstyle\sum_{t=0}^{n-1} \|s_t\|. \end{aligned} \tag{4.35}$$

The next theorem presents a generalisation of the Balance Theorem for sequences over any quaternion alphabet.

**Theorem 4.8** (Kuznetsov [46]). *Let $\boldsymbol{S} = (s_0, \ldots, s_{n-1})$ be a perfect sequence over any quaternion alphabet and $n = lm$, for some positive integers $l$ and $m$. Then*

$$\sum_{t_1=0}^{l-1} \left\| \sum_{t_2=0}^{m-1} s_{t_1+lt_2} \right\| = \sum_{t=0}^{n-1} \|s_t\|. \tag{4.36}$$

**Example 4.10.** *Consider the perfect sequence of length 6 over the basic quaternions $\{\pm 1, \pm i, \pm j, \pm k\}$*

$$\boldsymbol{S} = (1, k, 1, -1, -i, -k). \tag{4.37}$$

*By Theorem (4.8), we have*

$$\begin{aligned} \|s_0 + s_2 + s_4\| + \|s_1 + s_3 + s_5\| &= \|2 - i\| + \| - k\| = 6, \\ \|s_0 + s_3\| + \|s_1 + s_4\| + \|s_2 + s_5\| &= \|1 - k\| + \| - i + k\| + \|1 - k\| = 6. \end{aligned} \tag{4.38}$$

Theorems (4.7) and (4.8) can be thought of as giving necessary conditions for a sequence over the quaternions to be perfect.

## 4.7 Discrete Fourier transform of a perfect sequence over quaternions

**Definition 4.10.** *Let $\boldsymbol{S} = (s_0, \ldots, s_{m-1})$ be a sequence over any quaternion alphabet. The sequences $DFT^L(\boldsymbol{S}) = \boldsymbol{U}^L = (u_0^L, \ldots, u_{n-1}^L)$ and $DFT^R(\boldsymbol{S}) = \boldsymbol{U}^R =$*

*$(u_0^R, \ldots, u_{n-1}^R)$, with*

$$u_t^L = \sum_{r=0}^{n-1} \left( e^{-\frac{2\pi i}{n} tr} \right) s_t, \tag{4.39}$$

*and*

$$u_t^R = \sum_{r=0}^{n-1} s_t \left( e^{-\frac{2\pi i}{n} tr} \right), \tag{4.40}$$

*where $e^{\frac{2\pi i}{n}}$ is the principal n-th complex root of unity, are called the **left** and **right discrete Fourier transforms** of the sequence **S***

We wrote the following codes in *Mathematica* to compute the left and right discrete Fourier transform coefficients of a sequence over quaternions

```
In[1]:= << Quaternions`
In[2]:= i = Quaternion[0, 1, 0, 0]
Out[2]= Quaternion[0, 1, 0, 0]
In[3]:= j = Quaternion[0, 0, 1, 0]
Out[3]= Quaternion[0, 0, 1, 0]
In[4]:= k = Quaternion[0, 0, 0, 1]
Out[4]= Quaternion[0, 0, 0, 1]
```

```
In[5]:= DFTL[l_] :=  Table[Sum[ToQuaternion[E^(-2*Pi*I*s*r
     /Length[l])] ** l[[r + 1]], {r, 0, Length[l] - 1}],
     {s, 0, Length[l] - 1}]
```

```
In[6]:= DFTR[l_] :=  Table[Sum[l[[r + 1]] ** ToQuaternion[
     E^(-2*Pi*I*s*r/Length[l])], {r, 0, Length[l] - 1}],
     {s, 0, Length[l] - 1}]
```

Left and right discrete Fourier transforms of a sequence $S = (s_0, \dots, s_{m-1})$ are not necessarily the same, as we can see in the following example

**Example 4.11.** *The table below shows that left and right discrete Fourier transforms of the sequence $(1+i, i+j, j+k, k+1)$ are not necessarily equal.*

| *Left and Right Fourier transform of* $(1+i, i+j, j+k, k+1)$ | | |
|---|---|---|
| *Shift* | $\boldsymbol{U}^L$ | $\boldsymbol{U}^R$ |
| *0* | *2+2i+2j+2k* | *2+2i+2j+2k* |
| *1* | *2+2i-2j-2k* | *2+2i* |
| *2* | *0* | *0* |
| *3* | *0* | *-2j-2k* |

(4.41)

For sequences over the complex numbers, we have

1. A sequence $S$ is perfect if and only if all its discrete Fourier transform coefficients are of equal norm.
2. For any sequence $S$ with all elements of equal norm, the discrete Fourier transform of $S$ is perfect.

Perfection of a sequence over the quaternions is not equivalent to the conditon that the right and left Fourier transform coefficients are all of equal norm. Likewise, a sequence $S$ over the quaternions with all elements of equal norm does not imply that the right (or left) Fourier transform of the sequence $S$ is perfect, as we can see in the following examples

**Example 4.12.** *Consider the perfect sequence $S = (1, i, 1, k)$. The left and right Fourier transform coefficients of $S$ are listed below.*

$$\begin{aligned} DFT^L(S) &= (2+i+k, 1-j, 2-i-k, -1+j). \\ DFT^R(S) &= (2+i+k, 1+j, 2-i-k, -1-j). \end{aligned} \tag{4.42}$$

*The norms of the entries of $DFT^L(\mathbf{S})$ and $DFT^R(\mathbf{S})$ are listed below*

$$\begin{aligned} \textit{Norm of entries of } DFT^L(\mathbf{S}) &= (6,2,6,2). \\ \textit{Norm of entries of } DFT^R(\mathbf{S}) &= (6,2,6,2). \end{aligned} \tag{4.43}$$

*We can observe that the entries of the sequence $DFT^L(\mathbf{S})$ have different norms, and likewise for the sequence $DFT^R(\mathbf{S})$. So, perfection of a sequence over quaternions does not imply left and right Fourier transform coefficients have equal norm.*

**Example 4.13.** *Consider the non-perfect sequence $(1,1,j,-j)$. The left and right Fourier transforms of **S** are listed below.*

$$\begin{aligned} DFT^L(\mathbf{S}) &= (2,1-i-j-k,2j,1+i-j+k). \\ DFT^R(\mathbf{S}) &= (2,-1-i-j+k,2j,1+i-j-k). \end{aligned} \tag{4.44}$$

*The norms of the entries of $DFT^L(\mathbf{S})$ and $DFT^R(\mathbf{S})$ are listed below*

$$\begin{aligned} \textit{Norm of entries of } DFT^L(\mathbf{S}) &= (4,4,4,4). \\ \textit{Norm of entries of } DFT^R(\mathbf{S}) &= (4,4,4,4). \end{aligned} \tag{4.45}$$

*So, having left and right Fourier transform coefficients of equal norm does not imply perfection.*

**Example 4.14.** *Consider the non-perfect sequence $\mathbf{S} = (1,i,1,k)$ over the basic quaternions, whose entries all have norm 1. The left and right Fourier transforms of **S** are listed below.*

$$\begin{aligned} DFT^L(\mathbf{S}) &= (2+i+k,1-j,2-i-k,-1+j). \\ DFT^R(\mathbf{S}) &= (2+i+k,1+j,2-i-k,-1-j). \end{aligned} \tag{4.46}$$

*Neither the left nor the right Fourier transforms are perfect, since their correlations are*

$$\begin{aligned} AC^L_{DFT^L(\mathbf{S})} &= (16,8k,0,-8k), \\ AC^L_{DFT^R(\mathbf{S})} &= (16,8i,0,-8i), \end{aligned} \tag{4.47}$$

*respectively.*

CHAPTER

# 5

# LEE SEQUENCES

LEE Sequences are the cornerstone of the proof of the existence of perfect sequences of unbounded lengths over the basic quaternions. In order to introduce and prove this result, we need to understand the underlying structure of Lee Sequences.

In 1992, C. E. Lee presented a construction of perfect sequences over the alphabets $\{0, w_m^1, w_m^2, \ldots, 1\}$, where $w_m$ is a primitive $m$-th root of unity [50]. For the case $w = i$, where $i$ is the fourth root of unity, the alphabet is $\{0, 1, -1, i, -i\}$, and over this alphabet, Lee constructed a family of perfect sequences of unbounded lengths, namely for all lengths $m = p + 1 \equiv 2 \ (mod\ 4)$, with $p$ a prime number. That is, for $m = 6, 14, 18, 30...$ [49]. In 1996, H. D. Luke presented a generalisation of Lee's construction, for all lengths $m = p^k + 1 \equiv 2 \ (mod\ 4)$, where $k \in \mathbb{N}$ and $p$

is a prime number, that is, for $m = 6, 10, 14, 18, 26, 30...$ [54]. The sequences constructed by Lee in [49] and generalised by Luke in [54] are called **Lee Sequences** and they have the following properties: they have a single zero entry, are palindromic about two centres, alternate from $\pm i$ to $\pm 1$, ignoring the zero, and have even length.

## 5.1 Properties of Lee sequences

The following properties of Lee sequences come from Luke and Schotten's construction [57] and the Binary-to-Polyphase transform [54].

1. They exist for all lengths $m = p^a + 1 \equiv 2 \ (mod\ 4)$, with $p$ an odd prime number and $a$ any natural number. This follows from the existence of odd-perfect sequences of lengths $m = p^a + 1$ [27] and the Binary-to-Polyphase (BTP) transform [54].
2. They are almost quaternary, i.e., there is only one zero occurrence in the sequence. The rest of the entries are four roots of unity.
3. They are symmetric about the zero, i.e., from the zero, reading the sequence to the right with wrap around is the same as reading the sequence to the left with wrap around. This property follows from the skew symmetric property of the family of odd-perfect sequences given in Luke and Schotten construction [57].
4. They alternate from $\pm i$ to $\pm 1$, ignoring the zero.
5. They have even lengths. See Lemma (5.1).

In the next lemma we find some more properties of Lee sequences.

**Lemma 5.1** (Barrera and Hall [10]). *For any Lee sequence* $\mathbf{S}$ *of length* $m$*, with* $a, b, c$ *and* $d$ *being equal to the number of* $1, -1, i$ *and* $-i$ *occurrences, respectively, we have*

1. *$(a-b)^2+(c-d)^2 = m-1$.*
2. *$m$ is even.*
3. *Either $a-b$ and $a+b$ are odd, or $c-d$ and $c+d$ are odd.*
4. *$\frac{m}{2}$ is odd.*

*Proof.* 1. The Balance Theorem (3.3) for perfect sequences states that

$$\sum_{l=0}^{m-1} ||a_l|| = ||\sum_{l=0}^{m-1} a_l||, \tag{5.1}$$

which implies that

$$m-1 = ||a+b(-1)+ci+d(-i)|| = (a-b)^2+(c-d)^2. \tag{5.2}$$

2. This follows from cancellation occurring in pairs only, in the calculation of each off-peak autocorrelation value. If $t \neq 0$, then in the summation $\sum_{l=0}^{m-1} a_l a_{l+t}^*$ there are exactly two zeros. Therefore $a(1)+b(-1)+c(i)+d(-i)=0$. From this equation we conclude that $a=b$ and $c=d$ and so $m=2+2a+2b=2(1+a+b)$, which is an even number.
3. From (1), since $m-1$ is odd, we have either $a-b$ or $c-d$ is odd and the other is even. If $a-b$ is even, then so is $a-b+2b=a+b$. Similarly, if $c-d$ is even, then so is $c-d+2d=c+d$.
4. (a) Case $a-b$ is even and $c-d$ is odd. Set $a-b=2r$ and $c-d=2s+1$. Then

$$\begin{aligned} m &= (a-b)^2+(c-d)^2+1 \\ &= 4r^2+4s^2+4s+1+1 \\ &= 4(r^2+s^2+s)+2. \end{aligned}$$

Thus, $\frac{m}{2} = 2(r^2+s^2+s)+1$ is odd.

(b) Case $a - b$ is odd and $c - d$ is even. Similar.

□

## 5.2 Existence of Lee sequences

In the next theorem C. E. Lee proved the existence of infinitely many Lee Sequences [49].

**Theorem 5.1** (Lee [49]). *There exist Lee sequences of unbounded lengths, namely for lengths* $m = p + 1 \equiv 2 \ (mod\ 4)$, *where* $p$ *is a prime number, that is, for* $m = 6, 14, 18, 30...$

In the next theorem, Luke [54] generalised Theorem (5.1).

**Theorem 5.2** (Luke [54]). *There exist Lee sequences of unbounded lengths, namely for lengths* $m = p^a + 1 \equiv 2 \ (mod\ 4)$, *where* $p$ *is a prime number and* $a > 0$, *that is, for* $m = 6, 10, 14, 18, 26, 30....$

# Part II

# Research Results: Perfect Sequences and Arrays

CHAPTER

# 6

# PERFECT SEQUENCES OF UNBOUNDED LENGTHS OVER THE BASIC QUATERNIONS

PERFECT sequences over the quaternion algebra $\mathbb{H}$ were first introduced by O. Kuznetsov in 2009 [45]. One year later, O. Kuznetsov and T. Hall showed a construction of a perfect sequence of length $5,354,228,880$ over a quaternion alphabet with 24 elements, namely the double-tetrahedron group $\mathbb{H}_{24} = \{\pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2}\} \subset \mathbb{H}$ [47]. Kuznetsov and Hall posed the conjecture: There are perfect sequences of unbounded lengths over the double-tetrahedron group $\mathbb{H}_{24}$. The author and Hall [10] worked on this conjecture and found a family of perfect sequences of **unbounded lengths** over $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, which is an alphabet more likely to be implemented in Electronic Communication, smaller than $\mathbb{H}_{24}$ and easier to handle. The author considers the proof of this conjecture is important, since all known constructions of perfect sequences over $n$-roots of unity, only produces sequences of lengths less or equal o $n^2$.

In our proof of Kuznetsov and Hall's conjecture, we show that Lee sequences, which are defined over the alphabet $\{0, 1, -1, i, -i\}$ [49], can always be converted, with perfection preserved, into sequences over the basic quaternions $\{1, -1, i, -i, j\} \subset \mathbb{H}_8$, where each element has magnitude one. More generally, we show that every sequence over the complex numbers, that is palindromic about one or two zero-centres, can be converted into a sequence over the quaternions $\mathbb{H}$, preserving its off-peak autocorrelation values. Then, we use the existence of Lee sequences of unbounded lengths [49], [54] to show the existence of sequences over the basic quaternions $\{1, -1, i, -i, j\} \subset \mathbb{H}$ of unbounded lengths.

## 6.1 Palindromic sequences about one and two centres

**Definition 6.1.** *Let* $\boldsymbol{S}$ *be a sequence of odd length* $m = 2n + 1$*, with* $n \in \mathbb{N}$*, over the alphabet of complex numbers* $\mathbb{C}$*. We say that* $\boldsymbol{S}$ *is palindromic about the centre* $a_n$*, if* $a_i = a_{2n-i}$*, for* $i = 0, \ldots, n-1$*. That is, reading the sequence from left to right is the same as reading it from right to left. Notice that the sequence* $\boldsymbol{S}$ *can always be rotated cyclically, so that the centre* $a_n$ *can be the first term of the sequence. The concept of being palindromic about one centre is equivalent to the concept of being symmetric. Further, we define any shift of a palindromic sequence to also be palindromic.*

**Example 6.1.** *The sequence* $(a, b, c, d, c, b, a)$ *is palindromic about the centre* $d$*. By the last sentence of Definition (6.1), each shift is also called palindromic, for example the sequence* $(b, a, a, b, c, d, c)$ *is palindromic with centre* $d$*.*

**Definition 6.2.** *Barrera and Hall [10].*

*Let $\boldsymbol{S}$ be a sequence of even length $m = 2n$, with $n \in \mathbb{N}$, over the alphabet of complex numbers $\mathbb{C}$. We say that $\boldsymbol{S}$ is palindromic about the centres $a_0$ and $a_n$, if $a_i = a_{2n-i}$, for $i = 1, \ldots, n-1$. That is, starting at either centre, reading the sequence from left to right is the same as reading it from right to left.*

**Example 6.2.** *The sequence $(a, b, c, d, e, d, c, b)$ is palindromic about the centres $a$ and $e$.*

**Lemma 6.1.** *For every complex number $z = a + ib \in \mathbb{C}$, we have that $jz^* + zj^* = 0$ and $kz^* + zk^* = 0$, where $j$ and $k$ are the quaternions $(0, 0, 1, 0)$ and $(0, 0, 0, 1)$, respectively.*

*Proof.* From $ij = k$, $ji = -k$ and $j^* = -j$, we have

$$\begin{aligned} jz^* + zj^* = \;& j(a+ib)^* + (a+ib)j^* \\ = \;& j(a-ib) + (a+ib)(-j) \\ & = aj - jib + a(-j) + i(-j)b \\ & = aj - jib - aj - ijb \\ & = aj + kb - aj - bk = 0. \end{aligned} \tag{6.1}$$

as required. A similar argument shows that $kz^* + zk^* = 0$. □

**Theorem 6.1.** *Let $\boldsymbol{S}$ be a sequence of even length $m = 2n$, with $n \in \mathbb{N}$, over the alphabet of complex numbers $\mathbb{C}$ and palindromic about the centres $a_0 = 0$ and $a_n$, say*

$$\boldsymbol{S} = (0, a_1, \ldots, a_{n-1}, a_n, a_{n-1}, \ldots, a_1). \tag{6.2}$$

*If the element $a_0 = 0$ is replaced by the basic quaternion $j$ in the sequence $\boldsymbol{S}$, then the right (left) off-peak autocorrelation values of the new sequence*

$$\boldsymbol{T} = (j, a_1, \ldots, a_{n-1}, a_n, a_{n-1}, \ldots, a_1), \tag{6.3}$$

*are the same as those of $\boldsymbol{S}$. Also, the right and left peak values $AC^R_{\boldsymbol{T}}(0)$ and $AC^L_{\boldsymbol{T}}(0)$ are* *equal to* $AC_{\boldsymbol{S}}(0)+1$.

*Proof.* Since the sequence $\boldsymbol{S}$ is palindromic, the products $a_0a_t^*$ and $a_ta_0^*$ are included in the summation that gives the right $t$-autocorrelation value of $\boldsymbol{S}$, for $1 \leq t \leq 2n-1$. Therefore, this autocorrelation value can be written with $a_0a_t^*$ and $a_ta_0^*$ isolated, as follows

$$AC_{\boldsymbol{S}}(t) = (a_0a_t^* + a_ta_0^*) + \sum_{l=0}^{2n-1} a_la_{l+t}^*, \tag{6.4}$$

where $a_0 = 0$. From Equation (6.4), since $a_0 = 0$, we deduce that

$$AC_{\boldsymbol{S}}(t) = \sum_{l\neq 0,t}^{2n-1} a_la_{l+t}^*. \tag{6.5}$$

We need to prove that the right (left) off-peak autocorrelation values of $\boldsymbol{T}$ are exactly the same as those of $\boldsymbol{S}$. Let $1 \leq t \leq 2n-1$. Since the sequence $\boldsymbol{T}$ is also palindromic, the products $ja_t^*$ and $a_tj^*$ contribute to the summation that gives the right $t$-autocorrelation value of $\boldsymbol{T}$. Hence, since $a_0 = j$ in $\boldsymbol{T}$, this autocorrelation value can be written as

$$AC_{\boldsymbol{T}}^R(t) = (ja_t^* + a_tj^*) + \sum_{l=0}^{2n-1} a_la_{l+t}^* = \sum_{l\neq 0,t}^{2n-1} a_la_{l+t}^*. \tag{6.6}$$

Now, $ja_t^* + a_tj^* = 0$, by Lemma (6.1), so from Equations (6.6) and (6.5), we have $AC_{\boldsymbol{T}}^R(t) = AC_{\boldsymbol{S}}(t)$, for $1 \leq t \leq 2n-1$, as required. A similar argument shows that $AC_{\boldsymbol{T}}^L(t) = AC_{\boldsymbol{S}}(t)$, for $1 \leq t \leq 2n-1$. An easy calculation shows that $AC_{\boldsymbol{T}}^R(0)$ and $AC_{\boldsymbol{T}}^L(0)$ are equal to $AC_{\boldsymbol{S}}(0) + jj^* = AC_{\boldsymbol{S}}(0)+1$. □

If the element $a_0 = 0$ in Theorem (6.1) is replaced by the basic quaternion $k$, then the theorem remains valid.

**Corollary 6.1.** *If the sequence $\boldsymbol{S}$ in Theorem (6.1) has perfect autocorrelation, then the sequence $\boldsymbol{T}$ also has perfect autocorrelation.*

**Example 6.3.** *Let $w = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$, a primitive third root of unity. The sequence (found by exhaustive computer search on the **Monash Sun Grid**)*

$$\begin{aligned}\boldsymbol{S} = (&0,1,w,w^2,w,1,1,w,1,w^2,w^2,1,1,w^2,w,w^2,w,w^2,w^2,w^2,w^2,w,w,w^2,w,w,\\ &1,1,w^2,w,w^2,w^2,w^2,w,w^2,1,1,w,w,w^2,w,w,w^2,w^2,w^2,w^2,w,w^2,w,w^2,1,1,w^2,\\ &w^2,1,w,1,1,w,w^2,w,1),\end{aligned} \tag{6.7}$$

*of length 62 and palindromic about $a_0 = 0$, has perfect autocorrelation and hence so does the sequence*

$$\begin{aligned}\boldsymbol{T} = (&j,1,w,w^2,w,1,1,w,1,w^2,w^2,1,1,w^2,w,w^2,w,w^2,w^2,w^2,w^2,w,w,w^2,w,w,\\ &1,1,w^2,w,w^2,w^2,w^2,w,w^2,1,1,w,w,w^2,w,w,w^2,w^2,w^2,w^2,w,w^2,w,w^2,1,1,w^2,\\ &w^2,1,w,1,1,w,w^2,w,1).\end{aligned} \tag{6.8}$$

**Theorem 6.2.** *Let $\boldsymbol{S}$ be a sequence of even length $m = 2n$, with $n \in \mathbb{N}$, over the alphabet of complex numbers $\mathbb{C}$ and palindromic about the centres $a_0 = 0$ and $a_n = 0$, say $\boldsymbol{S} = (0, a_1, \ldots, a_{n-1}, 0, a_{n-1}, \ldots, a_1)$. If the elements $a_0 = 0$ and $a_n = 0$, in the sequence $\boldsymbol{S}$, are replaced by the basic quaternions $j$ and $k$, respectively, then the right (left) off-peak autocorrelation values of the new sequence $\boldsymbol{T} = (j, a_1, \ldots, a_{n-1}, k, a_{n-1}, \ldots, a_1)$ are the same as the off-peak autocorrelation values of $\boldsymbol{S}$. Also, the right and left peak values $AC^R_{\boldsymbol{T}}(0)$ and $AC^L_{\boldsymbol{T}}(0)$ are equal to $AC_{\boldsymbol{S}}(0) + 2$.*

*Proof.* Let $1 \leq t \leq 2n - 1$.

1. Case $t \neq n$: Since the sequence $S$ is palindromic, the products $a_0 a_t^*$, $a_t a_0^*$, $a_n a_{t+n}^*$ and $a_{t+n} a_n^*$ contribute to the summation that gives the right $t$-autoco-

rrelation value of $\boldsymbol{S}$. Therefore, this autocorrelation value can be written as

$$AC_{\boldsymbol{S}}(t) = \sum_{l=0}^{2n-1} a_l a_{l+t}^* = (a_0 a_t^* + a_t a_0^* + a_n a_{t+n}^* + a_{t+n} a_n^*) + \sum_{l \neq 0,t,n,t+n}^{2n-1} a_l a_{l+t}^*, \tag{6.9}$$

where $a_0 = 0$ and $a_n = 0$. From Equation (6.9), since $a_0 = a_n = 0$, we deduce that

$$AC_{\boldsymbol{S}}(t) = \sum_{l \neq 0,t,n,t+n}^{2n-1} a_l a_{l+t}^*. \tag{6.10}$$

We need to prove now that the right (left) off-peak autocorrelation values of $\boldsymbol{T}$ are exactly the same as those of $\boldsymbol{S}$, for $t \neq n$. Since the sequence $\boldsymbol{T}$ is also palindromic, the products $ja_t^*$, $a_t j^*$, $ka_{t+n}^*$ and $a_{t+n}k^*$ contribute to the summation that gives the right $t$-autocorrelation value of $\boldsymbol{T}$. Hence, this autocorrelation value can be written as

$$AC_{\boldsymbol{T}}^R(t) = \sum_{l=0}^{2n-1} a_l a_{l+t}^* = (ja_t^* + a_t j^* + ka_{t+n}^* + a_{t+n}k^*) + \sum_{l \neq 0,t,n,t+n}^{2n-1} a_l a_{l+t}^*, \tag{6.11}$$

since, in $\boldsymbol{T}$, $a_0 = j$ and $a_n = k$. Now, since the expression $ja_t^* + a_t j^* + ka_{t+n}^* + a_{t+n}k^*$ is always zero by Lemma (6.1), then from Equation (6.10), we conclude that $AC_{\boldsymbol{T}}^R(t) = AC_{\boldsymbol{S}}(t)$, for $1 \leq t \leq 2n-1$ and $t \neq n$, as required. A similar argument shows that $AC_{\boldsymbol{T}}^L(t) = AC_{\boldsymbol{S}}(t)$, for $1 \leq t \leq 2n-1$ and $t \neq n$.

2. Case $t = n$: Since the sequence $\boldsymbol{S}$ is palindromic, the products $a_0 a_n^*$ and $a_n a_0^*$ contribute to the summation that gives the right $n$-autocorrelation value of $\boldsymbol{S}$. Therefore, this autocorrelation value can be written as

$$AC_{\boldsymbol{S}}(n) = \sum_{l=0}^{2n-1} a_l a_{l+n}^* = (a_0 a_n^* + a_n a_0^*) + \sum_{l \neq 0,n}^{2n-1} a_l a_{l+n}^*, \tag{6.12}$$

where $a_0 = 0$ and $a_n = 0$. From Equation (6.12), since $a_0 = a_n = 0$, we deduce that

$$AC_{\boldsymbol{S}}(t) = \sum_{l \neq 0,n}^{2n-1} a_l a_{l+t}^*. \tag{6.13}$$

We need to prove now that the right (left) off-peak autocorrelation values of $\boldsymbol{T}$ are exactly the same as those of $\boldsymbol{S}$, for $t = n$. Since the sequence $\boldsymbol{T}$ is also palindromic, the products $jk^*$ and $kj^*$ contribute to the summation that gives the right $n$-autocorrelation value of $\boldsymbol{T}$. Hence, this autocorrelation can be written as

$$AC_{\boldsymbol{T}}^R(t) = \sum_{l=0}^{2n-1} a_l a_{l+n}^* = (jk^* + kj^*) + \sum_{l \neq 0,n}^{2n-1} a_l a_{l+n}^*, \tag{6.14}$$

since, in $\boldsymbol{T}$, $a_0 = j$ and $a_n = k$. Now, since the expression $jk^* + kj^* = j(-k) + k(-j) = -i + i = 0$ and from Equation (6.13), we conclude that $AC_{\boldsymbol{T}}^R(t) = AC_{\boldsymbol{S}}(t)$, for $t = n$, as required. A similar argument shows that $AC_{\boldsymbol{T}}^L(t) = AC_{\boldsymbol{S}}(t)$, for $t = n$.

A simple computation of the peak autocorrelation value of $\boldsymbol{T}$ shows that $AC_{\boldsymbol{T}}^R(0)$ and $AC_{\boldsymbol{T}}^L(0)$ are equal to $AC_{\boldsymbol{S}} + jj^* + kk^* = AC_{\boldsymbol{S}}(0) + 2$. □

**Corollary 6.2.** *If the sequence* $\boldsymbol{S}$ *in Theorem (6.2) has perfect autocorrelation, then the sequence* $\boldsymbol{T}$ *also has perfect autocorrelation.*

**Example 6.4.** *The sequence* $\boldsymbol{S} = (0, i, 1, -i, -1, -i, 0, -i, -1, -i, 1, i)$*, palindromic about* $a_0 = 0$ *and* $a_6 = 0$*, has almost perfect autocorrelation* $AC_{\boldsymbol{S}} = (10, 0, 0, 0, 0, 0, -6, 0, 0, 0, 0, 0)$*. We modify the sequence* $\boldsymbol{S}$ *to produce the sequence* $\boldsymbol{T} = (j, i, 1, -i, -1, -i, k, - i, -1, -i, 1, i)$*, which also has almost perfect autocorrelation, namely* $AC_{\boldsymbol{T}} = (12, 0, 0, 0, 0, 0, -6, 0, 0, 0, 0, 0)$*. The author is not aware of any* ***perfect*** *sequences that satisfy the conditions of Theorem (6.2).*

**Theorem 6.3.** *Let $\boldsymbol{S}$ be a sequence of odd length $m = 2n + 1$, with $n \in \mathbb{N}$, over the alphabet of complex numbers $\mathbb{C}$ and palindromic about the centre $a_0 = 0$, say $\boldsymbol{S} = (0, a_1, \ldots, a_n, a_n, \ldots, a_1)$. If the element $a_0 = 0$ is replaced by the basic quaternion $j$ in the sequence $\boldsymbol{S}$, then the left (right) off-peak autocorrelation values of the new sequence $T = (j, a_1, \ldots, a_n, a_n, \ldots, a_1)$ are the same as the off-peak autocorrelation values of $\boldsymbol{S}$.*

We omit this proof since it is similar to the proof of Theorem (6.1).

**Corollary 6.3.** *If the sequence $\boldsymbol{S}$ in Theorem (6.3) has perfect autocorrelation, then the sequence $\boldsymbol{T}$ also has perfect autocorrelation.*

**Example 6.5.** *Let $w = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$, a primitive third root of unity. The sequence $\boldsymbol{S} = (0, 1, w, w, 1)$, of length 5 and palindromic about $a_0 = 0$, has perfect autocorrelation and so does the sequence $\boldsymbol{T} = (j, 1, w, w, 1)$.*

## 6.2 Perfect sequences over the basic quaternions of unbounded length

In this section, we answer the question: Are there perfect sequences over the double-tetrahedron group $\mathbb{H}_{24} = \{\pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2}\}$ for unbounded lengths? We will show that Lee Sequences can be transformed into sequences over the basic quaternions $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, preserving their properties, that is, preserving alternating, palindromic and perfection. Even more important, this shows that there exist perfect sequences of unbounded lengths over $\{1, -1, i, -i, j\} \subset \mathbb{H}_8$.

Let $S$ be a Lee sequence of even length $m = 2n$, with $n \in \mathbb{N}$, say

$$S = (0, a_1, a_2, \ldots, a_t, \ldots, a_{n-1}, a_n, a_{n-1}, \ldots, a_t, \ldots, a_2, a_1). \tag{6.15}$$

This sequence is palindromic about $a_0 = 0$ and $a_n$, has even length, is defined over the set $\{0, 1, -1, i, -i\} \subset \mathbb{C}$ and has perfect autocorrelation. If we replace the element $a_0 = 0$ by the basic quaternion $j$, then we get the new sequence

$$\boldsymbol{T} = (j, a_1, a_2, \ldots, a_t, \ldots, a_{n-1}, a_n, a_{n-1}, \ldots, a_t, \ldots, a_2, a_1), \tag{6.16}$$

which has perfect autocorrelation by Theorem (6.1). Notice that the sequence $\boldsymbol{T}$ is defined over the alphabet $\{1, -1, i, -i, j\} \subset \mathbb{H}_8$, is palindromic about $j$ and $a_n$, is alternating and has even length.

**Theorem 6.4** (Barrera and Hall [10])**.** . *There exist perfect sequences over the basic quaternions $\mathbb{H}_8$ of unbounded length. Specifically each Lee sequence yields a perfect sequence over $\mathbb{H}_8$, by the changing of* 0 *to $j$.*

*Proof.* From Section (5.2), we know that there exist Lee Sequences of unbounded lengths. Namely for $n = p^k + 1 \equiv 2 \ (mod\ 4)$, for $p$ prime and $k \in \mathbb{N}$. Each of these sequences can be converted into a sequence over the basic quaternions $\mathbb{H}_8$, by replacing 0 by the basic quaternion $j$ (or $k$) and preserving perfection, as in Theorem (6.1). □

**Example 6.6.** *To illustrate Theorem 6.4, we are taking a Lee sequence,*

$$\begin{aligned} \boldsymbol{S} = (&0, i, -1, i, 1, i, -1, i, -1, -i, 1, i, -1, -i, 1, i, -1, -i, 1, -i, 1, -i, -1, -i, -1, i, \\ &1, i, -1, -i, 1, -i, 1, i, 1, i, 1, -i, 1, i, -1, i, 1, -i, 1, -i, 1, -i, -1, -i, -1, i, 1, i, 1, i, 1, \\ &i, 1, i, -1, -i, -1, -i, 1, -i, 1, -i, 1, i, -1, i, 1, -i, 1, i, 1, i, 1, -i, 1, -i, -1, i, 1, i, -1, \\ &-i, -1, -i, 1, -i, 1, -i, -1, i, 1, -i, -1, i, 1, -i, -1, i, -1, i, 1, i, -1, i), \end{aligned} \tag{6.17}$$

*of length 110 over $\{0, 1, -1, i, -i\}$, and changing* 0 *to $j$. By Theorem (6.4), the new* *sequence*

$$\begin{aligned}\boldsymbol{T} = (&j, i, -1, i, 1, i, -1, i, -1, -i, 1, i, -1, -i, 1, i, -1, -i, 1, -i, 1, -i, -1, -i, -1, i,\\ &1, i, -1, -i, 1, -i, 1, i, 1, i, 1, -i, 1, i, -1, i, 1, -i, 1, -i, 1, -i, -1, -i, -1, i, 1, i, 1, i, 1,\\ &i, 1, i, -1, -i, -1, -i, 1, -i, 1, -i, 1, i, -1, i, 1, -i, 1, i, 1, i, 1, -i, 1, -i, -1, i, 1, i, -1,\\ &-i, -1, -i, 1, -i, 1, -i, -1, i, 1, -i, -1, i, 1, -i, -1, i, -1, i, 1, i, -1, i),\end{aligned} \tag{6.18}$$

*is perfect.*

The **High Energy Efficiency** of the modified sequence in Theorem (6.4) is given by

$$E = \frac{\sum_{l=0}^{n-1} \|a_l\|^2}{n(max\{\|a_l\|\})} = 1, \tag{6.19}$$

since every entry in the sequence $\boldsymbol{T}$ has modulus 1, following the substitution of 0 by $j$.

## 6.3 Palindromic sequences about one and two centres: General Case

In the Theorems (6.1), (6.2) and (6.3), we showed that palindromic sequences about one or two zero centres, over the complex numbers, can be transformed into sequences over quaternions, preserving the off-peak autocorrelation values. In this section, we generalise Theorems (6.1) and (6.2), by considering sequences over quaternions of the form $q = a + ib + jc$ and by showing that these sequences are also transformed into sequences over general quaternions, preserving the off-peak autocorrelation values.

**Lemma 6.2.** *For every quaternion number of the form $q = a + ib + jc \in \mathbb{H}$, we have that $kq^* + qk^* = 0$.*

*Proof.* From $ik = -j$, $ki = j$, $jk = i$ and $kj = -i$, we have

$$\begin{aligned} kq^* + qk^* &= k(a + ib + jc)^* + (a + ib + jc)k^* \\ &= k(a - ib - jc) + (a + ib + jc)(-k) \\ &= ak - jb + ic - ak + jb - ic = 0. \end{aligned}$$

as required. □

**Theorem 6.5.** *Let* $\boldsymbol{S}$ *be a sequence of even length* $m = 2n$*, with* $n \in \mathbb{N}$*, over the alphabet* $\{a + ib + jc \mid a, b, c \in \mathbb{R}\}$ *and palindromic about the centres* $s_0 = a_0 + b_0 i + c_0 j$ *and* $s_n$*, say* $\boldsymbol{S} = (s_0, s_1, \ldots, s_{n-1}, s_n, s_{n-1}, \ldots, s_1)$*. If the element* $s_0$ *is replaced by the quaternion* $s_0 + d_0 k$*, with* $d_0 \in \mathbb{R}$*, in the sequence* $\boldsymbol{S}$*, then the right (left) off-peak autocorrelation values of the new sequence* $\boldsymbol{T} = (s_0 + d_0 k, s_1, \ldots, s_{n-1}, s_n, s_{n-1}, \ldots, s_1)$ *are the same as those of* $\boldsymbol{S}$*. Also, the right and left peak values* $AC^R_{\boldsymbol{T}}(0)$ *and* $AC^L_{\boldsymbol{T}}(0)$ *are equal to* $AC_{\boldsymbol{S}}(0) + d_0^2$*.*

*Proof.* Since the sequence $\boldsymbol{S}$ is palindromic, the products $(a_0 + b_0 i + c_0 j)s_t^*$ and $s_t(a_0 + b_0 i + c_0 j)^*$ contribute to the summation that gives the right $t$-autocorrelation value of $\boldsymbol{S}$, for $1 \le t \le 2n - 1$. Therefore, this autocorrelation value can be written as

$$AC_{\boldsymbol{S}}(t) = [(a_0 + b_0 i + c_0 j)s_t^* + s_t(a_0 + b_0 i + c_0 j)^*] + \sum_{l=0}^{2n-1} a_l a_{l+t}^* = \sum_{l \neq 0, t}^{2n-1} a_l a_{l+t}^*. \tag{6.20}$$

We need to prove that the right (left) off-peak autocorrelation values of $\boldsymbol{T}$ are exactly the same as those of $\boldsymbol{S}$. Let $1 \le t \le 2n - 1$. Since the sequence $\boldsymbol{T}$ is also palindromic, the products $(a_0 + b_0 i + c_0 j + d_0 k)s_t^*$ and $s_t(a_0 + b_0 i + c_0 j + d_0 k)^*$ contribute to the summation that gives the right $t$-autocorrelation value of $\boldsymbol{T}$. Hence, this autocorrelation value can be written as

$$\begin{aligned}
&AC^R_{\boldsymbol{T}}(t) = \\
&\textstyle\sum_{l=0}^{2n-1} s_l s^*_{l+t} = \\
&(a_0 + b_0 i + c_0 j + d_0 k)s^*_t + s_t(a_0 + b_0 i + c_0 j + d_0 k)^* + \textstyle\sum_{l\neq 0,t}^{2n-1} s_l s^*_{l+t} = \\
&[(a_0 + b_0 i + c_0 j)s^*_t + s_t(a_0 + b_0 i + c_0 j)^*] + [(d_0 k)s^*_t + s_t(d_0 k)^*] + \textstyle\sum_{l\neq 0,t}^{2n-1} s_l s^*_{l+t} = \\
&[(d_0 k)s^*_t + s_t(d_0 k)^*] + \Big([(a_0 + b_0 i + c_0 j)s^*_t + s_t(a_0 + b_0 i + c_0 j)^*] + \textstyle\sum_{l\neq 0,t}^{2n-1} s_l s^*_{l+t}\Big) = \\
&(d_0 k)s^*_t + s_t(d_0 k)^* + AC^R_{\boldsymbol{S}}(t).
\end{aligned} \tag{6.21}$$

Now, since the expression $ks^*_t + s_t k^*$ is always zero by Lemma (6.2), we conclude that $AC^R_{\boldsymbol{T}}(t) = AC_{\boldsymbol{S}}(t)$, for $1 \leq t \leq 2n-1$, as required. A similar argument shows that $AC^L_{\boldsymbol{T}}(t) = AC_{\boldsymbol{S}}(t)$, for $1 \leq t \leq 2n-1$. An easy calculation shows that $AC^R_{\boldsymbol{T}}(0)$ and $AC^L_{\boldsymbol{T}}(0)$ are equal to $AC_{\boldsymbol{S}}(0) + d_0^2$. □

**Corollary 6.4.** *Let* $\boldsymbol{S}$ *be a sequence of even length* $m = 2n$, *with* $n \in \mathbb{N}$, *over the alphabet of complex numbers* $\mathbb{C}$ *and palindromic about the centres* $s_0 = a_0 + b_0 i$ *and* $s_n$, *say* $\boldsymbol{S} = (s_0, s_1, \ldots, s_{n-1}, s_n, s_{n-1}, \ldots, s_1)$. *If the element* $s_0$ *is replaced by the quaternion* $s_0 + c_0 j + d_0 k$, *with* $c_0, d_0 \in \mathbb{R}$, *in the sequence* $\boldsymbol{S}$, *then the right (left) off-peak autocorrelation values of the new sequence* $\boldsymbol{T} = (s_0 + c_0 j + d_0 k, s_1, \ldots, s_{n-1}, s_n, s_{n-1}, \ldots, s_1)$ *are the same as those of* $\boldsymbol{S}$, *and the right and left peak values* $AC^R_{\boldsymbol{T}}(0)$ *and* $AC^L_{\boldsymbol{T}}(0)$ *are equal to* $AC_{\boldsymbol{S}}(0) + c_0^2 + d_0^2$. *Also,* $s_0$ *could be replaced by the quaternion* $s_0 + c_0 j$ *and* $s_n$ *by* $s_n + d_n k$, *in the sequence* $\boldsymbol{S}$, *and then the right (left) off-peak autocorrelation values of the new sequence* $\boldsymbol{U} = (s_0 + c_0 j, s_1, \ldots, s_{n-1}, s_n + d_n k, s_{n-1}, \ldots, s_1)$ *are the same as those of* $\boldsymbol{S}$, *and the right and left peak values* $AC^R_{\boldsymbol{U}}(0)$ *and* $AC^L_{\boldsymbol{U}}(0)$ *are equal to* $AC_{\boldsymbol{S}}(0) + c_0^2 + d_n^2$.

**Theorem 6.6.** *Let* $\boldsymbol{S}$ *be a sequence of odd length* $m = 2n+1$, *with* $n \in \mathbb{N}$, *over the alphabet* $\{a + ib + jc \mid a, b, c \in \mathbb{R}\}$ *and palindromic about the centre* $s_0 = a_0 + b_0 i + c_0 j$, *say* $\boldsymbol{S} = (s_0, s_1, \ldots, s_n, s_n, \ldots, s_1)$. *If the element* $s_0$ *is replaced, in the sequence* $\boldsymbol{S}$, *by the quaternion* $s_0 + d_0 k$, *with* $d_0 \in \mathbb{R}$, *then the right (left) off-peak autocorrelation values of the new sequence* $\boldsymbol{T} = (s_0 + d_0 k, s_1, \ldots, s_n, s_n, \ldots, s_1)$ *are the same as those of* $\boldsymbol{S}$. *Also,* *the right and left peak values* $AC^R_{\boldsymbol{T}}(0)$ *and* $AC^L_{\boldsymbol{T}}(0)$ *are equal to* $AC_{\boldsymbol{S}}(0) + d_0^2$.

A proof of Theorem (6.6) is entirely similar to the proof of Theorem (6.5).

**Corollary 6.5.** *If the sequence* **S** *in Theorems (6.5) and (6.6) has perfect (almost perfect) autocorrelation, then the sequence* **T** *also has perfect (almost perfect) autocorrelation.*

**Example 6.7.** *The sequence* $\boldsymbol{S} = (-1 + j, 1 - i, 1 + i, 1 + i, 1 - i)$ *has autocorrelation* $(10, 0, 0, 0, 0)$ *and so the sequence* $\boldsymbol{T} = (-1 + j + k, 1 - i, 1 + i, 1 + i, 1 - i)$ *has autocorrelation* $(11, 0, 0, 0, 0)$.

CHAPTER

# 7

# PERFECT SEQUENCES OF ODD UNBOUNDED LENGTHS OVER THE QUATERNIONS

IN his Ph.D. thesis, *Perfect Sequences over the Real Quaternions*, Kuznetsov presented a result that states that given a perfect sequence $S$ of length $n = n_1 n_2$, over the real quaternions, the sequence of balances of decimations

$$\left( \sum_{t=0}^{n_1-1} s_{tn_2}, \sum_{t=0}^{n_1-1} s_{1+tn_2}, \sum_{t=0}^{n_1-1} s_{2+tn_2}, \ldots, \sum_{t=0}^{n_1-1} s_{n_2-1+tn_2} \right) \tag{7.1}$$

is also perfect [46]. This result allows us to construct new families of perfect sequences over the alphabets $G = \{\pm 1 \pm i, i\}$, $U_4^* = \{\pm 1, \pm i, \frac{1 \pm i}{2}\}$ and $T = \{\pm 1 \pm i, 1 \pm j\}$, from existing families of perfect sequences over alphabets of complex numbers and quaternion.

## 7.1 Perfection of a sequence of balances of decimations of a perfect sequence

For the sake of understanding Theorem (7.1), due to Kuznetsov, we give the following example. Let $S = (a_0, a_1, a_2, a_3, a_4, a_5)$ be a perfect sequence, over any quaternion alphabet, of length $6 = 2 \times 3$. From the sequence $S$ we can produce two new sequences of lengths 2 and 3 as follows

$$\begin{aligned} S_1 &= (a_0 + a_2 + a_4, a_1 + a_3 + a_5). \\ S_2 &= (a_0 + a_3, a_1 + a_4, a_2 + a_5). \end{aligned} \tag{7.2}$$

Our claim is that the sequences $S_1$ and $S_2$ are perfect. We show that the off-peak autocorrelation values of $S_1$ and $S_2$, shown below, are sums of some off-peak autocorrelation values of $S$.

1. Autocorrelation values of $S_1$

$$\begin{aligned} AC^R S_1(0) = &\quad (a_0 + a_2 + a_4)(a_0 + a_2 + a_4)^* + (a_1 + a_3 + a_5)(a_1 + a_3 + a_5)^* \\ = &\quad a_0 a_0^* + a_1 a_1^* + a_2 a_2^* + a_3 a_3^* + a_4 a_4^* + a_5 a_5^* \\ = &\quad AC^R S(0). \end{aligned} \tag{7.3}$$

$$\begin{aligned}
AC^R\boldsymbol{S}_1(1) = &\quad (a_0+a_2+a_4)(a_1+a_3+a_5)^* + (a_1+a_3+a_5)(a_0+a_2+a_4)^* \\
= &\quad a_0a_1^* + a_0a_3^* + a_0a_5^* + a_2a_1^* + a_2a_3^* + a_2a_5^* + a_4a_1^* + a_4a_3^* + a_4a_5^* + \\
&\quad a_1a_0^* + a_1a_2^* + a_1a_4^* + a_3a_0^* + a_3a_2^* + a_3a_4^* + a_5a_0^* + a_5a_2^* + a_5a_4^* \\
= &\quad a_0a_1^* + a_1a_2^* + a_2a_3^* + a_3a_4^* + a_4a_5^* + a_5a_0^* + \\
&\quad a_0a_3^* + a_1a_4^* + a_2a_5^* + a_3a_0^* + a_4a_1^* + a_5a_2^* + \\
&\quad a_0a_5^* + a_1a_0^* + a_2a_1^* + a_3a_2^* + a_4a_3^* + a_5a_4^* \\
= &\quad AC_{\boldsymbol{S}}(1) + AC_{\boldsymbol{S}}(3) + AC_{\boldsymbol{S}}(5) = 0.
\end{aligned} \tag{7.4}$$

2. Autocorrelation values of $\boldsymbol{S}_2$

$$\begin{aligned}
AC^R_{\boldsymbol{S}_2}(0) = &\quad (a_0+a_3)(a_0+a_3)^* + (a_1+a_4)(a_1+a_4)^* + (a_2+a_5)(a_2+a_5)^* \\
= &\quad a_0a_0^* + a_1a_1^* + a_2a_2^* + a_3a_3^* + a_4a_4^* + a_5a_5^* \\
= &\quad AC^R_{\boldsymbol{S}}(0).
\end{aligned} \tag{7.5}$$

$$\begin{aligned}
AC^R_{\boldsymbol{S}_2}(1) = &\quad (a_0+a_3)(a_1+a_4)^* + (a_1+a_4)(a_2+a_5)^* + (a_2+a_5)(a_0+a_3)^* \\
= &\quad a_0a_1^* + a_0a_4^* + a_3a_1^*a_3a_4^* + a_1a_2^* + a_1a_5^* + a_4a_2^* + a_4a_5^* + \\
&\quad a_2a_0^* + a_2a_3^* + a_5a_0^* + a_5a_3 \\
= &\quad a_0a_1^* + a_1a_2^* + a_2a_3^* + a_3a_4^* + a_4a_5^* + a_5a_0^* + \\
&\quad a_0a_4^* + a_1a_5^* + a_2a_0^* + a_3a_1^* + a_4a_2^* + a_5a_3^* \\
= &\quad AC^R_{\boldsymbol{S}}(1) + AC^R_{\boldsymbol{S}}(4) = 0.
\end{aligned} \tag{7.6}$$

$$\begin{aligned}AC^R_{S_2}(2) = \;& (a_0+a_3)(a_2+a_5)^* + (a_1+a_4)(a_0+a_3)^* + (a_2+a_5)(a_1+a_4)^* \\ = \;& a_0a_2^* + a_0a_5^* + a_3a_2^*a_3a_5^* + a_1a_0^* + a_1a_3^* + a_4a_0^* + a_4a_3^* + \\ & a_2a_1^* + a_2a_4^* + a_5a_1^* + a_5a_4 \\ = \;& a_0a_2^* + a_1a_3^* + a_2a_4^* + a_3a_5^* + a_4a_0^* + a_5a_1^* + \\ & a_0a_5^* + a_1a_0^* + a_2a_1^* + a_3a_2^* + a_4a_3^* + a_5a_4^* \\ = \;& AC^R_S(2) + AC^R_S(5) = 0.\end{aligned} \tag{7.7}$$

We now give the general Theorem of Kuznetsov.

**Theorem 7.1** (Kuznetsov). *Let $S = (s_0, \ldots, s_{n-1})$ be a perfect sequence over any alphabet of complex numbers, and let $n_1$ and $n_2$ two integers such that $n_1, n_2 \geq 2$ and $n = n_1n_2$. The sequence*

$$\left(\sum_{t=0}^{n_1-1} s_{tn_2}, \sum_{t=0}^{n_1-1} s_{1+tn_2}, \sum_{t=0}^{n_1-1} s_{2+tn_2}, \ldots, \sum_{t=0}^{n_1-1} s_{n_2-1+tn_2}\right), \tag{7.8}$$

*of length $n_2$ is perfect.*

Theorem (7.1), applied to perfect sequences over the $n$-th roots of unity gives shorter sequences. But for a family of sequences of unbounded lengths, Theorem (7.1) will give us, again, a family of sequences of unbounded lengths. And these new families can be previously unknown families, as we show in Sections (7.2), (7.3) and (7.4).

For example, reducing each length by half, of a family of infinitely many perfect sequences, produces an infinite family of perfect sequences with different lengths, over a new (or equal) alphabet. It is convenient that the family of perfect sequences to be length-reduced should produce a new family of perfect sequences with a small and manageable alphabet (for example Lee sequences halve to odd length perfect sequences), as we will see in the following sections.

Henceforth, we will denote by $U_4$, $U_4^*$, $G$ and $T$, the following alphabets $\{\pm 1, \pm i\}$, $\{\pm 1, \pm i, \frac{1+i}{2}\}$, $\{\pm 1 \pm i, i\}$ and $\{\pm 1 \pm i, 1 \pm j\}$, respectively.

From Lee sequences, Theorem (7.1) will provide two new families of perfect sequences of odd unbounded lengths over the alphabets $G$ and $U_4^*$.

## 7.2 Perfect sequences of odd unbounded lengths over $G$

**Definition 7.1.** *For every natural number n, we define the **QAM alphabet** [18] as*

$$\phi_{n^2} = \{a + ib : \\ (a,b) \in \{-2n+1, -2n+3, \ldots, 2n-1\} \times \{-2n+1, -2n+3, \ldots, 2n-1\}\}. \tag{7.9}$$

*The alphabet $\phi_1 \cup U_4 = \{1, -1, i, -i, 1+i, 1-i, -1+i, -1-i\}$ is called a **two shell constellation**, in the sense of [18]. Sequences with good autocorrelation and energy have been constructed over the alphabets $\phi_{n^2}$, $\phi_{n^2} \cup \{0\}$ and $\phi_1 \cup U_4$ (see Boztas [18] and Garg et al [34]).*

The constructions presented in the rest of this chapter, are motivated by Theorem (7.1). The alphabet $G$, that arises in the next construction, is a subset of the QAM alphabet. The QAM alphabet has applications in electronic communication (see Boztas and Parampalli [19]).

We now present a construction of perfect sequences of odd unbounded lengths over the alphabet $G = \{\pm 1 \pm i, i\}$. From Section (5.1), we know that Lee Sequences have lengths divisible by two but not by four. Let $\boldsymbol{S}$ be a Lee sequence of length $m = 2n$, with $n$ an odd number, say

$$S = (0, s_1, s_2, \dots, s_t, \dots, s_{n-1}, s_n, s_{n-1}, \dots, s_t, \dots, s_2, s_1). \tag{7.10}$$

By Property (4) in Section (5.1), after multiplying the sequence $S$ by the constant $i$, if necessary, we can assume without loss of generality, that the Lee sequence has the form $(0, \pm i, \pm 1, \dots)$. Moreover, if the entry $s_n$ in the sequence $S$, is the complex number $-i$, then we can multiply the whole sequence $S$ by $-1$, without altering perfection, so that the sequence $S$ has the form $(0, \pm i, \pm 1, \dots, i, \dots, \pm 1, \pm i)$, if the sequence is not already of that form.

Now, for $n_1 = 2$ and $n_2 = n$, Theorem (7.1) gives the new sequence

$$T = (i, \pm 1 \pm i, \pm 1 \pm i, \dots, \pm 1 \pm i, \pm 1 \pm i), \tag{7.11}$$

of odd length $n$, with perfect autocorrelation. Notice that the first entry of $T$ is the complex number $i$ and the rest of the entries vary in the set $\{1+i, 1-i, -1+i, -1-i\}$, which is a subset of the Gaussian Integers $\mathbb{Z}[i] = \{a + ib | a, b \in \mathbb{Z}\}$ and the constellation $\phi_1 \cup U_4$.

**Theorem 7.2.** *There exist perfect sequences of odd unbounded lengths over the alphabet* $G = \{\pm 1 \pm i, i\}$.

*Proof.* From Theorem (5.2), we know that there exist Lee sequences of unbounded lengths, namely, for $n = p^a + 1 \equiv 2 \ mod(4)$, for $p$ prime and $a \in \mathbb{N}$. These sequences have even length, say $m = 2n$, with $n$ an odd number. Each Lee sequence can be converted into a new sequence of odd length $n$ over $G = \{\pm 1 \pm i, i\}$, preserving perfection, from Theorem (7.1). □

**Example 7.1.** *Given the 38-length Lee sequence*

$$(0,i,1,i,1,i,-1,-i,1,-i,-1,-i,1,i,1,-i,1,-i,-1,i,-1,-i,1,-i,1,i,1,-i,-1,\\ -i,1,-i,-1,i,1,i,1,i), \tag{7.12}$$

*we reduce it to half-length by Theorem (7.1), and obtain the new perfect sequence of length 19*

$$(i,-1+i,1-i,1+i,1-i,1+i,-1+i,1-i,1-i,-1-i,-1-i,1-i,1-i,\\ -1+i,1+i,1-i,1+i,1-i,-1+i). \tag{7.13}$$

## 7.3 Perfect sequences of odd unbounded lengths over $U_4^*$

Perfect sequences over the alphabet $G=\{\pm 1\pm i,i\}$ can be transformed into perfect sequences over the alphabet $U_4^*=\{\pm 1,\pm i,\frac{1+i}{2}\}$ as follows: take the sequence $\boldsymbol{T}$ in Equation (7.11), and multiply this sequence by $\frac{1}{1+i}$, this operation preserves perfection, according to Theorem (3.1). And so, we get the new sequence

$$\boldsymbol{V}=\left(\frac{1+i}{2},v_1,\ldots,v_n,\ldots,v_1\right), \tag{7.14}$$

where $v_i\in\{1,-1,i,-i\}$, for $1\leq i\leq n$.

**Theorem 7.3.** *There exist perfect sequences of odd unbounded lengths over the alphabet $U_4^*=\{\pm 1,\pm i,\frac{1+i}{2}\}$, with a single occurrence of the element $\frac{1+i}{2}$.*

*Proof.* By Theorem (7.1), each Lee sequence can be converted into a new sequence of odd length $n$ over $G = \{\pm 1 \pm i, i\}$. Each of these new sequences is then multiplied by the scalar $\frac{1}{1+i}$ and converted into a sequence over $U_4^* = \{\pm 1, \pm i, \frac{1+i}{2}\}$, preserving perfection according to Theorem (3.1), and with a single occurrence of the element $\frac{1+i}{2}$ □

**Example 7.2.** *The Lee sequence*

$$(0, i, 1, i, 1, i, -1, -i, 1, -i, -1, -i, 1, i, 1, -i, 1, -i, -1, i, -1, -i, 1, -i, 1, i, 1, -i, -1, \\ -i, 1, -i, -1, i, 1, i, 1, i), \tag{7.15}$$

*in Example (7.1), is transformed into the perfect sequence*

$$\left(\frac{1+i}{2}, i, -i, 1, -i, 1, i, -i, -i, -1, -1, -i, -i, i, 1, -i, 1, -i, i\right), \tag{7.16}$$

*of length 19, over the alphabet $U_4^* = \{\pm 1, \pm i, \frac{1+i}{2}\}$.*

The Balance Theorem (3.3) gives a necessary condition for perfection of a sequence $S$ over $\{\pm 1, \pm i\}$, namely, the sequence $S$ has to have even length. This condition implies that there are no perfect sequences of odd length over the alphabet $\{\pm 1, \pm i\}$. Introducing the element $\frac{1+i}{2}$ to the alphabet $\{\pm 1, \pm i\}$ allows us to have perfect sequences of odd length over $\{\pm 1, \pm i, \frac{1+i}{2}\}$, which is an alphabet close to $\{\pm 1, \pm i\}$. Now, since the alphabet $\{\pm 1 \pm i\}$ can be generated from $\{\pm 1, \pm i\}$ by multiplying the elements by $1 + i$, we can conclude by the Balance Theorem that there are no perfect sequences of odd length over $\{\pm 1 \pm i\}$. In the same way, introducing the element $i$ to the alphabet $\{\pm 1 \pm i\}$, allows us to have perfect sequences of odd length over the alphabet $\{\pm 1 \pm i, i\}$, which is an alphabet close to $\{\pm 1 \pm i\}$.

## 7.4 Perfect sequences of odd unbounded lengths over $T$

From Theorem (7.1), we produce a new family of perfect sequences of odd unbounded lengths over the set $T = \{\pm 1 \pm i, 1+j\}$, when applied to modified Lee sequences (in the sense of Barrera and Hall [10]).

From Theorem (6.4), we know there exist infinitely many sequences, over the basic quaternions $\{\pm 1, \pm i, \pm j, \pm k\}$, of the form

$$\boldsymbol{S} = (j, s_1, s_2, \ldots, s_t, \ldots, s_{n-1}, s_n, s_{n-1}, \ldots, s_t, \ldots, s_2, s_1), \tag{7.17}$$

where $s_t \in \{\pm 1, \pm i\}$, for $1 \leq t \leq n$. As we explained in Section (7.2), we can always assume, without loss of generality, the value $s_n$ is 1. Then, Equation (7.17) takes the following form

$$\boldsymbol{S} = (j, s_1, s_2, \ldots, s_t, \ldots, s_{n-1}, 1, s_{n-1}, \ldots, s_t, \ldots, s_2, s_1), \tag{7.18}$$

where $s_{2t-1} \in \{i, -i\}$, for $1 \leq t \leq \frac{n+1}{2}$ and $s_{2t} \in \{1, -1\}$, for $1 \leq t \leq \frac{n-1}{2}$. By Theorem (7.1), we reduce the sequence $\boldsymbol{S}$ into an odd-length perfect sequence, namely

$$\boldsymbol{U} = (1+j, u_1, u_2, \ldots, u_t, \ldots, u_{n-1}), \tag{7.19}$$

where $u_t \in \{1+i, 1-i, -1+i, -1-i\}$. Therefore, we have the following theorem.

**Theorem 7.4.** *There exist perfect sequences of odd unbounded lengths over the alphabet* $T = \{\pm 1 \pm i, 1+j\} \subset \{\pm 1 \pm i, \pm 1 \pm j, \pm 1 \pm k\}$.

**Example 7.3.** *The perfect sequence over the basic quaternions* $\{\pm 1, \pm i, j\} \subset \{\pm 1, \pm i,$

$\pm j, \pm k\}$.

$$(j, 1, -i, 1, i, -1, -i, -1, -i, 1, -i, -1, -i, -1, i, 1, -i, 1), \tag{7.20}$$

*is converted into the perfect sequence of odd length over the alphabet T*

$$(1 + j, 1 - i, -1 - i, 1 - i, -1 + i, -1 + i, 1 - i, -1 - i, 1 - i). \tag{7.21}$$

CHAPTER

# 8

# INFLATION AND SIZE REDUCTION OF PERFECT ARRAYS OVER THE BASIC QUATERNIONS

IN this chapter, we first explain, in a **matrix** approach rather than a polynomial approach, Arasu and de Launey's algorithm to inflate perfect quaternary arrays [4], into perfect quaternary arrays of larger sizes. Then, we produce a modification of Arasu and de Launey's algorithm, which we use to inflate perfect arrays over the basic quaternions $\{1, -1, i, -i, j, -j, k, -k\}$, preserving perfection. This result is then used in the next Chapter to show the existence of perfect arrays of unbounded sizes over the basic quaternions $\{1, -1, i, -i, j, -j, k, -k\}$.

In this Chapter, we also generalise the concept "Sequence of Balances of Decimations of a Perfect Sequence", to arrays of dimension two. We call this generalised process "Size Reduction of Perfect Arrays", and we prove size reduction of a perfect array is a left inverse process of inflating a perfect array, that is, inflating a perfect array and then reducing the size of this new array, gives back the initial one, up to multiplication by a constant.

## 8.1 Perfect arrays over the quaternion algebra

**Definition 8.1.** *Right and left periodic cross-correlation of arrays.*
*Let $\boldsymbol{A} = (a(r,s))$ and $\boldsymbol{B} = (b(r,s))$ be two arrays of size $m \times n$ over an arbitrary quaternion alphabet. For any pair of integers $(u,v)$, the $(u,v)$-**right** and **left periodic cross-correlation** values of $\boldsymbol{A}$ and $\boldsymbol{B}$ are*

$$CC^R_{\boldsymbol{A},\boldsymbol{B}}(u,v) = \sum_{r=0}^{m-1}\sum_{s=0}^{n-1} a(r,s)b^*(r+u,s+v), \tag{8.1}$$

*and*

$$CC^L_{\boldsymbol{A},\boldsymbol{B}}(u,v) = \sum_{r=0}^{m-1}\sum_{s=0}^{n-1} a^*(r,s)b(r+u,s+v), \tag{8.2}$$

*respectively. The indices $r+u$ and $s+v$ are calculated modulo $m$ and $n$, respectively. When $\boldsymbol{A} = \boldsymbol{B}$, we denote $CC^R_{\boldsymbol{A},\boldsymbol{B}}(u,v)$ and $CC^L_{\boldsymbol{A},\boldsymbol{B}}(u,v)$ by $AC^R_{\boldsymbol{A},\boldsymbol{B}}(u,v)$ and $AC^L_{\boldsymbol{A},\boldsymbol{B}}(u,v)$, respectively, and they are called the $(u,v)$-**right** and **left periodic autocorrelation** values of $\boldsymbol{A}$.*

*Also, as usual, the autocorrelation value of $\boldsymbol{A}$, for the shift $(0,0)$, is called the **peak value**. The right and left autocorrelation values of $S$, for all pairs $(u,v) \neq (0,0)$, are called **right and left off-peak values**.*

**Definition 8.2.** *Perfect arrays.*

*An array $\boldsymbol{A} = (a(r,s))$ of size $m \times n$ over an arbitrary quaternion alphabet is called* ***right (left) perfect****, if all the right (or left) periodic autocorrelation values are equal to zero, for all $(u,v) \neq (0,0)$.*

**Example 8.1.** *Below, we present a perfect array over the basic quaternions of size $4 \times 4$.*

$$\begin{pmatrix} 1 & -i & 1 & -i \\ -j & k & j & -k \\ 1 & i & 1 & i \\ -j & -k & j & k \end{pmatrix} \tag{8.3}$$

Kuznetsov has proved an important property of perfect sequences over the real quaternions, that is, the right perfection of any sequences is equivalent to the left perfection [45]. In the next theorem we prove the corresponding statement for arrays of dimension two. In preparation for this theorem, we present the following lemma, concerning the sum of the norms of the autocorrelation values of any array over $\mathbb{H}$, namely $\sum_{u=0}^{m-1}\sum_{v=0}^{n-1}\|AC_{\boldsymbol{A}}^{L}(u,v)\|$ and $\sum_{u=0}^{m-1}\sum_{v=0}^{n-1}\|AC_{\boldsymbol{A}}^{R}(u,v)\|$.

**Lemma 8.1.** *Let $\boldsymbol{A} = (a(r,s))$ be any two-dimensional array of size $m \times n$, with elements in the quaternion algebra $\mathbb{H}$ and let $AC_{\boldsymbol{A}}^{R}(u,v) = \sum_{r=0}^{m-1}\sum_{s=0}^{n-1} a_{r,s}a_{r+u,s+v}^{*}$ and $AC_{\boldsymbol{A}}^{L} = \sum_{t=0}^{m-1}\sum_{s=0}^{n-1} a_{r,s}^{*}a_{r+u,s+v}$ be the right and left autocorrelation functions of the array $\boldsymbol{A}$, respectively. Then*

$$\sum_{u=0}^{m-1}\sum_{v=0}^{n-1}\|AC_{\boldsymbol{A}}^{L}(u,v)\| = \sum_{t_1=0}^{m-1}\sum_{t_2=0}^{m-1}\sum_{s_1=0}^{n-1}\sum_{s_2=0}^{n-1} a_{t_1,s_1}^{*}\left(AC_{\boldsymbol{A}}^{R}\left(t_2-t_1,s_2-s_1\right)\right)a_{t_2,s_2}\,, \tag{8.4}$$

*and*

$$\sum_{u=0}^{m-1}\sum_{v=0}^{n-1}\|AC_{\boldsymbol{A}}^{R}(u,v)\| = \sum_{t_1=0}^{m-1}\sum_{t_2=0}^{m-1}\sum_{s_1=0}^{n-1}\sum_{s_2=0}^{n-1} a_{t_1,s_1}\left(AC_{\boldsymbol{A}}^{L}\left(t_2-t_1,s_2-s_1\right)\right)a_{t_2,s_2}^{*}. \tag{8.5}$$

*Proof.*

$$
\begin{aligned}
&\sum_{u=0}^{m-1}\sum_{v=0}^{n-1} \|AC_{\boldsymbol{A}}^{L}(u,v)\| = \\
&\sum_{u=0}^{m-1}\sum_{v=0}^{n-1} \| \sum_{t=0}^{m-1}\sum_{s=0}^{n-1} a_{t,s}^{*}a_{t+u,s+v} \| = \\
&\sum_{u=0}^{m-1}\sum_{v=0}^{n-1} \left( \sum_{t_1=0}^{m-1}\sum_{s_1=0}^{n-1} a_{t_1,s_1}^{*}a_{t_1+u,s_1+v} \right) \left( \sum_{t_2=0}^{m-1}\sum_{s_2=0}^{n-1} a_{t_2,s_2}^{*}a_{t_2+u,s_2+v} \right)^{*} = \\
&\sum_{u=0}^{m-1}\sum_{v=0}^{n-1}\sum_{t_1=0}^{m-1}\sum_{s_1=0}^{n-1}\sum_{t_2=0}^{m-1}\sum_{s_2=0}^{n-1} a_{t_1,s_1}^{*}a_{t_1+u,s_1+v}a_{t_2+u,s_2+v}^{*}a_{t_2,s_2} = \\
&\sum_{t_1=0}^{m-1}\sum_{s_1=0}^{n-1}\sum_{t_2=0}^{m-1}\sum_{s_2=0}^{n-1} a_{t_1,s_1}^{*} \left( \sum_{u=0}^{m-1}\sum_{v=0}^{n-1} a_{t_1+u,s_1+v}a_{t_2+u,s_2+v}^{*} \right) a_{t_2,s_2} = \\
&\sum_{t_1=0}^{m-1}\sum_{s_1=0}^{n-1}\sum_{t_2=0}^{m-1}\sum_{s_2=0}^{n-1} a_{t_1,s_1}^{*} \left( AC_{\boldsymbol{A}}^{R}(t_2-t_1,s_2-s_1) \right) a_{t_2,s_2}.
\end{aligned}
\tag{8.6}
$$

The second equation is proved in a similar way. □

Our proof of the following theorem is a modification of its one-dimensional version presented by Kuznetsov [45].

**Theorem 8.1.** *Let $\boldsymbol{A}$ be an array over an arbitrary quaternion alphabet. Then the array $\boldsymbol{A}$ is right perfect if and only if it is left perfect.*

*Proof.* Assume that $\boldsymbol{A}$ is a right perfect array. We will show that the sum of the norms of the left off-peak autocorrelation values $\sum_{u=0}^{m-1}\sum_{\substack{v=0\\(u,v)\neq(0,0)}}^{n-1}\|AC_{\boldsymbol{A}}^{L}(u,v)\|$ is equal to zero, for all $(u,v)\neq(0,0)$. By Lemma (8.1), Equation (8.4) we have

$$
\sum_{u=0}^{m-1}\sum_{v=0}^{n-1}\|AC_{\boldsymbol{A}}^{L}(u,v)\| = \sum_{t_1=0}^{m-1}\sum_{t_2=0}^{m-1}\sum_{s_1=0}^{n-1}\sum_{s_2=0}^{n-1} a_{t_1,s_1}^{*}(AC_{\boldsymbol{A}}^{R}\,(t_2-t_1,s_2-s_1))\,a_{t_2,s_2}\,, \tag{8.7}
$$

Since $\boldsymbol{A}$ is right perfect, all right autocorrelation values are equal to zero, for all shifts $(u,v) \neq (0,0)$. Besides, it is true that $AC^L_{\boldsymbol{A}}(0,0) = AC^R_{\boldsymbol{A}}(0,0)$. Then $AC^R_{\boldsymbol{A}}(t_2 - t_1, s_2 - s_1) = 0$, for $t_1 \neq t_2$ or $s_1 \neq s_1 \neq s_2$. In this way, the Equation (8.7) above continues to

$$\sum_{u=0}^{m-1}\sum_{v=0}^{n-1} \|AC^L_{\boldsymbol{A}}(u,v)\| = \sum_{t_1=0}^{m-1}\sum_{s_1=0}^{n-1} a^*_{t_1,s_1} a_{t_1,s_1} AC^R_{\boldsymbol{A}}(0,0). \tag{8.8}$$

Thus,

$$\|AC^L_{\boldsymbol{A}}(0,0)\| + \sum_{\substack{u=0 \\ (u,v)\neq(0,0)}}^{m-1}\sum_{v=0}^{n-1} \|AC^L_{\boldsymbol{A}}(u,v)\| = AC^L_{\boldsymbol{A}}(0,0)AC^R_{\boldsymbol{A}}(0,0). \tag{8.9}$$

It follows that

$$\sum_{\substack{u=0 \\ (u,v)\neq(0,0)}}^{m-1}\sum_{v=0}^{n-1} \|AC^L_{\boldsymbol{A}}(u,v)\| = 0. \tag{8.10}$$

Since the sum of non-negative real numbers is equal to zero, we have that every summand is necessarily equal to zero. Thus, $\|AC^L_{\boldsymbol{A}}(u,v)\| = 0$, for $(u,v) \neq (0,0)$. So, $\boldsymbol{A}$ is left perfect by definition. The other direction of the statement is proved similarly. □

## 8.2 Inflation of perfect quaternary arrays

Arasu and de Launey [4] showed that every quaternary array, that is, any array over the four roots of unity $\pm 1, \pm i$, $\boldsymbol{A}$, of size $m \times n$, can be inflated into a perfect quaternary array of size $mp \times np$, provided $p = mn - 1$ is a prime number. Following from this, they showed that every quaternary array $\boldsymbol{A}$, of size $m \times n$, can be inflated into a perfect quaternary array of size $mp \times np$, provided $p = 2mn - 1$ is a prime number and $p \equiv 3 \ (mod\ 4)$. We generalise these results by proving the following statements: (1) every array $\boldsymbol{A}$, of size $m \times n$ over the basic quaternions

$\{1, -1, i, -i, j, -j, k, -k\}$, with $p = mn - 1$ a prime number, can be inflated into another perfect array over the basic quaternions of size $mp \times np$. (2) every array $\boldsymbol{A}$, of size $m \times n$ over the basic quaternions, with $p = 2mn - 1$ a prime number and $p \equiv 3 \ (mod\ 4)$, can be inflated into another perfect array over the basic quaternions of size $mp \times np$.

Arasu and de Launey's algorithm for inflation of perfect quaternary arrays is explained in terms of inflation polynomials [4]. In the following construction, rather than a polynomial approach, we use a matrix approach.[1]

**Theorem 8.2** (Arasu and de Launey [4])**.** *If there is a perfect quaternary array of size $m \times n$ and $p = mn - 1$ is a prime number, then there is a perfect quaternary array of size $mp \times np$.*

**Construction 8.1.**

*We now present our modified method of Arasu and de Launey's algorithm by working with matrices instead of polynomials.*

1. *Take a Legendre sequence $\boldsymbol{L}_p = (0, s_1, \dots, s_{p-1})$ of length $p$ and replace the element $0$ by $i^{\frac{p+1}{2}}$, to obtain the sequence $\boldsymbol{S} = (i^{\frac{p+1}{2}}, s_1, \dots, s_{p-1})$. This change leaves the off-peak values unaltered and the peak value is increased by one.*
2. *Produce $p+1$ arrays, called inflation arrays, from $\boldsymbol{S}$ and the shifts $\boldsymbol{S}^k$ of $\boldsymbol{S}$, for $k = 0, 1, \dots, p-1$, as follows*

$$\boldsymbol{B}_0 = \begin{pmatrix} \boldsymbol{S} & \boldsymbol{S} & \cdots & \boldsymbol{S} \\ \downarrow & \downarrow & & \downarrow \end{pmatrix}^T, \boldsymbol{B}_1 = \begin{pmatrix} \boldsymbol{S} & \boldsymbol{S}^1 & \cdots & \boldsymbol{S}^{p-1} \\ \downarrow & \downarrow & & \downarrow \end{pmatrix}, \boldsymbol{B}_2 = \begin{pmatrix} \boldsymbol{S} & \boldsymbol{S}^{(1)2} & \cdots & \boldsymbol{S}^{(p-1)2} \\ \downarrow & \downarrow & & \downarrow \end{pmatrix}, \dots,$$

$$\boldsymbol{B}_{p-1} = \begin{pmatrix} \boldsymbol{S} & \boldsymbol{S}^{(1)(p-1)} & \cdots & \boldsymbol{S}^{(p-1)(p-1)} \\ \downarrow & \downarrow & & \downarrow \end{pmatrix}, \boldsymbol{B}_p = \begin{pmatrix} \boldsymbol{S} & \boldsymbol{S} & \cdots & \boldsymbol{S} \\ \downarrow & \downarrow & & \downarrow \end{pmatrix}. \tag{8.11}$$

*The inflation arrays $\boldsymbol{B}_0, \boldsymbol{B}_1, \dots, \boldsymbol{B}_p$ have the following properties:*

[1] The author acknowledges and thanks Nathan Jolly, Ph.D. candidate at Monash University, for explaining Arasu and De Launey's construction for inflating perfect quaternary arrays, in terms of matrices.

(a) *The autocorrelation arrays of the arrays* $\boldsymbol{B}_0, \boldsymbol{B}_1, \dots, \boldsymbol{B}_p$*, are*

$$\begin{pmatrix} p^2 & -p & \dots & -p \\ p^2 & -p & \dots & -p \\ \vdots & \vdots & & \vdots \\ p^2 & -p & \dots & -p \end{pmatrix}, \begin{pmatrix} p^2 & -p & \dots & -p \\ -p & p^2 & \dots & -p \\ \vdots & \vdots & & \vdots \\ -p & -p & \dots & p^2 \end{pmatrix}, \begin{pmatrix} p^2 & -p & \dots & -p \\ -p & -p & \dots & -p \\ -p & p^2 & \dots & -p \\ \vdots & \vdots & & \vdots \\ -p & -p & \dots & p^2 \\ -p & -p & \dots & -p \end{pmatrix}, \dots,$$

$$\begin{pmatrix} p^2 & -p & \dots & -p \\ -p & -p & \dots & p^2 \\ \vdots & \vdots & & \vdots \\ -p & p^2 & \dots & -p \\ -p & -p & \dots & -p \end{pmatrix}, \begin{pmatrix} p^2 & p^2 & \dots & p^2 \\ -p & -p & \dots & -p \\ \vdots & \vdots & & \vdots \\ -p & -p & \dots & -p \end{pmatrix}, \tag{8.12}$$

*respectively. We have that the sum of these autocorrelation arrays of* $\boldsymbol{B}_0$*,* $\boldsymbol{B}_1, \dots, \boldsymbol{B}_p$ *is*

$$AC_{\boldsymbol{B}_0} + \cdots + AC_{\boldsymbol{B}_p} = \begin{pmatrix} p^2(p+1) & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} \tag{8.13}$$

(b) *From Equation (8.13), and for* $0 \leq \alpha, \beta \leq p-1$*, the summation of all* $(\alpha, \beta)$ *off-peak autocorrelation values, of the arrays* $\boldsymbol{B}_0, \dots, \boldsymbol{B}_p$ *is equal to zero, that is, for* $(\alpha, \beta) \neq (0, 0)$

$$\sum_{r=0}^{m-1} \sum_{s=0}^{n-1} AC_{\boldsymbol{B}_{r+ns}}(\alpha, \beta) = 0. \tag{8.14}$$

(c) *For* $0 \leq r, s \leq p$*, with* $r \neq s$*, the cross-correlation values of* $\boldsymbol{B}_r$ *and* $\boldsymbol{B}_s$ *are constant, with value one, that is, for all* $0 \leq \alpha, \beta \leq p-1$

$$CC_{\boldsymbol{B}_r, \boldsymbol{B}_s}(\alpha, \beta) = 1. \tag{8.15}$$

3. *Arrange the two-dimensional arrays* $\boldsymbol{B}, \boldsymbol{B}_0, \boldsymbol{B}_1, \dots, \boldsymbol{B}_p$ *into a* ***four-dimensional***

*array* $\boldsymbol{C}$ *of size* $m \times p \times p \times n$, *(a two-dimensional array of two-dimensional arrays) as follows, in Array (8.16)*

$$\begin{pmatrix} a(0,0)\boldsymbol{B}_0 & a(0,1)\boldsymbol{B}_m & \dots & a(0,s)\boldsymbol{B}_{sm} & \dots & a(0,n-1)\boldsymbol{B}_{(n-1)m} \\ a(1,0)\boldsymbol{B}_1 & a(1,1)\boldsymbol{B}_{m+1} & \dots & a(1,s)\boldsymbol{B}_{sm+1} & \dots & a(1,n-1)\boldsymbol{B}_{(n-1)m+1} \\ \vdots & \vdots & & \vdots & & \vdots \\ a(r,0)\boldsymbol{B}_r & a(r,1)\boldsymbol{B}_{m+r} & \dots & a(r,s)\boldsymbol{B}_{sm+r} & \dots & a(r,n-1)\boldsymbol{B}_{(n-1)m+r} \\ \vdots & \vdots & & \vdots & & \vdots \\ a(m-1,0)\boldsymbol{B}_{m-1} & a(m-1,1)\boldsymbol{B}_{m+m-1} & \dots & a(m-1,s)\boldsymbol{B}_{sm+m-1} & \dots & a(m-1,n-1)\boldsymbol{B}_{(n-1)m+m-1} \end{pmatrix} \tag{8.16}$$

*Notice that every entry in the array* $\boldsymbol{C}$ *is a two-dimensional array of size* $p \times p$, *so* $\boldsymbol{C}$ *is of size* $m \times p \times p \times n$.

**Notation 8.1.** *If* $b_{r+ms}(u,v)$ *is the* $(u,v)$ *entry of the array* $\boldsymbol{B}_{r+ms}$, *then the* $(r,u,v,s)$ *entry of the array* $\boldsymbol{C}$ *is given by*

$$c(r,u,v,s) = a(r,s)b_{r+ms}(u,v). \tag{8.17}$$

4. *Reduce the dimension of the array* $\boldsymbol{C}$, *without reducing the number of entires, into a two-dimensional array* $\boldsymbol{D} = (d(r,s))$ *of size* $mp \times np$, *as follows: for* $0 \leq r \leq mp-1$ *and* $0 \leq s \leq np-1$, *the* $(r,s)$ *entry of the array* $\boldsymbol{D}$ *is the complex number*

$$d(r,s) = c(r\ (mod\ m), r\ (mod\ p), s\ (mod\ p), s\ (mod\ n)). \tag{8.18}$$

The following example illustrates Construction (8.1).

**Example 8.2.** *The perfect array*

$$\boldsymbol{A} = \begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix} \tag{8.19}$$

*of size* $2 \times 2$ *is inflated into a perfect array* $\boldsymbol{C}$ *of size* $6 \times 6$ *as follows: set* $m = n = 2$ *and* $p = mn - 1 = 3$. *Consider the sequence*

$$\boldsymbol{S} = (i^{\frac{p+1}{2}}, 1, -1) = (-1, 1, -1), \tag{8.20}$$

*which is a modified version of the Legendre sequence* $\boldsymbol{L}_3 = (0, 1, -1)$. *Now, produce* $p + 1 = 4$ *inflation arrays, by shifts of* $\boldsymbol{S}$ *as rows in* $\boldsymbol{B}_0$ *and as columns in* $\boldsymbol{B}_1$, $\boldsymbol{B}_2$ *and* $\boldsymbol{B}_3$, *as follows:*

$$\begin{aligned} \boldsymbol{B}_0 &= \begin{pmatrix} -1 & 1 & -1 \\ -1 & 1 & -1 \\ -1 & 1 & -1 \end{pmatrix}, \boldsymbol{B}_1 = \begin{pmatrix} -1 & -1 & 1 \\ 1 & -1 & -1 \\ -1 & 1 & -1 \end{pmatrix}, \\ \boldsymbol{B}_2 &= \begin{pmatrix} -1 & 1 & -1 \\ 1 & -1 & -1 \\ -1 & -1 & 1 \end{pmatrix}, \boldsymbol{B}_3 = \begin{pmatrix} -1 & -1 & -1 \\ 1 & 1 & 1 \\ -1 & -1 & -1 \end{pmatrix}. \end{aligned} \tag{8.21}$$

*From Equation (8.16), produce the four dimensional array (i.e. an array of arrays)* $\boldsymbol{C}$, *of size* $2 \times 3 \times 3 \times 2$, *as follows*

$$\boldsymbol{C} = \begin{pmatrix} 1\boldsymbol{B}_0 & i\boldsymbol{B}_2 \\ i\boldsymbol{B}_1 & -1\boldsymbol{B}_3 \end{pmatrix} \tag{8.22}$$

*which is equal to*

$$\begin{pmatrix} 1\begin{pmatrix} -1 & 1 & -1 \\ -1 & 1 & -1 \\ -1 & 1 & -1 \end{pmatrix} & i\begin{pmatrix} -1 & 1 & -1 \\ 1 & -1 & -1 \\ -1 & -1 & 1 \end{pmatrix} \\ i\begin{pmatrix} -1 & -1 & 1 \\ 1 & -1 & -1 \\ -1 & 1 & -1 \end{pmatrix} & -1\begin{pmatrix} -1 & -1 & -1 \\ 1 & 1 & 1 \\ -1 & -1 & -1 \end{pmatrix} \end{pmatrix} = \tag{8.23}$$

$$\begin{pmatrix} \begin{pmatrix} -1 & 1 & -1 \\ -1 & 1 & -1 \\ -1 & 1 & -1 \end{pmatrix} & \begin{pmatrix} -i & i & -i \\ i & -i & -i \\ -i & -i & i \end{pmatrix} \\ \begin{pmatrix} -i & -i & i \\ i & -i & -i \\ -i & i & -i \end{pmatrix} & \begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 1 \end{pmatrix} \end{pmatrix} \tag{8.24}$$

*Since Array (8.24) is a* $2 \times 2$ *matrix of* $3 \times 3$ *matrices, it is a four-dimensional array, of size* $2 \times 3 \times 3 \times 2$.

*Change the four-dimensional array* $\boldsymbol{C}$ *into a two-dimensional array* $\boldsymbol{D} = (d(r,s))$ *of size* $6 \times 6$ *via the equation*

$$d(r,s) = c(r\ (mod 2), r\ (mod 3), s\ (mod 3), s\ (mod 2)), \tag{8.25}$$

*for* $r = 0, \ldots, 5$ *and* $s = 0, \ldots, 5$*. Equation (8.25), determines the* $(r,s)$ *entry of the array* $\boldsymbol{D}$ *as a specific entry of the array* $\boldsymbol{C}$ *and all entries of* $\boldsymbol{C}$ *are used. And so, we reduce the dimension of* $\boldsymbol{C}$ *from 4 to 2, preserving perfection and without reducing the number* *of entries of* $\boldsymbol{C}$*. We obtain the perfect two-dimensional array of size* $6 \times 6$*.*

$$\boldsymbol{D} = \begin{pmatrix} -1 & i & -1 & -i & -1 & -i \\ i & -1 & -i & 1 & -i & 1 \\ -1 & -i & -1 & i & -1 & -i \\ -i & -1 & -i & 1 & i & 1 \\ 1 & -i & 1 & -i & 1 & i \\ -i & -1 & i & 1 & -i & 1 \end{pmatrix} \tag{8.26}$$

We wrote the following code in *Mathematica* to inflate quaternary arrays.

```
Arasu[A_] := (r = Dimensions[A][[1]]; s = Dimensions[A]
    [[2]]; p = Dimensions[A][[1]]*Dimensions[A][[2]] - 1;
    If[PrimeQ[p], (c = Prepend[Delete[Table[
    JacobiSymbol[k - 1, p], {k, p}], 1], I^((p + 1)/2)];
    L1 = Prepend[Table[Transpose[Table[RotateRight
    [c, j*(i - 1)], {i, p}]], {j, p}], Table[c,
    {i, p}]]; L2 = Table[A[[i, l]]*L1[[(i - 1) + r*(l - 1)
    + 1,j, k]], {i, 1, r}, {j, 1, p}, {k, 1, p}, {l, 1, s}];
    L3 = Table[L2[[Mod[i - 1, r] + 1, Mod[i - 1, p] + 1,
    Mod[j - 1,p] + 1, Mod[j - 1, s] + 1]], {i, r*p},
    {j, s*p}]), Print["p is not a prime"]]);
```

We now present Arasu and de Launey inflation algorithm for perfect quaternary matrices of size $mn = \frac{p+1}{2}$.

**Theorem 8.3** (Arasu and de Launey [4])**.** *If there is a perfect quaternary array of size* $m \times n$*,* $p = 2mn - 1$ *is a prime number and* $p \equiv 3 \ (mod\ 4)$*, then there is a perfect quaternary array of size* $mp \times np$*.*

**Construction 8.2** (Inflation of perfect quaternary arrays:
size $mn = \frac{p+1}{2}$**).**
*Let $p$ be a prime number, where $p \equiv 3 \pmod 4$ and let $\boldsymbol{A}$ be a perfect quaternary array of size $m \times n$, where $mn = \frac{p+1}{2}$, we inflate the perfect array $\boldsymbol{A}$, as follows:*

1. *Produce $p+1$ arrays, $\boldsymbol{B}_0, \boldsymbol{B}_1, \ldots, \boldsymbol{B}_p$, from the sequence $\boldsymbol{S}$, as in Construction (8.1). These arrays are all binary arrays, since $p \equiv 3 (mod\ 4)$.*
2. *Construct $\frac{p+1}{2}$ inflation arrays of size $p \times p$: for $r = 0, 1, \ldots, \frac{p-1}{2}$, and put*

$$\boldsymbol{C}_r = \left(\frac{1+i}{2}\right)(\boldsymbol{B}_{2r} + i\boldsymbol{B}_{2r+1}), \tag{8.27}$$

   *All the coefficients of this matrix are complex fourth roots of unity. The arrays $\boldsymbol{C}_0, \boldsymbol{C}_1, \ldots, \boldsymbol{C}_{\frac{p-1}{2}}$ satisfy the conditions of the inflation arrays stated in Construction (8.1)*
3. *Arrange the arrays $\boldsymbol{A}, \boldsymbol{C}_0, \boldsymbol{C}_1, \ldots, \boldsymbol{C}_{\frac{p-1}{2}}$ into a four-dimensional array $\boldsymbol{D}$ of size $m \times p \times p \times n$ as follows: if $c_{r+ms}(u,v)$ is the $(u,v)$ entry of the inflation array $\boldsymbol{D}_{r+ms}$, then for $0 \le r \le m-1$, $0 \le s \le n-1$ and $0 \le u, v \le p-1$, we have*

$$d(r,u,v,s) = a(r,s)c_{r+ms}(u,v), \tag{8.28}$$

   *and* $0 \le s \le np-1$.
4. *Reduce the dimension of the arrays $\boldsymbol{D}$ into a two dimensional array $\boldsymbol{E}$. The $(r,s)$ entry of the array $\boldsymbol{E}$ is*

$$e(r,s) = d(r\ (mod\ m), r\ (mod\ p), s\ (mod\ p), s(mod\ n)). \tag{8.29}$$

## 8.3 Inflation of perfect arrays over the basic quaternions: size $mn = p - 1$

We modify the algorithm of Arasu and de Launey [4], for inflating perfect quaternary arrays, into an algorithm to inflate perfect arrays over the basic quaternions. The new arrays will have larger size and perfect autocorrelation. We will inflate arrays of size $m \times n$, into arrays of size $mp \times np$, provided $p = mn - 1$ is a prime number. Then, we will prove that the newly inflated arrays have perfect autocorrelation.

**Theorem 8.4.** *If there is a perfect array, over the basic quaternions $\{\pm 1, \pm i, \pm j, \pm k\}$, of size $m \times n$ and $p = mn - 1$ is a prime number, then there is a perfect array of size $mp \times np$, over the basic quaternions.*

**Construction 8.3** (Inflation of perfect arrays over the basic quaternions:
size $mn = p + 1$**).**

*Let $\boldsymbol{A}$ be a perfect array of size $m \times n$ over the basic quaternions, where $p = mn - 1$ is a prime number.*

1. *Take a Legendre sequence $\boldsymbol{L}_p = (0, s_1, \dots, s_{p-1})$ of length $p$ and replace the element $0$ by $i^{\frac{p+1}{2}}$, to obtain the sequence $\boldsymbol{S}_i = (i^{\frac{p+1}{2}}, s_1, \dots, s_{p-1})$. The element $0$ can also be replaced by $j^{\frac{p+1}{2}}$ or $k^{\frac{p+1}{2}}$, producing the sequence $\boldsymbol{S}_j = (j^{\frac{p+1}{2}}, s_1, \dots, s_{p-1})$ or $\boldsymbol{S}_k = (k^{\frac{p+1}{2}}, s_1, \dots, s_{p-1})$, respectively. The following construction is valid for any of these sequences, since all three sequences have the same autocorrelation $(p, -1, \dots, -1)$. In this construction we use the sequence $\boldsymbol{S}_i$.*
2. *Produce $p + 1$ inflation arrays, $\boldsymbol{B}_0, \boldsymbol{B}_1, \dots, \boldsymbol{B}_p$, from the sequence $\boldsymbol{S}_i$, as in Construction (8.1), Section (8.2), by setting shifts of $\boldsymbol{S}$ as rows in $\boldsymbol{B}_0$ and as columns in $\boldsymbol{B}_1, \dots, \boldsymbol{B}_p$ in a similar manner.*
3. *Arrange the arrays $\boldsymbol{A}, \boldsymbol{B}_0, \boldsymbol{B}_1, \dots, \boldsymbol{B}_p$ into a four-dimensional array $\boldsymbol{C}$ of size $m \times p \times p \times n$ as follows.*

*From Equation (8.17), if $b(u,v)_{r+ms}$ is the $(u,v)$ entry of the inflation array $\boldsymbol{B}_{r+ms}$, then for $0 \leq r \leq m-1$, $0 \leq s \leq n-1$ and $0 \leq u,v \leq p-1$, the $(r,u,v,s)$ entry of the array $\boldsymbol{C}$ is given by*

$$c(r,u,v,s) = a(r,s)b_{r+ms}(u,v). \tag{8.30}$$

4. *Reduce the dimension of the array $\boldsymbol{C}$, without reducing the number of entries, into a two-dimensional array $\boldsymbol{D} = (d(r,s))$ of size $mp \times np$, as follows: for $0 \leq r \leq mp-1$ and $0 \leq s \leq np-1$, the $(r,s)$ entry of the array $\boldsymbol{D}$ is*

$$d(r,s) = c(r \ (mod\ m), r \ (mod\ p), s \ (mod\ p), s \ (mod\ n)). \tag{8.31}$$

We now show that the array $\boldsymbol{C}$ is perfect.

**Theorem 8.5.** *The array $\boldsymbol{C}$ in Equation (8.30) has perfect autocorrelation.*

*Proof.* We need to prove that all off-peak values of the array $\boldsymbol{C}$ are zero. First we write the autocorrelation function for the array $\boldsymbol{C}$ in terms of the arrays $\boldsymbol{A}, \boldsymbol{B}_0, \ldots, \boldsymbol{B}_p$.

The right $(\alpha, \beta, \gamma, \delta)$-autocorrelation value of $\boldsymbol{C}$ is given by the equation

$$AC^R_{\boldsymbol{C}}(\alpha,\beta,\gamma,\delta) = \sum_{r=0}^{m-1}\sum_{u=0}^{p-1}\sum_{v=0}^{p-1}\sum_{s=0}^{n-1} c(r,u,v,s)c^*(r+\alpha, u+\beta, v+\gamma, s+\delta), \tag{8.32}$$

where

$$c(r,u,v,s) = a(r,s)b_{r+ms}(u,v), \tag{8.33}$$

and $b_{r+ms}(u,v)$ is the $(u,v)$ entry of the inflation array $\boldsymbol{B}_{r+ms}$. So, we can write the right $(\alpha, \beta, \gamma, \delta)$-autocorrelation value of $\boldsymbol{C}$ as follows

$$AC^R_{\boldsymbol{C}}(\alpha, \beta, \gamma, \delta) =$$

$$\sum_{r=0}^{m-1}\sum_{u=0}^{p-1}\sum_{v=0}^{p-1}\sum_{s=0}^{n-1} a(r,s) b_{r+ms}(u,v) \left(a(r+\alpha, s+\delta) b_{r+\alpha+n(s+\delta)}(u+\beta, v+\gamma)\right)^* =$$

$$\sum_{r=0}^{m-1}\sum_{s=0}^{n-1} a(r,s) \left(\sum_{u=0}^{p-1}\sum_{v=0}^{p-1} b_{r+ms}(u,v) b^*_{r+\alpha+m(s+\delta)}(u+\beta, v+\gamma)\right) a^*(r+\alpha, s+\delta). \tag{8.34}$$

Since the expression $\sum_{u=0}^{p-1}\sum_{v=0}^{p-1} b_{r+ms}(u,v) b^*_{r+\alpha+n(s+\delta)}(u+\beta, v+\gamma)$ in Equation (8.34), is the cross-correlation of the arrays $\boldsymbol{B}_{r+ms}$ and $\boldsymbol{B}_{r+\alpha+m(s+\delta)}$, Equation (8.34) can be written as

$$AC^R_{\boldsymbol{C}}(\alpha, \beta, \gamma, \delta) = \sum_{r=0}^{m-1}\sum_{s=0}^{n-1} a(r,s) \left(CC_{\boldsymbol{B}_{r+ms}, \boldsymbol{B}_{r+\alpha+m(s+\delta)}}(\beta, \gamma)\right) a^*(r+\alpha, s+\delta). \tag{8.35}$$

In order to prove that $\boldsymbol{C}$ is perfect, we consider the following four cases $\alpha \neq 0, \beta \neq 0, \gamma \neq 0$ and $\delta \neq 0$.

Case 1. $\alpha \neq 0$. Then $\boldsymbol{B}_{r+ms}$ and $\boldsymbol{B}_{r+\alpha+m(s+\delta)}$ are different arrays. So, by Equation (8.15), the $(\beta, \gamma)$ cross-correlation value of $\boldsymbol{B}_{r+ms}$ and $\boldsymbol{B}_{r+\alpha+m(s+\delta)}$ is 1. So Equation (8.35), becomes

$$AC^R_{\boldsymbol{C}}(\alpha, \beta, \gamma, \delta) = \sum_{r=0}^{m-1}\sum_{s=0}^{n-1} a(r,s)\,(1)\, a^*(r+\alpha, s+\delta). \tag{8.36}$$

Now, since $\boldsymbol{A}$ is a perfect array, from Equation (8.36), we have

$$AC^R_{\boldsymbol{C}}(\alpha, \beta, \gamma, \delta) = 0. \tag{8.37}$$

Case 2. $\delta \neq 0$. Similar to Case 1.

Case 3. $\beta \neq 0$.

Case a. $\alpha = \delta = 0$. since $\alpha = \delta = 0$, we have $\boldsymbol{B}_{r+\alpha+m(s+\delta)} = \boldsymbol{B}_{r+ms}$ and so, the $(\beta, \gamma)$ cross-correlation value of $\boldsymbol{B}_{r+\alpha+m(s+\delta)}$ and $\boldsymbol{B}_{r+ms}$ becomes the $(\beta, \gamma)$ autocorrelation value of $\boldsymbol{B}_{r+ms}$. Equation (8.35) is written as

$$AC^R_{\boldsymbol{C}}(\alpha, \beta, \gamma, \delta) = \sum_{r=0}^{m-1} \sum_{s=0}^{n-1} a(r,s) \left(AC_{\boldsymbol{B}_{r+ms}}(\beta, \gamma)\right) a^*(r,s). \tag{8.38}$$

From Equation (8.12), $AC_{\boldsymbol{B}_{r+ms}}(\beta, \gamma)$ is either $p^2$ or $-p$, which are integers and commute with quaternions. Equation (8.39), becomes

$$\begin{gathered} AC^R_{\boldsymbol{C}}(\alpha, \beta, \gamma, \delta) = \\ \sum_{r=0}^{m-1} \sum_{s=0}^{n-1} a(r,s) a^*(r,s) \left(AC_{\boldsymbol{B}_{r+ms}}(\beta, \gamma)\right) = \\ \sum_{r=0}^{m-1} \sum_{s=0}^{n-1} 1 \left(AC_{\boldsymbol{B}_{r+ms}}(\beta, \gamma)\right). \end{gathered} \tag{8.39}$$

Now from Equation (8.14), we have that

$$\sum_{r=0}^{m-1} \sum_{s=0}^{n-1} AC_{\boldsymbol{B}_{r+ms}}(\beta, \gamma) = 0. \tag{8.40}$$

Thus, $AC^R_{\boldsymbol{C}}(\alpha, \beta, \gamma, \delta) = 0$

Case b. $\alpha \neq 0$. See Case 1.

Case c. $\delta \neq 0$. See Case 2.

Case 4. $\gamma \neq 0$. Similar to Case 3.

As required. □

We now show that the array $\boldsymbol{D}$ has perfect autocorrelation.

**Theorem 8.6.** *The array $\boldsymbol{D}$ in Equation (8.31) has perfect autocorrelation.*

*Proof.* In this proof we will show that an off-peak autocorrelation value of the array $\boldsymbol{D}$ is equal to an off-peak autocorrelation value of the array $\boldsymbol{C}$, which is perfect. We will do this by showing that, if the shift $(\alpha, \beta)$ is non trivial, then the shift of $\boldsymbol{C}$ associated with $(\alpha, \beta)$ is also non trivial.

For $(\alpha, \beta) \in \mathbb{Z}_{mp} \times \mathbb{Z}_{np} \setminus \{(0,0)\}$, we use the equation

$$d(r,s) = c(r \ (mod\ m), r \ (mod\ p), s \ (mod\ p), s \ (mod\ n)), \tag{8.41}$$

to produce the right $(\alpha, \beta)$-autocorrelation value of $\boldsymbol{D}$ as follows

$$\begin{gathered} AC^R_{\boldsymbol{D}}(\alpha,\beta) = \\ \sum_{r=0}^{mp-1}\sum_{s=0}^{np-1} d(r,s)d^*(r+\alpha, s+\beta) = \\ \sum_{r=0}^{mp-1}\sum_{s=0}^{np-1} c(r\ (mod\ m), r\ (mod\ p), s\ (mod\ p) s\ (mod\ n)) \\ c(r\ (mod\ m) + \alpha\ (mod\ m), r\ (mod\ p) + \alpha\ (mod\ p), s\ (mod\ p) + \beta\ (mod\ p), s(mod\ n) + \beta\ (mod\ n)). \end{gathered} \tag{8.42}$$

So Equation (8.41) above continues

$$\begin{gathered} \sum_{u=0}^{m-1}\sum_{v=0}^{p-1}\sum_{x=0}^{p-1}\sum_{y=0}^{n-1} c(u,v,x,y)c^*(u+\alpha\ (mod\ m), v+\alpha\ (mod\ p), x+\beta\ (mod\ p), y+\beta\ (mod\ n)) = \\ AC^R_C(\alpha\ (mod\ m), \alpha\ (mod\ p), \beta\ (mod\ p), \beta\ (mod\ n)). \end{gathered} \tag{8.43}$$

Case 1. $\alpha \neq 0$. Since $0 \leq \alpha \leq mp - 1$ and $GCD(m,p) = 1$, this implies that no number less than $mp$ is divisible by $m$ and $p$. Therefore, if $\alpha \equiv 0 \ (mod\ m)$, then $\alpha \not\equiv 0\ (mod\ p)$, and similarly if $\alpha \equiv 0\ (mod\ p)$, then $\alpha \not\equiv 0\ (mod\ m)$. Thus, the shift $(\alpha\ (mod\ m), \alpha\ (mod\ p), \beta\ (mod\ p), \beta\ (mod\ n))$ of $\boldsymbol{C}$ is not equivalent to the shift $(0,0,0,0)\ mod\ (m,p,p,n)$.

Case 2. $\beta \neq 0$. Similar to Case 1.

□

**Example 8.3.** *The perfect array*

$$A = \begin{pmatrix} 1 & i \\ j & k \end{pmatrix} \tag{8.44}$$

*of size* $2 \times 2$ *is inflated into a perfect array* $\boldsymbol{C}$ *of size* $6 \times 6$ *as follows: set* $m = n = 2$ *and* $p = 3$*. Consider the sequence* $\boldsymbol{S} = (i^{\frac{p+1}{2}}, 1, -1) = (-1, 1, -1)$*, which is a modification of the Legendre sequence* $(0, 1, -1)$*. Produce* $p + 1 = 4$ *inflation arrays, with shifts of* $\boldsymbol{S}$ *as rows in* $\boldsymbol{B}_0$ *and as columns in* $\boldsymbol{B}_1$*,* $\boldsymbol{B}_2$ *and* $\boldsymbol{B}_3$*, as follows:*

$$\begin{gathered} \boldsymbol{B}_0 = \begin{pmatrix} -1 & 1 & -1 \\ -1 & 1 & -1 \\ -1 & 1 & -1 \end{pmatrix}, \boldsymbol{B}_1 = \begin{pmatrix} -1 & -1 & 1 \\ 1 & -1 & -1 \\ -1 & 1 & -1 \end{pmatrix}, \\ \boldsymbol{B}_2 = \begin{pmatrix} -1 & 1 & -1 \\ 1 & -1 & -1 \\ -1 & -1 & 1 \end{pmatrix}, \boldsymbol{B}_3 = \begin{pmatrix} -1 & -1 & -1 \\ 1 & 1 & 1 \\ -1 & -1 & -1 \end{pmatrix}. \end{gathered} \tag{8.45}$$

*From Equation (8.16), produce the four dimensional array (a* $2 \times 2$ *array of* $3 \times 3$ *arrays)* $\boldsymbol{C}$*, of size* $2 \times 3 \times 3 \times 2$*, as follows:*

$$\boldsymbol{C} = \begin{pmatrix} 1\begin{pmatrix} \text{-}1 & 1 & \text{-}1 \\ \text{-}1 & 1 & \text{-}1 \\ \text{-}1 & 1 & \text{-}1 \end{pmatrix} & i\begin{pmatrix} \text{-}1 & 1 & \text{-}1 \\ 1 & \text{-}1 & \text{-}1 \\ \text{-}1 & \text{-}1 & 1 \end{pmatrix} \\ j\begin{pmatrix} \text{-}1 & \text{-}1 & 1 \\ 1 & \text{-}1 & \text{-}1 \\ \text{-}1 & 1 & \text{-}1 \end{pmatrix} & k\begin{pmatrix} \text{-}1 & \text{-}1 & \text{-}1 \\ 1 & 1 & 1 \\ \text{-}1 & \text{-}1 & \text{-}1 \end{pmatrix} \end{pmatrix} =$$

$$\begin{pmatrix} \begin{pmatrix} \text{-}1 & 1 & \text{-}1 \\ \text{-}1 & 1 & \text{-}1 \\ \text{-}1 & 1 & \text{-}1 \end{pmatrix} & \begin{pmatrix} \text{-}i & i & \text{-}i \\ i & \text{-}i & \text{-}i \\ \text{-}i & \text{-}i & i \end{pmatrix} \\ \begin{pmatrix} \text{-}j & \text{-}j & j \\ j & \text{-}j & \text{-}j \\ \text{-}j & j & \text{-}j \end{pmatrix} & \begin{pmatrix} k & k & k \\ \text{-}k & \text{-}k & \text{-}k \\ k & k & k \end{pmatrix} \end{pmatrix} \tag{8.46}$$

*We reduce the dimension of the array* $\boldsymbol{C}$*, without reducing the number of entries, into a two-dimensional array* $\boldsymbol{D} = (d(r,s))$ *of size* $6 \times 6$ *via the equation*

$$d(r,s) = c(r\ (mod\ 2), r\ (mod\ 3), s\ (mod\ 3), s\ (mod\ 2)) \tag{8.47}$$

*for* $r = 0, \ldots, 5$ *and* $s = 0, \ldots, 5$*, preserving perfection and the number of entries. And so, we obtain the perfect two-dimensional array of size* $6 \times 6$

$$\boldsymbol{D} = \begin{pmatrix} \text{-}1 & i & \text{-}1 & \text{-}i & 1 & \text{-}i \\ j & k & \text{-}j & k & \text{-}j & k \\ \text{-}1 & \text{-}i & \text{-}1 & \text{-}i & 1 & i \\ \text{-}j & \text{-}k & j & \text{-}k & \text{-}j & \text{-}k \\ \text{-}1 & \text{-}i & \text{-}1 & i & 1 & \text{-}i \\ \text{-}j & \text{-}k & \text{-}j & \text{-}k & j & \text{-}k \end{pmatrix} \tag{8.48}$$

We wrote the following code in *Mathematica* to inflate arrays over the basic quaternions.

```
In[1]:= << Quaternions'
In[2]:= i = Quaternion[0, 1, 0, 0]
Out[2]= Quaternion[0, 1, 0, 0]
In[3]:= j = Quaternion[0, 0, 1, 0]
Out[3]= Quaternion[0, 0, 1, 0]
In[4]:= k = Quaternion[0, 0, 0, 1]
Out[4]= Quaternion[0, 0, 0, 1]

In[5]:= ArasuQ[A_] := (r = Dimensions[A][[1]]; s =
          Dimensions[A][[2]];
          p = Dimensions[A][[1]]*Dimensions[A][[2]] - 1;
          If[PrimeQ[p], (c = Prepend[Delete[Table[
          JacobiSymbol[k - 1, p], {k, p}], 1],I^((p + 1)
          /2)]; L1 = Prepend[Table[Transpose
          [Table[RotateRight[c, j*(i - 1)], {i, p}]],
          {j, p}], Table[c,{i, p}]] ; L2 = Table[A[[i, l]]
           ** L1[[(i - 1) + r*(l - 1) + 1, j, k]],
           {i, 1, r},{j, 1, p}, {k, 1, p}, {l, 1, s}]; L3 =
           Table[L2[[Mod[i - 1, r] + 1, Mod[i - 1, p] + 1,
          Mod[j - 1, p] + 1, Mod[j - 1, s]+ 1]],
          {i, r*p}, {j, s*p}]), Print["p is not a prime"]]);
```

And we wrote the following code in *Mathematica* to compute the autocorrelation of two-dimensional arrays over the basic quaternions.

```
In[6]:= LACVM[m_] := Table[Table[Simplify[Sum[
         Sum[m[[i, j]] ** Conjugate[m[[If[0 < Mod[i + k - 1,
          Dimensions[m][[1]]] < Dimensions[m][[1]],
Mod[i + k - 1, Dimensions[m][[1]]], If[Mod[i + k
- 1, Dimensions[m][[1]]] > Dimensions[m][[1]],
Mod[i + k - 1, Dimensions[m][[1]]] + 1,
Dimensions[m][[1]]]], If[0 < Mod[j + l - 1,
Dimensions[m][[2]]] < Dimensions[m][[2]],
Mod[j + l - 1, Dimensions[m][[2]]],
If[Mod[j + l - 1, Dimensions[m][[2]]] > Dimensions
[m][[2]],Mod[j + l - 1, Dimensions[m][[2]]] + 1,
Dimensions[m][[2]]]]]]]], {j, 1, Dimensions[m]
[[2]]}], {i, 1, Dimensions[m][[1]]}]],{1,
Dimensions[m][[2]]}], {k, 1, Dimensions[m][[1]]}];
```

## 8.4 Inflation of perfect arrays over the basic quaternions: size $mn = \frac{p-1}{2}$

We now present another construction for inflating perfect arrays over the basic quaternions. This construction is a modification of Arasu and de Launay [4] algorithm explained in Construction (8.2) for inflating quaternary arrays of size $mn = \frac{p-1}{2}$, where $p$ is a prime number and $p \equiv 3 \ (mod\ 4)$.

If the size $m \times n$ of the array $\boldsymbol{A}$ in Construction (8.3) (Inflation of Perfect Arrays over the basic quaternions), is such that $p = 2mn - 1$, for $p$ a prime number and $p \equiv 3 \ (mod\ 4)$, then we can produce $\frac{p+1}{2}$ inflation arrays. So, we will inflate arrays of size $m \times n$, into arrays of size $mp \times np$, provided $p = 2mn - 1$ is a prime number and $p \equiv 3 \ (mod\ 4)$. Then, we will prove that the newly inflated arrays have perfect autocorrelation in Theorem (8.7)

**Construction 8.4** (Inflation of perfect arrays over the basic quaternions: size $mn = \frac{p+1}{2}$).

*Let $p$ be a prime number, where $p \equiv 3 \pmod 4$ and let $\boldsymbol{A}$ be a perfect array of size $m \times n$ over the basic quaternions, where $mn = \frac{p+1}{2}$, we inflate the perfect array $\boldsymbol{A}$, as follows:*

1. *Take a Legendre sequence $\boldsymbol{L}_p = (0, s_1, \ldots, s_{p-1})$ of length $p$ and replace the element $0$ by $i^{\frac{p+1}{2}}$, to obtain the sequence $\boldsymbol{S}_i = (i^{\frac{p+1}{2}}, s_1, \ldots, s_{p-1})$. Since $p \equiv 3 \ (mod 4)$, we have $i^{\frac{p+1}{2}}$ is either 1 or -1, producing the binary sequence $\boldsymbol{S}_i = (\pm 1, s_1, \ldots, s_{p-1})$. The autocorrelation of the sequence $\boldsymbol{S}_i$ is $(p, -1, \ldots, -1)$.*
2. *Produce $p+1$ arrays, $\boldsymbol{B}_0, \boldsymbol{B}_1, \ldots, \boldsymbol{B}_p$, from the sequence $\boldsymbol{S}_i$, as in Construction (8.1). These arrays are all binary arrays.*
3. *Construct $\frac{p+1}{2}$ inflation arrays of size $p \times p$: for $r = 0, 1, \ldots, \frac{p-1}{2}$, and put*

$$\boldsymbol{C}_r = \left(\frac{1+i}{2}\right)(\boldsymbol{B}_{2r} + i\boldsymbol{B}_{2r+1}). \tag{8.49}$$

   *All the coefficients of this matrix are complex fourth roots of unity. In Equation (8.49), we can replace the quaternion i by the quaternion j or k and the construction is still valid. The arrays $\boldsymbol{C}_0, \boldsymbol{C}_1, \ldots, \boldsymbol{C}_{\frac{p-1}{2}}$ satisfy the conditions of the inflation arrays stated in Construction (8.1).*

4. *Arrange the arrays $\boldsymbol{A}, \boldsymbol{C}_0, \boldsymbol{C}_1, \ldots, \boldsymbol{C}_{\frac{p-1}{2}}$ into a four-dimensional array $\boldsymbol{D}$ of size $m \times p \times p \times n$ as follows: if $c_{r+ms}(u, v)$ is the $(u, v)$ entry of the inflation array $\boldsymbol{D}_{r+ms}$, then for $0 \le r \le m-1$, $0 \le s \le n-1$ and $0 \le u, v \le p-1$, we have*

$$d(r, u, v, s) = a(r, s)c_{r+ms}(u, v). \tag{8.50}$$

5. *Reduce the dimension of the array $\boldsymbol{D}$, without reducing the number of entries, into a two-dimensional array $\boldsymbol{E} = (d(r, s))$ of size $mp \times np$, as follows: for $0 \le r \le mp-1$ and $0 \le s \le np-1$, the $(r, s)$ entry of the array $\boldsymbol{E}$ is*

$$e(r, s) = d(r \ (mod\ m), r \ (mod\ p), s \ (mod\ p), s \ (mod\ n)). \tag{8.51}$$

**Theorem 8.7.** *Every perfect array over the basic quaternions of size $m \times n$, where $p = 2mn - 1$ is a prime number and $p \equiv 3 \pmod 4$, can be inflated into a perfect array of size $mp \times np$, over the basic quaternions.*

*Proof.* Given a perfect array $\boldsymbol{A}$ over the basic quaternions of size $m \times n$, where $mn = \frac{p+1}{2}$, where $p$ is a prime number and $p \equiv 3 \pmod 4$, from Construction (8.4), we inflate the array $\boldsymbol{A}$ into an array $\boldsymbol{B}$ of size $mp \times np$. A proof of perfection of the array $\boldsymbol{B}$ is similar to the proof of Theorem (8.6). □

**Example 8.4.** *The perfect two-dimensional array*

$$\begin{pmatrix} 1 & i \\ j & -k \end{pmatrix} \tag{8.52}$$

*of size* $2 \times 2$ *is inflated into a perfect two-dimensional array of size* $14 \times 14$*. Since* $7 \equiv 3 \pmod 4$*, we construct* $8$ *binary inflation arrays of size* $7 \times 7$

$$\boldsymbol{B}_0 = \begin{pmatrix} 1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 \end{pmatrix} \quad \boldsymbol{B}_1 = \begin{pmatrix} 1 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & -1 & 1 & -1 \\ -1 & 1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & 1 & -1 & 1 & 1 & 1 & -1 \\ -1 & -1 & 1 & -1 & 1 & 1 & 1 \end{pmatrix}$$

$$\boldsymbol{B}_2 = \begin{pmatrix} 1 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 & -1 & 1 & -1 \\ -1 & -1 & 1 & -1 & 1 & 1 & 1 \\ -1 & 1 & 1 & 1 & -1 & -1 & 1 \end{pmatrix} \quad \boldsymbol{B}_3 = \begin{pmatrix} 1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 1 \\ -1 & 1 & -1 & -1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & -1 & 1 \end{pmatrix} \tag{8.53}$$

$$\boldsymbol{B}_4 = \begin{pmatrix} 1 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 & 1 & -1 \\ 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & 1 & -1 & -1 & 1 \\ -1 & 1 & -1 & 1 & 1 & 1 & -1 \end{pmatrix} \quad \boldsymbol{B}_5 = \begin{pmatrix} 1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 1 \\ -1 & -1 & 1 & 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & -1 & 1 & 1 & 1 \end{pmatrix}$$

$$\boldsymbol{B}_6 = \begin{pmatrix} 1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 1 & -1 & 1 \\ -1 & 1 & 1 & 1 & -1 & 1 & -1 \end{pmatrix} \quad \boldsymbol{B}_7 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 \end{pmatrix} \tag{8.54}$$

*We use Equation (8.49) to produce* 4 *inflation arrays of size* 7 × 7

$$\boldsymbol{C}_0 = \begin{pmatrix} i & 1 & 1 & -1 & 1 & -1 & -1 \\ i & i & 1 & -i & i & -i & -1 \\ i & i & i & -i & 1 & -1 & -i \\ 1 & i & i & -1 & 1 & -i & -1 \\ i & 1 & i & -1 & i & -i & -i \\ 1 & i & 1 & -1 & i & -1 & -i \\ 1 & 1 & i & -i & i & -1 & -1 \end{pmatrix} \quad \boldsymbol{C}_1 = \begin{pmatrix} i & -1 & -1 & 1 & -1 & 1 & 1 \\ i & -i & i & 1 & 1 & -1 & -1 \\ i & 1 & -i & -1 & i & -1 & 1 \\ -i & i & -1 & i & 1 & i & -i \\ i & i & 1 & -1 & -i & 1 & -1 \\ -i & -1 & 1 & -i & i & i & i \\ -i & 1 & i & i & -1 & -i & i \end{pmatrix}$$

$$\boldsymbol{C}_2 = \begin{pmatrix} i & -1 & -1 & 1 & -1 & 1 & 1 \\ i & 1 & 1 & -1 & -1 & i & -i \\ i & -1 & 1 & i & 1 & -i & -1 \\ -i & -i & i & -1 & i & 1 & i \\ i & 1 & -1 & -i & 1 & -1 & i \\ -i & i & i & i & -i & -1 & 1 \\ -i & i & -i & 1 & i & i & -1 \end{pmatrix} \quad \boldsymbol{C}_3 = \begin{pmatrix} i & i & i & -1 & i & -1 & -1 \\ i & i & -1 & i & -1 & -1 & i \\ i & -1 & i & -1 & -1 & i & i \\ -i & 1 & -i & -i & 1 & 1 & 1 \\ i & -1 & -1 & i & i & i & -1 \\ -i & -i & 1 & 1 & 1 & -i & 1 \\ -i & 1 & 1 & 1 & -i & 1 & -i \end{pmatrix} \tag{8.55}$$

*We use arrays the* $\boldsymbol{C}_0$, $\boldsymbol{C}_1$, $\boldsymbol{C}_2$ *and* $\boldsymbol{C}_3$, *to produce the perfect array*

$$\begin{pmatrix}
i & -i & 1 & i & 1 & i & -1 & -1 & 1 & -i & -1 & -i & -1 & i \\
-k & j & -k & j & j & k & j & j & k & k & j & k & j & j \\
i & -i & i & -1 & 1 & 1 & -i & -1 & i & i & -i & i & -1 & -i \\
k & -k & j & j & j & -k & k & j & -k & j & -k & -k & -k & -k \\
i & i & i & 1 & i & -i & -i & -1 & 1 & -i & -1 & i & -i & -1 \\
k & j & j & -k & -k & j & -k & j & j & -k & k & -k & -k & -k \\
1 & -1 & i & i & i & -1 & -1 & 1 & 1 & 1 & -i & -1 & -1 & -i \\
-k & j & j & k & j & k & j & j & j & j & j & j & j & k \\
i & i & 1 & -i & i & -1 & -1 & -1 & i & i & -i & -i & -i & 1 \\
-k & k & k & k & -k & j & j & j & j & j & j & k & j & j \\
1 & 1 & i & -i & 1 & i & -1 & 1 & i & -1 & -1 & -1 & -i & -1 \\
-k & k & j & j & k & j & j & j & -k & k & j & j & j & k \\
1 & -1 & 1 & -1 & i & -i & -i & 1 & i & -1 & -1 & 1 & -1 & i \\
k & -k & -k & -k & j & -k & -k & j & j & -k & -k & j & k & j
\end{pmatrix} \tag{8.56}$$

*of size* 14 × 14 *and random appearance over the basic quaternions.*

We wrote the following code in *Mathematica* to implement Construction (8.4) and inflate arrays over the basic quaternions.

```
In[1]:= << Quaternions‘
In[2]:= i = Quaternion[0, 1, 0, 0]
Out[2]= Quaternion[0, 1, 0, 0]
In[3]:= j = Quaternion[0, 0, 1, 0]
Out[3]= Quaternion[0, 0, 1, 0]
In[4]:= k = Quaternion[0, 0, 0, 1]
Out[4]= Quaternion[0, 0, 0, 1]
```

```
In[5]:= ArasuQ1[A_, p_] :=
  (r = Dimensions[A][[1]]; s = Dimensions[A][[2]];
  If[PrimeQ[p], (c = Prepend[Delete[Table[JacobiSymbol
  [k - 1, p], {k, p}], 1], I^((p + 1)/2)]; L1 = Prepend[
  Table[Transpose[Table[RotateRight[c, j*(i - 1)], {i, p}]]
  ,{j, p}], Table[c, {i, p}]] ; L12 = Table[
  Quaternion[1/2, 1/2, 0, 0] ** (L1[[2*l - 1]] +
  Quaternion[0, 1, 0, 0] ** L1[[2*l]]), {l, 1, (p + 1)/2}];
  L2 = Table[A[[i, l]] ** L12[[(i - 1) + r*(l - 1) + 1, j,
  k]], {i, 1, r}, {j, 1, p}, {k, 1, p}, {l, 1, s}]; L3 =
  Table[L2[[Mod[i - 1, r] + 1, Mod[i - 1, p] + 1, Mod[j - 1
  , p] + 1, Mod[j - 1, s] + 1]], {i, r*p}, {j, s*p}]),
  Print["p is not a prime"]]);
```

## 8.5 Size reduction of arrays - Array of balances of a decimation of a perfect array

In this section, we generalise Theorem (7.1) (Perfection of a Sequence of Balances of Decimations of a Perfect Sequences) from sequences to arrays. We call this process "Size Reduction of a Perfect Array". We prove in this section that reducing the size of an array is a left inverse process of inflating an array.

**Theorem 8.8.** *Let $m$ and $n$ be two natural numbers, such that $m = m_1 m_2$ and $n = n_1 n_2$, with $m_1, m_2, n_1, n_2 \geq 2$. Let*

$$\boldsymbol{A} = \begin{pmatrix} a(0,0) & \dots & a(0,n-1) \\ \vdots & & \vdots \\ a(m-1,0) & \dots & a(m-1,n-1) \end{pmatrix} \tag{8.57}$$

*be a perfect two-dimensional array of size $m \times n$. The array $\boldsymbol{B} = (b(u,v))$, where $0 \leq u \leq m_2 - 1$, $0 \leq v \leq n_2 - 1$ and*

$$b(u,v) = \sum_{t=0}^{m_1-1} \sum_{s=0}^{n_1-1} a(m_2t + u, n_2s + v), \tag{8.58}$$

*of size $m_2 \times n_2$, is perfect.*

*Proof.* For any shift $(\alpha, \beta) \neq (0,0)$, we have

$$\begin{aligned}
&RAC_{\boldsymbol{B}}(\alpha,\beta) = \\
&\sum_{u=0}^{m_2-1} \sum_{v=0}^{n_2-1} b(u,v) b^*(u+\alpha, v+\beta) = \\
&\sum_{u=0}^{m_2-1} \sum_{v=0}^{n_2-1} \left( \left( \sum_{t_1=0}^{m_1-1} \sum_{s_1=0}^{n_1-1} a(m_2t_1 + u, n_2s_1 + v) \right) \left( \sum_{t_2=0}^{m_1-1} \sum_{s_2=0}^{n_1-1} a(m_2t_2 + u + \alpha, n_2s_2 + v + \beta) \right)^* \right) = \\
&\sum_{u=0}^{m_2-1} \sum_{v=0}^{n_2-1} \sum_{t_1=0}^{m_1-1} \sum_{s_1=0}^{n_1-1} \sum_{t_2=0}^{m_1-1} \sum_{s_2=0}^{n_1-1} a(m_2t_1 + u, n_2s_1 + v) a^*(m_2t_2 + u + \alpha, n_2s_2 + v + \beta) = \\
&\sum_{t_1=0}^{m_1-1} \sum_{t_2=0}^{m_1-1} \sum_{u=0}^{m_2-1} \sum_{s_1=0}^{n_1-1} \sum_{s_2=0}^{n_1-1} \sum_{v=0}^{n_2-1} a(m_2t_1 + u, n_2s_1 + v) a^*(m_2t_2 + u + \alpha, n_2s_2 + v + \beta) = \\
&\sum_{t_1=0}^{m_1-1} \sum_{x=0}^{m_1-1} \sum_{u=0}^{m_2-1} \sum_{s_1=0}^{n_1-1} \sum_{y=0}^{n_1-1} \sum_{v=0}^{n_2-1} a(m_2t_1 + u, n_2s_1 + v) a^*(m_2(t_1 + x) + u + \alpha, n_2(s_1 + y) + v + \beta) = \\
&\sum_{x=0}^{m_1-1} \sum_{y=0}^{n_1-1} \sum_{t_1=0}^{m_1-1} \sum_{u=0}^{m_2-1} \sum_{s_1=0}^{n_1-1} \sum_{v=0}^{n_2-1} a(m_2t_1 + u, n_2s_1 + v) a^*(m_2t_1 + u + (m_2x + \alpha), n_2s_1 + v + (n_2y + \beta)) = \\
&\sum_{x=0}^{m_1-1} \sum_{y=0}^{n_1-1} RAC_{\boldsymbol{A}}(m_2x + \alpha, n_2y + \beta).
\end{aligned} \tag{8.59}$$

Case 1. $\alpha \neq 0$. For $0 < \alpha \leq m_2 - 1$. We prove that $m_2x + \alpha \not\equiv 0 \ (mod\ m)$. Since $0 <$

$\alpha \leq m_2 - 1$, we have $0 < 1 \leq m_2 - \alpha$. Therefore, $m_2 - \alpha$ is positive, and so $m - (m_2 - \alpha) < m$. Now, we multiply the inequality $0 \leq x \leq m_1 - 1$ by $m_2$ and then we add $\alpha$, to obtain, $\alpha \leq xm_2 + \alpha \leq m_1 m_2 - m_2 + \alpha = m - (m_2 - \alpha)$. Now, since $o < \alpha$ and $m - (m_2 - \alpha) < m$, we have $0 < m - (m_2 - \alpha) < m$, that is, $m_2 x + \alpha \not\equiv 0 \ (mod\ m)$. Therefore $(m_2 x + \alpha, n_2 y + \beta) \neq (0,0)$. Since $A$ is a perfect array, then $\sum_{x=0}^{m_1-1} \sum_{y=0}^{n_1-1} RAC_{A}(m_2 x + \alpha, n_2 y + \beta) = 0$. Thus,

$$RAC_{B}(\alpha, \beta) = 0. \tag{8.60}$$

for all $(\alpha, \beta) \neq (0,0)$.

Case 2. $\alpha \neq 0$. Similar to Case 1.

As required. □

We wrote the following code in *Mathematica* to reduce the size of a perfect array:

```
In[1]:= << Quaternions'
In[2]:= i = Quaternion[0, 1, 0, 0]
Out[2]= Quaternion[0, 1, 0, 0]
In[3]:= j = Quaternion[0, 0, 1, 0]
Out[3]= Quaternion[0, 0, 1, 0]
In[4]:= k = Quaternion[0, 0, 0, 1]
Out[4]= Quaternion[0, 0, 0, 1]
In[1]:= << Quaternions'

In[5]:= Reductor2D[matrix_, d_, e_] :=
(m = Dimensions[matrix][[1]]/d; n = Dimensions[matrix][[2]]
/e;Table[Table[Sum[matrix[[j + i*m, k + l*n]],
{i, 0, d − 1}, {l, 0, e − 1}], {j,1, m}], {k, 1, n}])
```

**Example 8.5.** *By adding entries three apart, horizontally and vertically, the perfect array,*

$$\boldsymbol{A} = \begin{pmatrix} -1 & i & -1 & -i & 1 & -i \\ j & k & -j & k & -j & k \\ -1 & -i & -1 & -i & 1 & i \\ -j & -k & j & -k & -j & -k \\ -1 & -i & -1 & i & 1 & -i \\ -j & -k & -j & -k & j & -k \end{pmatrix} \tag{8.61}$$

*of size* $6 \times 6$*, is size reduced into a perfect array of size* $3 \times 3$*, over the alphabet* $\{\pm 1 \pm i \pm j \pm k\}$

$$\boldsymbol{B} = \begin{pmatrix} -1-i-j-k & 1+i-j-k & -1-i+j-k \\ -1+i+j+k & 1-i-j+k & -1-i-j+k \\ -1-i-j-k & 1-i+j-k & -1+i-j-k \end{pmatrix} \tag{8.62}$$

*By adding entries two apart, horizontally and vertically, the array* $\boldsymbol{A}$ *is also size reduced into an array of size* $2 \times 2$

$$\boldsymbol{C} = \begin{pmatrix} \text{-3} & \text{-3}i \\ \text{-3}j & \text{-3}k \end{pmatrix} \tag{8.63}$$

*which is equivalent to the array*

$$\boldsymbol{D} = \begin{pmatrix} 1 & i \\ j & k \end{pmatrix} \tag{8.64}$$

*In this case the deflation process preserved the original alphabet of the array* $\boldsymbol{A}$.

**Example 8.6.** *By adding entries seven apart, horizontally and vertically, the perfect array*

$$\boldsymbol{A} = \begin{pmatrix}
i & -1 & -1 & 1 & -1 & 1 & 1 & -i & -1 & -1 & 1 & -1 & 1 & 1 \\
i & i & -i & i & -1 & -1 & -i & i & 1 & -1 & -i & -1 & i & -1 \\
1 & -i & -1 & -i & -1 & -1 & i & i & -i & -i & i & i & 1 & 1 \\
-i & 1 & 1 & -i & i & 1 & -1 & -i & -i & -i & -1 & -i & 1 & 1 \\
1 & i & -i & -1 & -1 & 1 & i & i & -1 & -i & 1 & -i & i & -i \\
-i & -i & i & 1 & -i & -i & 1 & -i & 1 & -i & -1 & 1 & -1 & 1 \\
i & 1 & -i & -1 & -i & -i & i & -i & -1 & 1 & i & -1 & 1 & i \\
-i & 1 & -1 & -i & -1 & -i & 1 & -i & -1 & 1 & 1 & 1 & 1 & -i \\
1 & -i & -1 & 1 & -i & -i & 1 & i & -1 & i & i & -i & i & -1 \\
i & -1 & 1 & -1 & -i & -1 & -i & i & -1 & i & i & -1 & -i & i \\
i & 1 & -i & i & -1 & -1 & 1 & -i & -i & -1 & i & 1 & i & -i \\
i & -1 & -1 & -1 & 1 & i & i & i & -i & -1 & -i & i & -i & -1 \\
i & -1 & -1 & -i & -i & i & i & -i & -i & 1 & 1 & 1 & i & -1 \\
-i & -i & -i & 1 & 1 & 1 & -1 & -i & i & 1 & 1 & -i & -1 & -i
\end{pmatrix} \tag{8.65}$$

*of size* $14 \times 14$ *is size reduced into a perfect array of size* $2 \times 2$

$$\boldsymbol{B} = \begin{pmatrix} 7i & -7i \\ -7i & -7i \end{pmatrix} \tag{8.66}$$

*which is equivalent to the perfect array*

$$\boldsymbol{C} = \begin{pmatrix} -i & i \\ \\ i & i \end{pmatrix} \tag{8.67}$$

When we inflate a perfect array $\boldsymbol{A}$ of size $m \times n$ into an array $\boldsymbol{B}$ of size $mp \times np$, where $p$ a prime number, and then we reduce the array $\boldsymbol{B}$ into an array $\boldsymbol{C}$ of size $m \times n$, we have noticed that the arrays $\boldsymbol{A}$ and $\boldsymbol{C}$ are the same (up to multiplication by a constant). We can think of this process in terms of operators, as follows:

Let $In$ be the operator the inflates perfect arrays over the basic quaternions, and let $SR$ the operator that reduces the size of a perfect array over the quaternion. We have the following theorem relating these two operators.

**Theorem 8.9.** *Reducing the size of an array is a left inverse process of inflating an array, that is, if $\boldsymbol{A}$ is a perfect array over the basic quaternions as in Construction (8.3) or Construction ((8.4)), then $SR \circ In(\boldsymbol{A}) = SR(In(\boldsymbol{A})) = k\boldsymbol{A}$, where k is a constant.*

*Proof.* Let $\boldsymbol{A}$ be a perfect array of size $m \times n$, over the basic quaternions.

Case 1. Assume $p = mn - 1$ is a prime number. We use Construction (8.3) to inflate the array $\boldsymbol{A}$ into a perfect array $\boldsymbol{D}$ of size $mp \times np$, where

$$d(r,s) = c(r \ (mod \ m), r \ (mod \ p), s \ (mod \ p), s \ (mod \ n)), \tag{8.68}$$

as in Equation (8.31) and

$$c(r,u,v,s) = a(r,s)b_{r+ms}(u,v), \tag{8.69}$$

as in Equation (8.30).

We reduce the size $mp \times np$ of the perfect array $\boldsymbol{D}$ into a perfect array $\boldsymbol{E}$ of size $m \times n$, by adding the $p$-apart elements of $\boldsymbol{E}$, as follows, for $0 \leq r \leq m-1$ and $0 \leq s \leq n-1$, we have

$$e(r,s) = \sum_{u=0}^{p-1} \sum_{v=0}^{p-1} d(r+mu, s+nv). \tag{8.70}$$

We prove that the array $\boldsymbol{E}$ is a multiple of the array $\boldsymbol{A}$. We will prove that every entry $e(r,s)$ of the array $\boldsymbol{E}$ is $p(i^{\frac{p+1}{2}})$-times the entry $a(r,s)$ of the array $\boldsymbol{A}$. For $0 \leq r \leq m-1$ and $0 \leq s \leq n-1$, we have

$$e(r,s) = \sum_{u=0}^{p-1} \sum_{v=0}^{p-1} d(r+mu, s+nv). \tag{8.71}$$

By Equation (8.31), we write Equation (8.71) as

$$\begin{aligned}
&\sum_{u=0}^{p-1} \sum_{v=0}^{p-1} d(r+mu, s+nv) = \\
&\sum_{u=0}^{p-1} \sum_{v=0}^{p-1} c((r+mu)\ (mod\ m), (r+mu)\ (mod\ p), (s+mv)\ (mod\ p), (s+nv)\ (mod\ n)) = \\
&\sum_{u=0}^{p-1} \sum_{v=0}^{p-1} c(r\ (mod\ m), (r+mu)\ (mod\ p), (s+mv)\ (mod\ p), s\ (mod\ n)).
\end{aligned} \tag{8.72}$$

By Equation (8.30), the last sum in Equation (8.72) is

$$\sum_{u=0}^{p-1} \sum_{v=0}^{p-1} a(r\ (mod\ m), s\ (mod\ n)) b_{r\ (mod\ m)+m(s\ (mod\ n)}((r+mu)\ (mod\ p), (s+mv)\ (mod\ p)). \tag{8.73}$$

Since $a(r,s)$ does not depend on $u$ and $v$, we write Equation (8.73) as follows

$$a(r\ (mod\ m), s\ (mod\ n)) \sum_{u=0}^{p-1} \sum_{v=0}^{p-1} b_{r+ms}((r+mu)\ (mod\ p), (s+mv)\ (mod\ p)). \tag{8.74}$$

For $0 \le u \le p-1$ and $0 \le v \le p-1$, the index $(r+mu)\ (mod\ p)$ takes each of the values $0, 1, \ldots, p-1$, once and only once, so we can use the index $x$, with $0 \le x \le p-1$. Similarly, the index $(s+mv)\ (mod\ p)$ takes each of the values $0, 1, \ldots, p-1$, once and only once, so we can use the index $y$, with $0 \le y \le p-1$, as follows

$$e(r,s) \quad = a(r,s) \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} b_{r\ (mod\ m)+m(s\ (mod\ n))}(x,y). \tag{8.75}$$

Now, the columns of the array $\boldsymbol{B}_{r+ms}$ are Legendre sequences, except for the zero term that has been converted into $i^{\frac{p+1}{2}}$. Since the sum of all non $i^{\frac{p+1}{2}}$ elements in a modified Legendre sequence is equal to zero, we have

$$e(r,s) \quad = a(r,s)p(i^{\frac{p+1}{2}}). \tag{8.76}$$

Case 2. Assume $p = 2mn - 1$ is a prime number. We use Construction (8.4) to inflate the array $\boldsymbol{A}$ into a perfect array $\boldsymbol{E}$ of size $mp \times np$, where

$$e(r,s) = d(r\ (mod\ m), r\ (mod\ p), s\ (mod\ p), s\ (mod\ n)), \tag{8.77}$$

as in Equation (8.51) and

$$d(r,u,v,s) = a(r,s)c_{r+ms}(u,v), \tag{8.78}$$

as in Equation (8.50) and

$$\boldsymbol{C}_r = \left(\frac{1+i}{2}\right)(\boldsymbol{B}_{2r} + i\boldsymbol{B}_{2r+1}), \tag{8.79}$$

as in Equation (8.49).

We reduce the size the perfect array $\boldsymbol{E}$ of size $mp \times np$ into a perfect array $\boldsymbol{F}$ of size $m \times n$, by adding the $p$-apart elements of $\boldsymbol{F}$, as follows, for $0 \leq r \leq m-1$ and $0 \leq s \leq n-1$, we have

$$f(r,s) = \sum_{u=0}^{p-1}\sum_{v=0}^{p-1} e(r+mu, s+nv). \tag{8.80}$$

We prove that the array $\boldsymbol{F}$ is a multiple of the array $\boldsymbol{A}$. We will prove that every entry $e(r,s)$ of the array $\boldsymbol{F}$ is $p(i^{\frac{p+3}{2}})$-times the entry $a(r,s)$ of the array $\boldsymbol{A}$. For $0 \leq r \leq m-1$ and $0 \leq s \leq n-1$, we have

$$f(r,s) = \sum_{u=0}^{p-1}\sum_{v=0}^{p-1} e(r+mu, s+nv). \tag{8.81}$$

By Equation (8.51), the right hand side term in Equation (8.81), becomes

$$\sum_{u=0}^{p-1}\sum_{v=0}^{p-1} c((r+mu)\ (mod\ m), (r+mu)\ (mod\ p), (s+mv)\ (mod\ p), (s+nv)\ (mod\ n)) =$$

$$\sum_{u=0}^{p-1}\sum_{v=0}^{p-1} c(r\ (mod\ m), (r+mu)\ (mod\ p), (s+mv)\ (mod\ p), s\ (mod\ n)). \tag{8.82}$$

By Equation (8.50), the right hand side term in Equation (8.82), becomes

$$= \textstyle\sum_{u=0}^{p-1}\sum_{v=0}^{p-1} a(r\ (mod\ m), s\ (mod\ n))c_{r\ (mod\ m)+m(s\ (mod\ n)}((r+mu)\ (mod\ p), (s+mv)\ (mod\ p))$$

$$= \textstyle\sum_{u=0}^{p-1}\sum_{v=0}^{p-1} a(r\ (mod\ m), s\ (mod\ n))\left(\frac{1+i}{2}\right)\Big[b_{2(r+ms)}((r+mu)\ (mod\ p), (s+mv)\ (mod\ p))$$

$$+ib_{2(r+ms)+1}((r+mu)\ (mod\ p), (s+mv)\ (mod\ p))\Big]. \tag{8.83}$$

Since $a(r,s)$ does not depend on $u$ and $v$, Equation (8.83), becomes

$$a(r\ (mod\ m), s\ (mod\ n))\left(\frac{1+i}{2}\right)\Big[\textstyle\sum_{u=0}^{p-1}\sum_{v=0}^{p-1} b_{2(r+ms)}((r+mu)\ (mod\ p), (s+mv)\ (mod\ p))+$$

$$i\textstyle\sum_{u=0}^{p-1}\sum_{v=0}^{p-1} b_{2(r+ms)+1}((r+mu)\ (mod\ p), (s+mv)\ (mod\ p))\Big]. \tag{8.84}$$

For $0 \leq u \leq p-1$ and $0 \leq v \leq p-1$, the index $(r+mu)\ (mod\ p)$, in $\boldsymbol{B}_{2(r+ms)}$, takes each of the values $0, 1, \ldots, p-1$, once and only once, so we can use the index $x$, with $0 \leq x \leq p-1$. Similarly, the index $(s+mv)\ (mod\ p)$, in $\boldsymbol{B}_{2(r+ms)+1}$, takes each of the values $0, 1, \ldots, p-1$, once and only once, so we can use the index $y$, with $0 \leq y \leq p-1$, as follows

$$f(r,s) =$$

$$a(r\ (mod\ m), s\ (mod\ n))\left(\frac{1+i}{2}\right)\left[\sum_{x=0}^{p-1}\sum_{y=0}^{p-1} b_{2(r+ms)}(x,y) + i\sum_{x=0}^{p-1}\sum_{y=0}^{p-1} b_{2(r+ms)+1}(x,y)\right]. \tag{8.85}$$

Now, the columns of the arrays $\boldsymbol{B}_{2(r+ms)}$ and $\boldsymbol{B}_{2(r+ms)+1}$ are Legendre sequences, except for the zero term that has been converted into $i^{\frac{p+1}{2}}$. Since the sum of all non $i^{\frac{p+1}{2}}$ elements in a modified Legendre sequence is equal to zero, we have

$$\begin{aligned} e(r,s) &= a(r,s)\left(\tfrac{1+i}{2}\right)\left[p(i^{\frac{p+1}{2}}) + ip(i^{\frac{p+1}{2}})\right] \\ &= a(r,s)\tfrac{(1+i)}{2}p(i^{\frac{p+1}{2}})(1+i) = a(r,s)\tfrac{(1+i)^2}{2}p(i^{\frac{p+1}{2}}) \\ &= a(r,s)p(i^{\frac{p+3}{2}}). \end{aligned} \tag{8.86}$$

□

CHAPTER

# 9

# PERFECT ARRAYS OVER THE BASIC QUATERNIONS OF UNBOUNDED SIZES

IN this Chapter, we use the **Composition Construction Theorem**, due to Arasu and de Launey [4], to produce perfect arrays over the basic quaternions of other sizes. In particular, we construct arrays of sizes $(426) \times (426)$, $(1,490) \times (2,235)$, $(31,922) \times (47,883)$, $(154,617,126) \times (154,617,126)$ and $(9,923,845,510)$ $\times (14,885,768,265)$.

We also state and answer the key questions: are there perfect two-dimensional arrays of unbounded sizes over the basic quaternions $\{1,-1,i,-i,j,-j,k,-k\}$?

If so, can we produce these arrays with random occurrences of the elements $1, -1, i, -i, j, -j, k, -k$? In order to answer these two questions, we use the Construction (8.3), to inflate a family of sequences into perfect arrays over the basic quaternions. More specifically, we show that all modified Lee Sequences (in the sense of [10]) of length $m = p + 1 \equiv 2 \ (mod\ 4)$, where $p$ is a prime number, can be folded into a perfect two-dimensional array (with only one occurrence of the element $j$) of size $2 \times \frac{m}{2}$, with $GCD(2, \frac{m}{2}) = 1$. Then, each of these arrays can be inflated into a perfect array of size $2p \times \frac{m}{2}p$, with random occurrences of all the elements $1, -1, i, -i, j, -j, k, -k$.

## 9.1 Existence of some perfect arrays over the basic quaternions

The next theorem, due to Arasu and de Launey [4], explains how two sets of inflation arrays can be composed to produce a set of inflation arrays of larger size.

**Theorem 9.1** (Arasu and de Launey [4]). *If there are $m$ inflation arrays of order $u$ and $mu^2$ inflation arrays of order $v$ coprime to $u$, then there are $m$ inflation arrays of order $uv$.*

This result allows us to construct perfect arrays over the basic quaternions of other sizes.

**Theorem 9.2.** *There are perfect arrays over the basic quaternions of sizes* $426 \times 426$, $(1,490) \times (2,235)$, $(31,922) \times (47,883)$, $(154,617,126) \times (154,617,126)$ *and* $(9,923,845,510) \times (14,885,768,265)$.

*Proof.* 1. Existence of a perfect array of size 426 × 426: the perfect array

$$A = \begin{pmatrix} 1 & \mathrm{i} \\ \mathrm{j} & \mathrm{k} \end{pmatrix} \tag{9.1}$$

of size 2 × 2, in Example (8.3), was inflated, by Construction (8.3), into a perfect array over the basic quaternions of size 6 × 6, with 36 entries. Since $p = 2(36) - 1 = 71$ is a prime number and $71 \equiv 3\ (mod 4)$, from Construction (8.4), we produce a perfect array over the basic quaternions of size $(6 \cdot 71) \times (6 \cdot 71) = 426 \times 426$ and $181,475$ entries.

2. Existence of a perfect array of size $(154,617,126) \times (154,617,126)$: Since $p = 2(181,475) - 1 = 362,951$ is a prime number and $362,951 \equiv 3\ (mod\ 4)$, we use Construction (8.4) to produce a perfect array over the basic quaternions of size $(426 \cdot 362,951) \times (426 \cdot 362,951) = (154,617,126) \times (154,617,126)$.

3. Existence of a perfect array of size $(31,922) \times (47,883)$: the perfect array

$$\begin{pmatrix} j & 1 & 1 \\ -i & i & i \end{pmatrix} \tag{9.2}$$

of size 2 × 3, is inflated, by Construction (8.3), into a perfect array over the basic quaternions of size 10 × 15, with 150 entries. Since $p = 150 - 1 = 149$ is a prime number, we use Construction (8.3) to produce a perfect array over the basic quaternions of size $(1,490) \times (2,235)$ and $3,330,150$ entries.

4. Existence of a perfect array of size $(9,923,845,510) \times (14,885,768,265)$: Since $p = 2(3,330,150) - 1 = 6,660,299$ is a prime number and $6,660,299 \equiv 3\ (mod\ 4)$, we use Construction (8.4), to produce a perfect array over the basic quaternions

of size $(1,490 \cdot 6,660,299) \times (2,235 \cdot 6,660,299) = (9,923,845,510) \times (14,885,768, 265)$.

5. Existence of a perfect array size $(31,922) \times (47,883)$: Since $p = 2(6) - 1 = 11$ is prime number and $11 \equiv 3\ (mod\ 4)$, the perfect array

$$\begin{pmatrix} j & 1 & 1 \\ \\ -i & i & i \end{pmatrix} \tag{9.3}$$

of size 2 × 3, can be inflated into a perfect array over the basic quaternions of size 22 × 33 and 726 entries. Now, since $q = 2(726) - 1 = 1,451$ is a prime number and $1451 \equiv 3\ (mod\ 4)$, we use Construction (8.4), to produce a perfect array over the basic quaternions of size $(22 \cdot 1,451) \times (33 \cdot 1,451) = (31,922) \times (47,883)$. □

## 9.2 From Lee sequences to an infinite family of inflated perfect arrays over the basic quaternions

We construct a family of inflated perfect arrays over the basic quaternions from a family of Lee Sequences. Lee Sequences of length $m = p + 1 \equiv 2\ (mod\ 4)$, where $p$ is a prime number, can be folded into arrays of size $n \times 2$, with $m = 2n$ and $GCD(n, 2) = 1$. These arrays meet the conditions of Theorem (8.4), and so they can be inflated into perfect arrays of sizes $np \times 2p$.

**Theorem 9.3.** *There exist perfect arrays over the basic quaternions of unbounded sizes.*

*Proof.* From Theorem (5.2), we know that there exist Lee sequences of unbounded lengths, namely for lengths $m = p + 1 \equiv 2\ (mod\ 4)$, for $p$ a prime number. Now, by Theorem (6.4), each of these sequences is converted into a same-length perfect sequence over the basic quaternions by changing zero to $j$. Then, each of these altered sequences is folded diagonally into a perfect two dimensional array of size $n \times 2$, with $m = 2n$ and $GCD(n, 2) = 1$. Now, since $GCD(n, 2) = 1$ and $p$ is a prime number, each of these arrays can be inflated into a perfect array of size $np \times 2p$ by Theorem (8.4). □

**Example 9.1.** *The modified Lee sequence $\boldsymbol{S} = (j, i, 1, -i, 1, i)$ is folded into a perfect array of size $3 \times 2$, namely*

$$\boldsymbol{B} = \begin{pmatrix} j & 1 & 1 \\ \\ -i & i & i \end{pmatrix} \tag{9.4}$$

*This array is inflated into a perfect array of size $15 \times 10$, namely*

$$\boldsymbol{C} = \begin{pmatrix} -i & -1 & -1 & j & -1 & -k & j & 1 & -1 & j & -k & 1 & j & 1 & 1 \\ -i & -i & i & i & i & i & j & j & i & i & i & i & -i & -i & i \\ -i & -k & 1 & j & 1 & -1 & j & -1 & -k & j & -1 & -1 & j & 1 & 1 \\ i & j & -i & j & i & -i & i & -i & -i & -i & -i & -i & -i & i & -i \\ -i & -1 & 1 & j & 1 & 1 & j & -k & -1 & j & 1 & -k & j & -1 & -1 \\ j & -i & j & i & -i & j & -i & i & j & -i & j & j & i & i & j \\ -i & 1 & -1 & j & -1 & 1 & j & -1 & 1 & j & 1 & -1 & j & -k & -k \\ i & i & -i & -i & j & -i & -i & i & -i & i & -i & -i & j & -i & -i \\ -i & 1 & -k & j & -k & -1 & j & 1 & 1 & j & -1 & 1 & j & -1 & -1 \\ -i & i & i & -i & -i & i & i & -i & i & j & i & i & i & j & i \end{pmatrix} \tag{9.5}$$

## 9.3 Inflation of folded modified Lee sequences of length $n = \frac{p+1}{2}$

When a modified Lee sequence of length $n$ satisfies the conditions of Construction (8.4), that is, $n = \frac{p+1}{2}$, for $p$ a prime number and $p \equiv 3 \ (mod\ 4)$, we fold this sequence into an array of size $\frac{n}{2} \times 2$ and then we inflate this array, into a perfect array of size $\frac{n}{2}p \times 2p$, over the basic quaternions by Construction (8.4). And so, we have the following theorem.

**Theorem 9.4.** *If $\boldsymbol{S}$ is a modified Lee sequence of length $n$, where $n = \frac{p+1}{2}$, with $p$ a prime number and $p \equiv 3 \ (mod\ 4)$, then, there exists a perfect array of size $\frac{n}{2}p \times 2p$, over the basic quaternions.*

**Example 9.2.** *The modified Lee sequence $\boldsymbol{S} = (j, i, 1, -i, 1, i)$ is folded into the perfect array*

$$\boldsymbol{A} = \begin{pmatrix} j & 1 & 1 \\ -i & i & i \end{pmatrix}^T \tag{9.6}$$

*of size $2 \times 3$, which can be inflated into a perfect array of size $33 \times 22$. Since $11 \equiv 3 \ (mod\ 4)$ and $\frac{11-1}{2} = 2 \times 3$, there are $6$ inflation arrays of size $11 \times 11$. We use Construction (8.4) to produce the perfect array of size $33 \times 22$. See next page.*

$$\begin{pmatrix}
k & 1 & k & 1 & j & 1 & k & -1 & k & 1 & k & -1 & j & -1 & j & 1 & j & -1 & k & -1 & j & -1 \\
-i & -i & 1 & 1 & -i & -i & -1 & i & i & i & -1 & -1 & -i & 1 & -1 & i & 1 & 1 & 1 & -i & i & -1 \\
-1 & -1 & -i & -1 & -i & -i & 1 & i & i & -i & i & 1 & -1 & i & 1 & -i & -1 & 1 & -i & 1 & 1 & i \\
j & i & j & i & -k & -1 & -k & 1 & -k & -i & j & -i & -k & i & j & -i & j & -1 & -k & -1 & j & 1 \\
-i & 1 & -1 & i & -i & i & 1 & -1 & 1 & -i & i & -1 & -1 & 1 & i & -i & -i & i & -1 & 1 & 1 & -i \\
1 & -i & -1 & -i & -1 & -i & -1 & i & 1 & -1 & i & i & 1 & 1 & -i & -1 & i & 1 & -i & 1 & -i & i \\
j & i & k & -1 & j & 1 & k & -1 & k & -1 & j & i & k & -i & k & -i & k & -i & j & i & j & 1 \\
i & i & -i & -1 & 1 & 1 & -1 & i & -i & -i & 1 & 1 & -i & i & -1 & 1 & -1 & -i & i & -i & 1 & -1 \\
-1 & -1 & 1 & -i & -1 & -i & -i & i & -i & -i & i & 1 & 1 & 1 & 1 & -1 & -i & i & i & i & -1 & 1 \\
j & -i & -k & i & j & -i & j & -1 & j & i & -k & -i & -k & -1 & -k & -1 & j & i & -k & 1 & j & 1 \\
i & 1 & -i & i & -1 & -i & -i & -i & 1 & -1 & i & 1 & 1 & -i & -i & 1 & 1 & i & -1 & -1 & -1 & i \\
-i & -1 & -i & -1 & i & -1 & -i & 1 & -i & -1 & -i & 1 & i & 1 & i & -1 & i & 1 & -i & 1 & i & 1 \\
j & i & -k & -i & -k & -i & -k & 1 & j & -1 & -k & -i & j & -1 & j & i & -k & 1 & j & i & j & -1 \\
i & -i & i & 1 & -1 & i & 1 & -i & -1 & 1 & -i & 1 & 1 & i & -1 & -1 & -i & -1 & -i & -i & 1 & i \\
1 & -1 & -i & -i & -i & -i & i & 1 & -1 & -1 & -1 & i & -i & i & i & -i & 1 & i & 1 & 1 & -1 & 1 \\
j & -i & -k & -1 & j & i & j & -1 & -k & -i & j & -i & j & 1 & j & i & -k & 1 & -k & -1 & -k & i \\
-i & i & 1 & -i & -1 & -i & -1 & -i & -1 & i & 1 & -1 & i & i & 1 & 1 & -i & -1 & i & 1 & -i & 1 \\
-1 & -i & i & -1 & -1 & -i & -i & 1 & i & -1 & -i & 1 & -i & 1 & -1 & -i & 1 & i & 1 & i & 1 & i \\
j & -i & k & i & k & -1 & k & -i & j & -1 & j & i & j & i & k & 1 & j & -i & k & 1 & k & -1 \\
i & 1 & 1 & 1 & 1 & -1 & -i & i & i & i & -1 & 1 & -1 & -1 & 1 & -i & -1 & -i & -i & i & -i & -i \\
1 & -i & -1 & -1 & 1 & -1 & -i & i & -1 & -i & 1 & i & -i & 1 & -i & -i & -1 & i & i & 1 & i & 1 \\
j & 1 & j & -i & j & -1 & k & -i & j & i & k & i & k & 1 & j & -1 & k & i & k & -1 & k & -i \\
-i & -1 & -i & -1 & i & -1 & -i & 1 & -i & -1 & -i & 1 & i & 1 & i & -1 & i & 1 & -i & 1 & i & 1 \\
1 & -i & i & -1 & -i & -i & 1 & 1 & -i & -i & -1 & i & i & i & -1 & -1 & -i & 1 & -1 & i & 1 & 1 \\
j & -1 & k & -1 & k & -i & j & 1 & k & 1 & k & i & k & -i & j & i & j & -1 & j & -i & k & i \\
-i & i & i & -i & 1 & i & 1 & 1 & -1 & 1 & 1 & -1 & -i & -i & -i & -i & i & 1 & -1 & -1 & -1 & i \\
1 & -1 & 1 & -i & i & -1 & -1 & 1 & i & -i & -i & i & -1 & 1 & 1 & -i & -i & 1 & -1 & i & -i & i \\
j & -1 & j & -i & j & i & -k & i & -k & i & -k & -i & j & 1 & -k & -i & j & -1 & j & 1 & -k & -1 \\
i & -1 & -1 & -i & -i & 1 & i & -1 & -i & 1 & -i & 1 & -1 & -i & 1 & i & 1 & i & 1 & i & -1 & -i \\
-1 & -i & i & -i & 1 & -1 & i & i & -i & -1 & 1 & 1 & -1 & i & -i & -i & 1 & 1 & -i & i & -1 & 1 \\
j & -1 & j & 1 & k & i & j & i & k & -i & k & i & j & -1 & k & -1 & k & 1 & k & -i & j & -i \\
-i & -i & -1 & i & i & 1 & i & 1 & 1 & -i & -1 & -1 & 1 & -1 & -i & i & -1 & -i & 1 & i & -i & 1 \\
-1 & -i & -i & -i & 1 & -1 & i & 1 & 1 & -i & -i & 1 & 1 & i & -1 & -1 & -1 & i & i & 1 & -i & i
\end{pmatrix}$$

CHAPTER

# 10

# PERFECT *M*-DIMENSIONAL ARRAYS WITH A RECURSIVE AUTOCORRELATION FUNCTION

ANTWEILER et al [2] showed that the kronecker product of a perfect sequence with a two-dimensional aperiodic perfect array is also a perfect array. Using this idea, they showed that perfect three and higher dimensional arrays can be produced. Following on from their work, we construct new arrays by combining a finite sequence $S$ of length $n_0$ with specially selected shifts of a finite $(m-1)$-dimensional array $\boldsymbol{A}$ of size $n_1 \times \cdots \times n_{m-1}$, in particular, we modify the construction in [2] by (1) using a new shift of $\boldsymbol{A}$ for each multiplication by an element of $S$ and (2) with not necessarily all shifts of $A$ involved. The autocorrelation function of the new $m$-dimensional array is the product of the autocorrelation functions of the sequence $S$ and the array $\boldsymbol{A}$. So, if the seed sequence and array have perfect autocorrelation, then the newly constructed array also has perfect autocorrelation. We generalise our construction to the use of any sequence whose length is any multiple of $LCM(\frac{n_1}{d_1}, \dots, \frac{n_{m-1}}{d_{m-1}})$, where each $d_i$ is any chosen divisor of $n_i$ ( in the case, where each $d_i = n_i$, the diagonal construction is obtained). There need be no bound on the length of the seed sequence, since, while there is very likely to be a bound of $n^2$ on the length of perfect sequences over the $n$-roots of unity, there also exist several types of sequences over real numbers, complex numbers, and recently quaternions, which are perfect and of unbounded lengths. There are also arrays, over 4 roots of unity, of unbounded sizes, constructed by Arasu and de Launey [4], that can be used in our construction. A generalisation in a different direction is given by S. Blake et al in [15] (to appear). In that construction, they generalise the construction of Antweiler et al in [2] by rotating a number of columns at a time, rather than a single column.

## 10.1 Multi-dimensional arrays

We recall the basic definitions regarding multi-dimensional arrays. Given a **finite m-dimensional array** $\boldsymbol{A} = \{a(i_0, i_1, \dots, i_{m-1})\}$, where $0 \leq i_j \leq n_j - 1$ and $0 \leq j \leq m-1$, over an alphabet $\mathcal{A}$, the **shift** of the array $\boldsymbol{A}$ by the $m$-tuple $(j_0, j_1, \dots, j_{m-1})$ is $\boldsymbol{A}^{(j_0, j_1, \dots, j_{m-1})} = \{a(i_0 + j_0, i_1 + j_1, \dots, i_{m-1} + j_{m-1})\}$, where indices are calculated modulo $n_j$, for $0 \leq j \leq m-1$. The **periodic** $(j_0, j_1, \dots, j_{m-1})$**-autocorrelation value** of $\boldsymbol{A}$ is defined as follows:

$$AC_{\boldsymbol{A}}(j_0, j_1, \dots, j_{m-1}) = \sum_{i_0=0}^{n_0-1} \sum_{i_1=0}^{n_1-1} \cdots \sum_{i_{m-1}=0}^{n_{m-1}-1} a(i_0, i_1, \dots i_{m-1}) a^*(i_0 + j_0, i_1 + j_1, \dots, i_{m-1} + j_{m-1}), \tag{10.1}$$

where $(j_0, j_1 \dots, j_{m-1}) \in \mathbb{Z}_{n_0} \times \mathbb{Z}_{n_1} \times \dots, \times \mathbb{Z}_{n_{m-1}}$ and $Z_{n_i}$ denotes the group of integers under addition modulo $n_i$. The star means conjugation in those alphabets where it makes sense to conjugate. The function $AC_{\boldsymbol{A}}$ is called the autocorrelation function of $\boldsymbol{A}$.

The autocorrelation value $AC_{\boldsymbol{A}}(j_0, j_1, \dots, j_{m-1})$, that is, the inner product between the array $\boldsymbol{A}$ and the array $\boldsymbol{A}$ shifted by $(j_0, j_1, \dots, j_{m-1})$, is sometimes denoted by

$$\boldsymbol{A} \cdot \boldsymbol{A}^{(j_0, j_1, \dots, j_{m-1})}. \tag{10.2}$$

The autocorrelation value $AC_{\boldsymbol{A}}(0, \dots, 0)$ is called the **peak-value** and all the other autocorrelation values are called **off-peak values**. We say the array $\boldsymbol{A}$ has **constant off-peak autocorrelation**, if all the off-peak autocorrelation values of $\boldsymbol{A}$ are equal. In particular, we say the array $\boldsymbol{A}$ is **perfect**, if all the off-peak autocorrelation values of $\boldsymbol{A}$ are zero.

## 10.2 Orbit of a multi-dimensional array

**Definition 10.1.** *Orbit of an array.*
*Let $\boldsymbol{A} = \{a(i_0, i_1, \dots, i_{m-1})\}$ be a m-dimensional array, where $0 \leq i_j \leq n_j - 1$ and $0 \leq j \leq m-1$, over an alphabet $\mathcal{A}$. Given an m-tuple $P = (p_0, \dots, p_{m-1}) \in \mathbb{Z}_{n_0} \times \dots \times \mathbb{Z}_{n_{m-1}}$, the set*

$$\mathcal{O} = \{\boldsymbol{A}^{iP} | i = 0, 1, \dots\}, \tag{10.3}$$

*of all the shifts of $\boldsymbol{A}$ determined by $P$, is finite and is called an **orbit** of $\boldsymbol{A}$, where $\boldsymbol{A}^{0P} = \boldsymbol{A}$. The minimum value $n \neq 0$ for which $\boldsymbol{A}^{nP} = \boldsymbol{A}$, is called the **order** of the orbit $\mathcal{O}$. Henceforth, we will denote $iP$ also by $P_i$.*

In the following lemma, we present a formula to find the size of the orbit $\mathcal{O} =$

$\{A^{iP} | i = 0, 1, \dots\}$ of the array $A$.

**Lemma 10.1.** *Given a finite m-dimensional array $\{a(i_0, i_1, \dots, i_{m-1})\}$, where $0 \leq i_j \leq n_j - 1$ and $0 \leq j \leq m-1$, over the set $\mathcal{A}$, and the m-tuple $P = (p_0, \dots, p_{m-1}) \in \mathbb{Z}_{n_0} \times \cdots \times \mathbb{Z}_{n_{m-1}}$, then the order of the orbit $\mathcal{O} = \{A^{P_i} | i = 0, 1, \dots\}$, is the least common multiple of $r_0, \dots, r_{m-1}$, where $r_j$ is the order of $p_j$ in $\mathbb{Z}_{n_j}$, that is,*

$$|\mathcal{O}| = LCM(r_0, \dots, r_{m-1}). \tag{10.4}$$

*Proof.* The indices of the array $A$ can be understood as the $m$-tuples in the direct product $\mathbb{Z}_{n_0} \times \cdots \times \mathbb{Z}_{n_{m-1}}$. Then, finding the order of the orbit $\mathcal{O}$ is translated into finding the order of the subgroup $\langle (p_0, \dots, p_{m-1}) \rangle$ of the group $\mathbb{Z}_{n_0} \times \cdots \times \mathbb{Z}_{n_{m-1}}$ under component-wise addition, which is exactly $LCM(r_0, \dots, r_{m-1})$. □

## 10.3 Invariance property

As for a sequence, a property of finite arrays is the invariance of the autocorrelation values under any shift, that is, an array and all its shifts share the same autocorrelation values, as shown in the following lemma.

**Lemma 10.2.** *Let $A = \{a(i_0, \dots, i_{m-1})\}$ be an m-dimensional array, where $0 \leq i_j \leq n_j - 1$ and $0 \leq j \leq m-1$, over an alphabet $\mathcal{A}$. For any m-tuples $(j_0, j_1, \dots, j_{m-1})$ and $(k_0, k_1, \dots, k_{m-1}) \in \mathbb{Z}_{n_0} \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_{m-1}}$, we have*

$$AC_{A}(k_0, k_1, \dots, k_{m-1}) = AC_{A^{(j_0, j_1, \dots, j_{m-1})}}(k_0, k_1, \dots, k_{m-1}). \tag{10.5}$$

*Proof.* For the sake of simplicity, let $J$ and $K$ denote the $m$-tuples $(j_0, j_1, \dots, j_{m-1})$ and $(k_0, k_1, \dots, k_{m-1})$, respectively. Let $\sigma_{j_k} : \mathbb{Z}_{n_k} \to \mathbb{Z}_{n_k}$, be the bijection that sends

$i_k$ into $(i_k + j_k)\ mod(n_k)$ , that is,

$$i_k \mapsto (i_k + j_k)\ mod(n_k), \tag{10.6}$$

and let $\sigma_J : \mathbb{Z}_{n_0} \times \cdots \times \mathbb{Z}_{n_{m-1}} \to \mathbb{Z}_{n_0} \times \cdots \times \mathbb{Z}_{n_{m-1}}$ be the bijection that sends $(i_0, \ldots, i_{m-1})$ to $(\sigma_{j_0}(i_0), \ldots, \sigma_{j_{m-1}}(i_{m-1}))$, that is,

$$(i_0, \ldots, i_{m-1}) \mapsto (\sigma_{j_0}(i_0), \ldots, \sigma_{j_{m-1}}(i_{m-1})). \tag{10.7}$$

With this notation, the array $\boldsymbol{A}^J$ can be thought of as $\{a(\sigma_J(i_0, \ldots, i_{m-1}))\}$. Therefore

$$AC_{\boldsymbol{A}^J}(k_0, \ldots, k_{m-1}) = \sum_{i_0=0}^{n_0-1} \sum_{i_1=1}^{n_1-1} \cdots \sum_{i_{m-1}=0}^{n_{m-1}-1} a(\sigma_J(i_0, \ldots, i_{m-1}))\bar{a}(\sigma_K \circ \sigma_J(i_0, \ldots, i_{m-1})). \tag{10.8}$$

Since the bijection $\sigma_J$ ranges all over $\mathbb{Z}_{n_0} \times \cdots \times \mathbb{Z}_{n_{m-1}}$, we have

$$\begin{aligned} AC_{\boldsymbol{A}^J}(k_0, \ldots, k_{m-1}) &= \textstyle\sum_{i_0=0}^{n_0-1} \sum_{i_1=1}^{n_1-1} \cdots \sum_{i_{m-1}=0}^{n_{m-1}-1} a(i_0, \ldots, i_{m-1})\bar{a}(\sigma_K(i_0, \ldots, i_{m-1})) \\ &= AC_{\boldsymbol{A}}(k_0, k_1, \ldots, k_{m-1}). \end{aligned} \tag{10.9}$$

As required. □

## 10.4 Multi-dimensional arrays with a recursive autocorrelation function

In this section, we present a construction of $m$-dimensional arrays with recursive autocorrelation function. This construction takes an $(m-1)$-dimensional array $\boldsymbol{A}$ over any alphabet of complex numbers, an orbit of $\boldsymbol{A}$ of size $n_0$ and a sequence

$S$ of length $n_0$ over any alphabet of complex numbers, and we produce an $m$-dimensional array with a recursive autocorrelation function.

**Construction 10.1.**

*Let $\boldsymbol{A} = \{a(i_1, \ldots, i_{m-1})\}$ be an $(m-1)$-dimensional array over any alphabet of complex numbers $\mathcal{A}$, where $0 \leq i_k \leq n_k - 1$ and $1 \leq k \leq m-1$. Let*

$$\mathcal{O} = \{\boldsymbol{A}^{P_0}, \boldsymbol{A}^{P_1}, \ldots, \boldsymbol{A}^{P_{n_0-1}}\}, \tag{10.10}$$

*be the orbit of $\boldsymbol{A}$ of order, say $n_0$, where $P_i = iP$ and $P = (p_1, \ldots, p_{m-1}) \in \mathbb{Z}_{n_0} \times \cdots \times \mathbb{Z}_{n_{m-1}}$. Let $\boldsymbol{S} = \{s_0, \ldots, s_{n_0-1}\}$ be a sequence of length, say $n_0$, over any alphabet of complex numbers $\mathcal{S}$. We construct an $m$-dimensional array*

$$\boldsymbol{B} = \{b(i_0, \ldots, i_{m-1})\}, \tag{10.11}$$

*where $0 \leq i_j \leq n_j - 1$ for $0 \leq j \leq m-1$, from $\boldsymbol{A}$ and $S$ by using the orbit $\mathcal{O}$ of $\boldsymbol{A}$, as follows*

$$B = \left\{s_0\boldsymbol{A}^{P_0}, s_1\boldsymbol{A}^{P_1}, \ldots, s_{n_0-1}\boldsymbol{A}^{P_{n_0-1}}\right\}, \tag{10.12}$$

*where $P_i$ means $iP$, for $i = 0, \ldots, n_0 - 1$ and $\boldsymbol{A}^{P_0} = \boldsymbol{A}$.*

## 10.5 Shift of the newly constructed array $B$

We now describe a general shift of the newly constructed array $\boldsymbol{B}$, in preparation for calculating the autocorrelation value of $\boldsymbol{B}$ for that shift, in Theorem (10.1)

**Lemma 10.3.** *For each $m$-tuple $(j, k_1, k_2, \ldots, k_{m-1}) \in \mathbb{Z}_{n_0} \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_{m-1}}$ and $K = (k_1, \ldots, k_{m-1})$, the array $\boldsymbol{B}$ shifted by $(j, k_1, k_2, \ldots, k_{m-1})$ is*

$$\boldsymbol{B}^{(j,k_1,\ldots,k_{m-1})} = \left\{s_j\left(\boldsymbol{A}^{P_j}\right)^K, s_{j+1}\left(\boldsymbol{A}^{P_{j+1}}\right)^K, \ldots, s_{j+n-1}\left(\boldsymbol{A}^{P_{j+n-1}}\right)^K\right\}. \tag{10.13}$$

*Proof.* The array $\boldsymbol{B}$ in Equation (10.12) contains $n_0$ sub-arrays of dimension $(m-1)$, namely $s_0\boldsymbol{A}^{P_0}, s_1\boldsymbol{A}^{P_1}, \dots,$ and $s_{n_0-1}\boldsymbol{A}^{P_{n_0-1}}$. The number $j$ moves the position of the these $(m-1)$-dimensional sub-arrays within $B$, namely $s_j\boldsymbol{A}^{P_j}, s_{j+1}\boldsymbol{A}^{P_{j+1}}, \dots,$ and $s_{j+n_0-1}\boldsymbol{A}^{P_{j+n_0-1}}$. The tuple $(k_1, \dots, k_{m-1})$ shifts independently every $(m-1)$-dimensional sub-array, producing

$$s_j\left(\boldsymbol{A}^{P_j}\right)^K, s_{j+1}\left(\boldsymbol{A}^{P_{j+1}}\right)^K, \dots, s_{j+n-1}\left(\boldsymbol{A}^{P_{j+n-1}}\right)^K, \tag{10.14}$$

where the expression $s_l\left(\boldsymbol{A}^{P_l}\right)^K$ means: shift $\boldsymbol{A}$ by $P_l = l(p_1, \dots, p_{m-1})$, then by $K = (k_1, \dots, k_{m-1})$ and finally multiply it by the constant $s_l$, for $l = j, j+1, \dots, j+n-1$. □

## 10.6 Autocorrelation of the newly constructed array B

We now describe the autocorrelation function of the array $\boldsymbol{B}$, by a recursive formula.

**Theorem 10.1.** *For all $(j, k_1, k_2, \dots, k_{m-1}) \in \mathbb{Z}_{n_0} \times \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_{m-1}}$ and $P_j = jP$, the m-dimensional array $\boldsymbol{B}$ of Equation (10.12), has autocorrelation*

$$AC_{\boldsymbol{B}}(j, k_1, \dots k_{m-1}) = AC_{\boldsymbol{S}}(j)AC_{\boldsymbol{A}}((k_1, \dots, k_{n-1}) + P_j). \tag{10.15}$$

*Proof.* For the shift $(j, k_1, k_2, \dots, k_{m-1}) \in \mathbb{Z}_{n_0} \times \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_{m-1}}$, the $(j, k_1, \dots, k_{m-1})$-autocorrelation value, $AC_{\boldsymbol{B}}(j, k_1, \dots, k_{m-1})$, of $\boldsymbol{B}$ is computed as follows:

$$AC_{\boldsymbol{B}}(j,k_1,\ldots,k_{m-1}) = \boldsymbol{B}\cdot\boldsymbol{B}^{(j,k_1,\ldots,k_{m-1})}. \tag{10.16}$$

Now, from Lemma 10.2, Equation (10.16), becomes

$$\begin{gathered}
\left\{s_0\boldsymbol{A}^{P_0}, s_1\boldsymbol{A}^{P_1},\ldots,s_{n_0-1}\boldsymbol{A}^{P_{n_0-1}}\right\}\cdot\left\{s_j\left(\boldsymbol{A}^{P_j}\right)^K, s_{j+1}\left(\boldsymbol{A}^{P_{j+1}}\right)^K,\ldots,s_{j+n_0-1}\left(\boldsymbol{A}^{P_{j+n_0-1}}\right)^K\right\} = \\
\left\{s_0\boldsymbol{A}^{P_0}, s_1\boldsymbol{A}^{P_1},\ldots,s_{n_0-1}\boldsymbol{A}^{P_{n_0-1}}\right\}\cdot\left\{s_j\left(\boldsymbol{A}^{P_0}\right)^{P_j+K}, s_{j+1}\left(\boldsymbol{A}^{P_1}\right)^{P_j+K},\ldots,s_{j+n_0-1}\left(\boldsymbol{A}^{P_{n_0-1}}\right)^{P_j+K}\right\} = \\
s_0s_j^*\left[\boldsymbol{A}^{P_0}\cdot\left(\boldsymbol{A}^{P_0}\right)^{P_j+K}\right] + s_1s_{j+1}^*\left[\boldsymbol{A}^{P_1}\cdot\left(\boldsymbol{A}^{P_1}\right)^{P_j+K}\right] + \cdots + s_{n_0-1}s_{j+n_0-1}^*\left[\boldsymbol{A}^{P_{n_0-1}}\cdot\left(\boldsymbol{A}^{P_{n_0-1}}\right)^{P_j+K}\right].
\end{gathered} \tag{10.17}$$

From Lemma 10.3, Equation 10.17, becomes

$$\begin{gathered}
s_0s_j^*\left[\boldsymbol{A}^{P_0}\cdot\left(\boldsymbol{A}^{P_0}\right)^{P_j+K}\right] + s_1s_{j+1}^*\left[\boldsymbol{A}^{P_0}\cdot\left(\boldsymbol{A}^{P_0}\right)^{P_j+K}\right] + \cdots + s_{n_0-1}s_{j+n_0-1}^*\left[\boldsymbol{A}^{P_0}\cdot\left(\boldsymbol{A}^{P_0}\right)^{P_j+K}\right] = \\
\left(s_0s_j^* + s_1s_{1+j}^* + \cdots + s_{n_0-1}s_{j+n_0-1}^*\right)\left[\boldsymbol{A}^{P_0}\cdot\left(\boldsymbol{A}^{P_0}\right)^{P_j+K}\right] = \\
\left(s_0s_j^* + s_1s_{1+j}^* + \cdots + s_{n_0-1}s_{j+n_0-1}^*\right)\left[\boldsymbol{A}\cdot\boldsymbol{A}^{P_j+K}\right] = \\
AC_{\boldsymbol{S}}(j)AC_{\boldsymbol{A}}(K+P_j) = \\
AC_{\boldsymbol{S}}(j)AC_{\boldsymbol{A}}((k_1,\ldots,k_{m-1})+P_j).
\end{gathered} \tag{10.18}$$

As required. □

**Corollary 10.1.** *If the array **A** and sequence **S** in the construction are both perfect, then the m-dimensional array **B** of Equation (10.12) is also perfect.*

*Proof.* If $S$ and $\boldsymbol{A}$ are perfect, then it follows from Equation (10.15) that all the off-peak autocorrelation values of $\boldsymbol{B}$ are zero. □

In Construction (10.1), we have taken some selected shifts of $\boldsymbol{A}$ to produce the array $\boldsymbol{B}$, namely we have taken those shifts of $\boldsymbol{A}$ in the orbit $\mathcal{O}$. In particular, when $\boldsymbol{A}$ is also a sequence of length $n_0$, we use $P = n_0 - 1$ to produce the orbit $\mathcal{O} = \{\boldsymbol{A}, \boldsymbol{A}^{n_0-1}, \ldots, \boldsymbol{A}^2, \boldsymbol{A}^1\}$, and so, our construction includes the **folklore** or **diagonal construction** of product of sequences as in the following example.

**Example 10.1.** *We use the perfect sequence* $\boldsymbol{S} = (1, i, -1, i)$ *and* $P = 3$, *to get the four elements orbit* $\mathcal{O} = \{\boldsymbol{S}, \boldsymbol{S}^1, \boldsymbol{S}^2, \boldsymbol{S}^3\}$. *We use the perfect sequence* $\boldsymbol{U} = (1, 1, 1, -1)$ *and the orbit* $\mathcal{O}$ *to produce the perfect two-dimensional array*

$$A = \left( 1 \begin{pmatrix} 1 \\ i \\ -1 \\ i \end{pmatrix} \; 1 \begin{pmatrix} i \\ 1 \\ i \\ -1 \end{pmatrix} \; 1 \begin{pmatrix} -1 \\ i \\ 1 \\ i \end{pmatrix} \; -1 \begin{pmatrix} i \\ -1 \\ i \\ 1 \end{pmatrix} \right) = \begin{pmatrix} 1 & i & -1 & -i \\ i & 1 & i & 1 \\ -1 & i & 1 & -i \\ i & -1 & i & -1 \end{pmatrix} \tag{10.19}$$

A more general case is presented in the next example.

**Example 10.2.** *We use the perfect array*

$$\boldsymbol{A} = \begin{pmatrix} 1 & i & -1 & i \\ -i & -1 & i & -1 \end{pmatrix}^T \tag{10.20}$$

*and* $P = (3,1)$ *to obtain the size 4 orbit*

$$\begin{aligned} \mathcal{O} = \; & \{\boldsymbol{A}, \boldsymbol{A}^{(3,1)}, \boldsymbol{A}^{(0,2)}, \boldsymbol{A}^{(3,3)}\} \\ = \; & \left\{ \begin{pmatrix} 1 & -i \\ i & -1 \\ -1 & i \\ i & -1 \end{pmatrix}, \begin{pmatrix} -1 & i \\ -i & 1 \\ -1 & i \\ i & -1 \end{pmatrix}, \begin{pmatrix} -1 & i \\ i & -1 \\ 1 & -i \\ i & -1 \end{pmatrix}, \begin{pmatrix} -1 & i \\ i & -1 \\ -1 & i \\ -i & 1 \end{pmatrix} \right\} \end{aligned} \tag{10.21}$$

*of* $\boldsymbol{A}$*. Then, we use the perfect sequence* $S = \{1, i, -1, i\}$ *of length 4 and the size 4 orbit* $\mathcal{O}$ *in Equation (10.21) to produce the perfect* 3*-dimensional array* $\boldsymbol{B}$ *of size* $4 \times 4 \times 2$

$$\begin{aligned} \boldsymbol{B} = \; & \left( 1 \begin{pmatrix} 1 & -i \\ i & -1 \\ -1 & i \\ i & -1 \end{pmatrix}, i \begin{pmatrix} -1 & i \\ -i & 1 \\ -1 & i \\ i & -1 \end{pmatrix}, -1 \begin{pmatrix} -1 & i \\ i & -1 \\ 1 & -i \\ i & -1 \end{pmatrix}, i \begin{pmatrix} -1 & i \\ i & -1 \\ -1 & i \\ -i & 1 \end{pmatrix} \right) \\ = \; & \left( \begin{pmatrix} 1 & -i \\ i & -1 \\ -1 & i \\ i & -1 \end{pmatrix}, \begin{pmatrix} -i & -1 \\ 1 & i \\ -i & -1 \\ -1 & -i \end{pmatrix}, \begin{pmatrix} 1 & -i \\ -i & 1 \\ -1 & i \\ -i & 1 \end{pmatrix}, \begin{pmatrix} -i & -1 \\ -1 & -i \\ -i & -1 \\ 1 & i \end{pmatrix} \right) \end{aligned} \tag{10.22}$$

We now introduce a generalisation of our construction, which allows the length of $\boldsymbol{S}$ to be any multiple of the size of the orbit $\mathcal{O}$.

**Theorem 10.2.** *If the sequence $\boldsymbol{S}$ of length $n_0$ in our construction in Equation (10.12) is replaced by a sequence $\boldsymbol{T} = \{t_0, \ldots, t_{kn_0-1}\}$ of length $kn_0$, then for all $(j, k_1, k_2, \ldots, k_{m-1})$ in $\mathbb{Z}_{kn_0} \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_{m-1}}$, the m-dimensional array $\boldsymbol{B}$, equal to,*

$$\{t_0\boldsymbol{A}^{P_0}, \ldots, t_{n_0-1}\boldsymbol{A}^{P_{n_0-1}}, t_{n_0}\boldsymbol{A}^{P_0}, \ldots, t_{2n_0-1}\boldsymbol{A}^{P_{n_0-1}}, \ldots, t_{(k-1)n_0}\boldsymbol{A}^{P_0}, \ldots, t_{kn_0-1}\boldsymbol{A}^{P_{n_0-1}}\}, \tag{10.23}$$

*has autocorrelation*

$$AC_{\boldsymbol{B}}(j, k_1, \ldots k_{m-1}) = AC_{\boldsymbol{T}}(j) AC_{\boldsymbol{A}}((k_1, \ldots, k_{n-1}) + P_j). \tag{10.24}$$

We omit the proof since it is a replica of the proof of Theorem (10.1).

**Example 10.3.** *We use a perfect $6 \times 6$ array over 4 roots of unity, constructed by the algorithm of Arasu and de Launey in [4], namely*

$$\boldsymbol{A} = \begin{pmatrix} -1 & i & -1 & -i & -1 & -i \\ i & -1 & -i & 1 & -i & 1 \\ -1 & -i & -1 & i & -1 & -i \\ -i & -1 & -i & 1 & i & 1 \\ 1 & -i & 1 & -i & 1 & i \\ -i & -1 & i & 1 & -i & 1 \end{pmatrix} \tag{10.25}$$

*and the step $P = (3, 3)$ to produce the orbit*

$$\begin{aligned}\mathcal{O} = \ & \{\boldsymbol{A}, \boldsymbol{A}^{(3,3)}\} \\ = \ & \left\{ \begin{pmatrix} -1 & i & -1 & -i & -1 & -i \\ i & -1 & -i & 1 & -i & 1 \\ -1 & -i & -1 & i & -1 & -i \\ -i & -1 & -i & 1 & i & 1 \\ 1 & -i & 1 & -i & 1 & i \\ -i & -1 & i & 1 & -i & 1 \end{pmatrix}, \begin{pmatrix} 1 & i & 1 & -i & -1 & -i \\ -i & 1 & i & 1 & -i & 1 \\ 1 & -i & 1 & -i & -1 & i \\ -i & -1 & -i & -1 & i & -1 \\ 1 & -i & 1 & i & -1 & -i \\ i & -1 & -i & -1 & -i & -1 \end{pmatrix} \right\}\end{aligned} \tag{10.26}$$

*We now use the perfect sequence $(1, i, -1, i)$ and the orbit $\mathcal{O}$ twice, to produce the perfect $6 \times 6 \times 4$*

$$\boldsymbol{B} = \left( \begin{array}{c} \begin{pmatrix} -1 & i & -1 & -i & -1 & -i \\ i & -1 & -i & 1 & -i & 1 \\ -1 & -i & -1 & i & -1 & -i \\ -i & -1 & -i & 1 & i & 1 \\ 1 & -i & 1 & -i & 1 & i \\ -i & -1 & i & 1 & -i & 1 \end{pmatrix}, \begin{pmatrix} -i & -1 & -i & 1 & -i & 1 \\ 1 & i & -1 & i & 1 & -i \\ i & 1 & i & -1 & i & 1 \\ -1 & i & 1 & i & 1 & -i \\ -i & 1 & -i & 1 & -i & -1 \\ 1 & i & 1 & i & -1 & -i \end{pmatrix}, \\ \begin{pmatrix} 1 & -i & 1 & i & 1 & i \\ -i & 1 & i & -1 & i & -1 \\ 1 & i & 1 & -i & 1 & i \\ i & 1 & i & -1 & -i & -1 \\ -1 & i & -1 & i & -1 & -i \\ i & 1 & -i & -1 & i & -1 \end{pmatrix}, \begin{pmatrix} -i & -1 & -i & 1 & -i & 1 \\ 1 & i & -1 & i & 1 & -i \\ i & 1 & i & -1 & i & 1 \\ -1 & i & 1 & i & 1 & -i \\ -i & 1 & -i & 1 & -i & -1 \\ 1 & i & 1 & i & -1 & -i \end{pmatrix} \end{array} \right) \tag{10.27}$$

**Example 10.4.** *Let $w = \frac{1}{2} + \frac{i\sqrt{3}}{2}$, a sixth primitive root of unity. We use the perfect*

*2-dimensional array*

$$\boldsymbol{A} = \begin{pmatrix} 1 & w & 1 & -1 & w^4 & -1 \\ \\ 1 & 1 & w^2 & 1 & 1 & w^2 \end{pmatrix}^T \tag{10.28}$$

*and* $P = (3,1)$ *to produce the size 2 orbit*

$$\begin{aligned} \mathcal{O} = & \ \{\boldsymbol{A}, \boldsymbol{A}^{(3,1)}\} \\ = & \left\{ \begin{pmatrix} 1 & 1 \\ w & 1 \\ 1 & w^2 \\ -1 & 1 \\ w^4 & 1 \\ -1 & w^2 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & -w \\ w^2 & -1 \\ 1 & 1 \\ 1 & w \\ w^2 & 1 \end{pmatrix} \right\} \end{aligned} \tag{10.29}$$

*of* **A**. *Now, we use the perfect sequence* $\boldsymbol{T} = \{1, 1, 1, -1\}$ *of length 4 and the orbit* $\mathcal{O}$ *of size 2, to produce the perfect* 3*-dimensional array* **B** *of size* $4 \times 6 \times 2$, *namely*

$$\boldsymbol{B} = \left( \begin{pmatrix} 1 & 1 \\ w & 1 \\ 1 & w^2 \\ -1 & 1 \\ w^4 & 1 \\ -1 & w^2 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & -w \\ w^2 & -1 \\ 1 & 1 \\ 1 & w \\ w^2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ w & 1 \\ 1 & w^2 \\ -1 & 1 \\ w^4 & 1 \\ -1 & w^2 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & w \\ w^5 & 1 \\ -1 & -1 \\ -1 & w^4 \\ w^5 & -1 \end{pmatrix} \right) \tag{10.30}$$

*by repeating the orbit* $\mathcal{O}$ *and using Theorem (10.2).*

# CHAPTER 11

# CONCLUSION

IN this research we studied the existence of perfect sequences and arrays over complex numbers and quaternions. We answered the question posed by Kuznetsov and Hall: Are there perfect sequences of unbounded lengths over the double-tetrahedron group $\mathbb{H}_{24} = \{\pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2}\}$? The author and Hall worked on this problem and found a family of perfect sequences of **unbounded lengths** over $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. The author also posed and answered affirmatively the question: Are there perfect arrays of unbounded sizes over the group $\mathbb{H}_8$?

## 11.1 Summary of Contributions

In this research we

1. Proved the existence of infinitely many perfect sequences over the basic quaternions $\{\pm 1, \pm i, \pm j, \pm k\}$, namely for lengths $m = p^a + 1 \equiv 2 \ (mod\ 4)$, where $p$ is a prime number and $a > 0$. We also showed a construction to produce these sequecences.
2. Proved the existence of Infinitely many perfect sequences of odd length over the alphabets $\{\pm 1, \pm i, \frac{1 \pm i}{2}\}$ and $\{\pm 1 \pm i, j\}$, namely for lengths $\frac{m}{2}$, where $m = p^a + 1 \equiv 2 \ (mod\ 4)$, $p$ is a prime number and $a > 0$. We also showed a construction to produce these sequences.
3. Proved that every sequence $\boldsymbol{S}$ of even length $m = 2n$, with $n \in \mathbb{N}$, over the alphabet of complex numbers $\mathbb{C}$ and palindromic about the centres $a_0 = 0$ and $a_n$, can be converted into a sequence over the quaternions by changing $a_0 = 0$ to the basic quaternion $j$, preserving the off-peak values.
4. Proved that every sequence $\boldsymbol{S}$ of even length $m = 2n$, with $n \in \mathbb{N}$, over the alphabet of complex numbers $\mathbb{C}$ and palindromic about the centres $a_0 = 0$ and $a_n = 0$, can be converted into a sequence over the quaternions by changing $a_0 = 0$ and $a_n = 0$ to the basic quaternions $j$ and $k$, respectively, preserving the off-peak values.
5. Proved that every sequence $\boldsymbol{S}$ of even length $m = 2n + 1$, with $n \in \mathbb{N}$, over the alphabet of complex numbers $\mathbb{C}$ and palindromic about the centre $a_0 = 0$, can be converted into a sequence over the quaternions by changing $a_0 = 0$ to the basic quaternion $j$, preserving the off-peak values.
6. Proved that every sequence $\boldsymbol{S}$ of even length $m = 2n$, with $n \in \mathbb{N}$, over the alphabet $\{a + ib + jc \mid a, b, c \in \mathbb{R}\}$ and palindromic about the centres $s_0 = a_0 + b_0 i + c_0 j$ and $s_n$, can be converted into another sequence over the quaternions by changing $s_0$ to $s_0 + d_0 k$, with $d \in \mathbb{R}$, preserving the off-peak

values.

7. Proved that every sequence $S$ of odd length $m = 2n+1$, with $n \in \mathbb{N}$, over the alphabet $\{a + ib + jc \mid a, b, c \in \mathbb{R}\}$ and palindromic about the centre $s_0 = a_0 + b_0 i + c_0 j$, can be converted into a sequence over the quaternions by changing $s_0$ to $s_0 + dk$, with $d \in \mathbb{R}$, preserving the off-peak values.
8. Modified the Arasu and de Launey inflation of perfect quaternary arrays construction, for arrays of sizes $mn = p+1$, where $p$ is a prime number, to inflate perfect arrays over the basic quaternions of size $mn = p+1$, where $p$ is a prime number.
9. Modified the Arasu and de Launey inflation of perfect quaternary arrays construction, for arrays of sizes $mn = \frac{p+1}{2}$, where $p$ is a prime number and $p \equiv 3 \ (mod\ 4)$, to inflate perfect arrays over the basic quaternions of size $mn = \frac{p+1}{2}$, where $p$ is a prime number and $p \equiv 3 \ (mod\ 4)$.
10. Proved the existence of perfect arrays over the basic quaternions of sizes $426 \times 426$, $(1,490) \times (2,235)$, $(31,922) \times (47,883)$, $(154,617,126) \times (154,617,126)$ and $(9,923,845,510) \times (14,885,768,265)$.
11. Proved the existence of infinitely many perfect arrays over the basic quaternions, namely for sizes $2p \times np$, where $m = 2n = p+1 \equiv 2 \ (mod\ 4)$, and $p$ is a prime number. We also showed a construction to produce these arrays.
12. Constructed new arrays by combining a finite sequence $S$ of length $n_0$ with special selected shifts of a finite $(m-1)$-dimensional array $\boldsymbol{A}$ of size $n_1 \times \cdots \times n_{m-1}$ by (1) using a new shift of $\boldsymbol{A}$ for each multiplication by an element of $S$ and (2) with not necessarily all shifts of $\boldsymbol{A}$ involved. The autocorrelation function of the new $m$-dimensional array is the product of the autocorrelation functions of the sequence $S$ and the array $\boldsymbol{A}$. So, if the seed sequence and array have perfect autocorrelation, then the newly constructed array also has perfect autocorrelation.

13. Generalised our construction in 12, to the use of any sequence whose length is any multiple of $LCM(\frac{n_1}{d_1}, \ldots, \frac{n_{m-1}}{d_{m-1}})$, where each $d_i$ is any chosen divisor of $n_i$ ( in the case, where each $d_i = n_i$, the diagonal construction is obtained).

## 11.2 Future Research

For future research we will

1. Look for alternative constructions of perfect sequences and arrays over the basic quaternions that produce sequences and/or arrays of different sizes to those obtained in this research.
2. Study relative difference sets of quaternion groups in order to look for perfect arrays over the basic quaternions.

# BIBLIOGRAPHY

[1] W.O. Alltop. Complex sequences with low periodic correlations. *IEEE Trans. Inf. Theory (USA)*, Vol: IT-26:pp. 350 – 354, 1980.

[2] M. Antweiler, L. Bomer, and H. Luke. Perfect ternary arrays. *IEEE Transactions on Information Theory*, Vol. 36(3):pp 696–705, 1990.

[3] K.T. Arasu. Sequences and arrays with desirable correlation properties. *nformation Security, Coding Theory and Related Combinatorics*, pages 136–171, 2011.

[4] K.T. Arasu and W De Launey. Two-dimensional perfect quaternary arrays. *IEEE Transactions on Information Theory*, Vol. 47(4):pp 1482–1493, 2001.

[5] K.T. Arasu, W. De Launey, and S.L. Ma. On circulant complex hadamard matrices. *Des. Codes Cryptogr. (Netherlands)*, Vol. 25(2):pp 123 – 42, 2002/02/.

[6] K.T Arasu and J.F. Dillon. Perfect ternary arrays. *NATO Volume on Difference Sets, Sequences and their Correlation Properties*, pages pp 1–15, 1999.

[7] K.T. Arasu and S.L. Ma. Some new results on circulant weighing matrices. *J. Algebraic Combinatorics*, Vol. 14:pp. 641–650, 1997.

[8] B. Artmann. *The concept of number: from quaternions to monads and topological fields*. Halsted Press: a Division of John Willey and Sons, Chichester, 1988.

[9] S. Barrera Acevedo. Perfect $m$-dimensional arrays with a recursive autocorrelation function. *Preprint*, 2013.

[10] S. Barrera Acevedo and T. E. Hall. Perfect sequences of unbounded lengths over the basic quaternions. *Sequences and Their Applications - SETA 2012. Proceedings 7th International Conference*, pages 159–67, 2012.

[11] S. Barrera Acevedo and N. Jolly. Perfect arrays of unbounded size over the basic quaternions. *Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences*, 2013.

[12] L.D. Baumert. Cyclic difference sets. *Lectures Notes in Mathematics*, Vol. 182, 1971.

[13] V. Belevitch. Theory of 2n-terminal networks with applications to conference telephony. *Electrical Communication*, Vol. 27:pp. 231–244, 1950.

[14] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory, 2nd Edition*. Cambridge University Press, Cambridge, 1999.

[15] S.T. Blake, T.E. Hall, and A.Z. Tirkel. Arrays over the roots of unity with perfect autocorrelation and good zcz cross-correlation. *To appear*, 2013.

[16] L. Bomer and M. Antweiler. New perfect three-level and three-phase sequences. *IEEE Proceedings of International Symposium on Information Theory*, page 280, 1991.

[17] L. Bomer and M. Antweiler. Perfect n-phase sequences and arrays [spread spectrum communication]. *IEEE J. Sel. Areas Commun. (USA)*, Vol. 10(4):pp. 782 – 9, 1992/05/.

[18] S. Boztas. New lower bounds on the periodic crosscorrelation of qam codes with arbitrary energy. *Lecture Notes in Computer Science*, Vol. 1719:510–519, 1999.

[19] S. Boztas and U. Parampalli. Nonbinary sequences with perfect and nearly perfect autocorrelations. *IEEE Proceedings of International Symposium on Information Theory*, pages 1300–1304, 2012.

[20] J.A. Chang. Ternary sequence with zero correlation. *Proceedings of the IEEE*, Vol. 55(7):pp. 1211 – 1213, 1967/07/.

[21] Y.M. Chee, Y. Tan, and Y. Zhou. Almost p-ary perfect sequences. *Lectures Notes in Computer Science, Sequences and Their Applications, SETA 2010*, Vol. 6338:pp. 399–415, 201.

[22] D.C. Chu. Polyphase codes with good periodic correlation properties. *IEEE Transactions on Information Theory*, Vol. 18:pp. 531–532, 1972.

[23] H. Chung and P.V. Kumar. A new general construction for generalized bent functions. *IEEE Transactions on Information Theory*, Vol. 35(1):pp. 206–209, 1989.

[24] I.J. Cox and M.L. Miller. Electronic watermark: The first 50 years. *IEEE Fourth Workshop on Multimedia Signal Processing*, pages 225–230, 2001.

[25] M. Darnell and P.Z. Fan. Perfect sequences derived from m-sequences. *IEEE Proceedings of International Symposium on Information Theory*, page 461, 1995.

[26] S. De Leo and P. Rotelly. Quaternionic electroweak theroy. *Journal of Physics, G: Nuclear Particles Physics*, Vol. 22:pp. 1137–1150, 1996.

[27] P. Delsarte, J. M. Goethals, and J. J. Seidel. Orthogonal matrices with zero diagonal. *Canadian Journal of Mathematics*, Vol. 23:pp. 816?–832, 1971.

[28] J.F. Dillon. Some really beautiful hadamard matrices. *Cryptography Communications*, Vol. 2:pp. 271–291, 2010.

[29] P.Z. Fan and M. Darnell. The synthesis of perfect sequences. *Cryptography and Coding. 5th IMA Conference. Proceedings*, Vol. 1025:pp 63 – 73, 1995.

[30] R.L. Frank. Phase shift pulse codes with good periodic correlation properties (correspondence). *IRE Transactions on Information Theory*, Vol. 8:pp. 381–382, 1962.

[31] E.M. Gabidulin. Non-binary sequences with the perfect periodic autocorrelation and with optimal periodic cross-correlation. *Proceedings of the 1993 IEEE International Symposium on Information Theory*, Vol. 1:p. 412, 1993.

[32] E.M. Gabidulin. Partial classification of sequences with perfect autocorrelation and bent functions. *Proceedings 1995 IEEE International Symposium on Information Theory (Cat. No.95CH35738)*, page 467, 1995.

[33] E.M. Gabidulin and V.V. Shorin. New sequences with zero autocorrelation. *Probl. Inf. Transm. (Russia)*, Vol. 38(4):pp. 255 – 67, 2002/10/.

[34] P. Garg, G. Vijay Kumar and C. E. Veni Machavan. Two new families of low-correlation interleaved qam sequences. *Lectures notes in computer science*, Vol. 5203:pp. 130–141, 2008.

[35] T.E. Hall and A.Z. Tirkel. A unique watermark for every image. *IEEE Multimedia*, 8:pp. 30–37, 2001.

[36] J. Hammer and J.R. Seberry. Higher dimensional orthogonal designs and applications. *IEEE Transaction on Information Theory*, Vol. 26:pp. 772–779, 1981.

[37] R.C. Heimiller. Phase shift pulse codes with good periodic correlation properties. *IRE Transactions on Information Theory*, Vol. IT-7:pp. 254–257, 1961.

[38] T. Helleseth. Some results about the cross-correlation function between two maximal linear sequences. *Discrete Mathematics*, Vol. 16:pp. 209–232, 1961.

[39] T. Hoholdt and J. Justesen. Ternary sequences with perfect periodic autocorrelation. *IEEE Transactions on Information Theory*, Vol. 29:pp. 597–600, 1983.

[40] K.J. Horadam. *Hadamard Matrices and their Applications*. Princeton University Press, 1999.

[41] V.P. Ipatov. Ternary sequences with ideal autocorrelation properties. *Radio Engineering and Electronic Physics*, Vol. 24:pp. 75–79, 1979.

[42] J. Jedwab. Generalized perfect arrays and menon difference sets. *Des. Codes Cryptogr.*, Vol. 2:pp. 19–68, 1992.

[43] D. Jungnickel and A. Pott. *Difference sets: An introduction*, volume Vol. 542, Series C: Mathematical and Physical Studies, Difference Sets, Sequences and their Correlation Properties. Kluwer Academic Publisher, 1999.

[44] G.A. Koz, A. Triantafyllidis, and A. Aydin. Three-dimensional television: Capture, transmission, and display. In Levent Onura Haldun M. Ozaktas, editor, *3D watermarking: techniques and directions*, pages 427–470. Springer Verlag, 2007.

[45] O. Kuznetsov. Perfect sequences over the real quaternions. *IEEE Proceedings of the Fourth International Workshop on Signal Design and its Applications in Communications*, pages 17–20, 2009.

[46] O. Kuznetsov. *Perfect sequences over the real quaternions*. PhD thesis, Monash University, 2010.

[47] O. Kuznetsov and T. Hall. Perfect sequences over the real quaternions of longer length. *The Online Journal on Mathematics and Statistics. The 2010 World Congress on Mathematics and Statistics, WCMS 10*, Vol. 1:pp. 8–11, 2010.

[48] Serge Lang. *Algebra*. Addison-Wisley Pub. Co., 1993.

[49] C.M. Lee. Perfect q-ary sequences from multiplicative characters over gf(p). *Electronic Letters*, Vol. 28:pp 833–835, 1992.

[50] C.M. Lee. *On a new class of 5-ary sequences exhibiting ideal periodic autocorrelation properties with applications to spread spectrum system*. PhD thesis, Missisipi State University, 1998.

[51] B.L. Lewis and F.F. Kretschmer. Linear frequency modulation derived polyphase pulse compression codes. *IEEE Transactions on Aerospace and Electronic System*, Vol. AES-18(5):pp. 637–641, 1982.

[52] H. D. Luke, L. Bomer, M. Antweiler, and F.M. Markus. Perfect binary arrays. *Signal Processing*, Vol. 16:pp. 69–80, 1989.

[53] H.D. Luke. Sequences and arrays with perfect periodic correlation. *IEEE Trans. Aerosp. Electron. Syst. (USA)*, Vol. 24(3):pp. 287 – 94, 1988/05/.

[54] H.D. Luke. Btp transform and perfect sequences with small phase alphabet. *IEEE Trans. Aerosp. Electron. Syst. (USA)*, Vol. 32(3):pp. 497–499, 1996.

[55] H.D. Luke. Binary and quadriphase sequences with optimal autocorrelation properties: A survey. *IEEE Transactions on Information Theory*, Vol. 49(3):pp. 3271–3282, 2003.

[56] H.D. Luke. Cubical binary arrays with perfect odd-periodic autocorrelation. *Signal Processing*, Vol. 84:pp. 125–132, 2004.

[57] H.D. Luke and H. D. Schotten. Odd-perfect, almost binary correlation sequences. *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 31:495–498, 1995.

[58] S.L. Ma and W.S. Ng. On non-existence of perfect and nearly perfect sequences. *International Journal of Information and Coding Theory*, Vol. 1(1):pp. 15–38, 2009.

[59] F. J. MacWilliam and N. J. A. Sloane. Pseudo-random sequences and arrays. *Proceedings of IEEE*, Vol. 64:p.1715–1729, 1976.

[60] A. Milewski. Periodic sequence with optimal properties for channel estimation and fast start-up equalization. *IBM Journal of Research and Development*, Vol. 27(5):pp. 426–431, 1983.

[61] P.S. Moharir. Generalized pn sequences. *IEEE Transactions on Information Theory*, Vol. IT-23(6):pp. 782–784, 1977.

[62] W.H. Mow. *A study of correlation of sequences*. PhD thesis, University of Hong Kong, 1993.

[63] W.H. Mow. *Sequences design for spread spectrum*. PhD thesis, The Chinese University of Hong Kong Press, Sha Tin, Hong Kong, 1995.

[64] W.H. Mow. A unified construction of perfect polyphase sequences. *IEEE Proceedings of International Symposium on Information Theory*, page 459, 1995.

[65] J.S. Pan, H.C. Huang, and L.C. Jain. *Intelligent Watermarking Techniques*. World Scientific Publishing Company, Singapore, 2004.

[66] J. Salvi, J. Pages, and J. Batlle. Pattern codification strategies in structured light systems. *Pattern Recognition*, Vol. 37:pp. 827–849, 2004.

[67] D.V. Sarwate and M.B. Pursley. Crosscorrelation properties of pseudorandom and related sequences. *Proceedings of the IEEE*, Vol. 68:pp. 593–619, 1980.

[68] M.R. Schroeder. *Number Theory in Science and Communications, with applications to physics, digital information, computing, and self-similarity*. Springer, 2006.

[69] D.V. Shedd, D.A. Sarwate. Construction of sequences with good correlation properties. *IEEE Transactions on Information Theory*, Vol. IT-25(1), 1979.

[70] H. Stark and R. Naab. Application of optimum coding sequences to computerized classical tomography. *Applied Optics*, Vol. 17:pp. 3133–3137, 1978.

[71] D.N. Tompkins. Codes with zero correlation. *Hughes Aircraft Company, Calver City, California*, Technical Memo 651, 1960.

[72] B.L. Van der Waerden. Hamilton's discovery of quaternions. *Mathematics Magazine*, Vol. 49:pp. 227–234, 1976.

[73] A.L. Whiteman. A family of difference sets. *Illinois J. Math.*, Vol. 6:pp. 107–121, 1962.

[74] R.M. Young. When is $\mathbb{R}^n$ a field? *The Mathematical Gazette*, Vol. 72:128–129, 1988.

[75] N. Zhang and S.W. Golomb. Polyphase sequence with low autocorrelations. *IEEE Transactions on Information Theory*, Vol. 39:pp. 1085–1089, 1993.