Perfect Sequences over the Real Quaternions

Oleg Kuznetsov

This Thesis submitted in fulfillment of the requirements for the award of the degree

Doctor of Philosophy

School of Mathematical Sciences

Monash University

December 2010

Declaration

This Thesis contains no material that has been accepted for the award of any other degree in any University. To the best of my knowledge and belief, this Thesis contains no material previously published or written by any other person, except where due reference is given in the text.

Signed:

Date:

Copyright Notices

Notice 1

Under the Copyright Act 1968, this thesis must be used only under the normal conditions of scholarly fair dealing. In particular no results or conclusions should be extracted from it, nor should it be copied or closely paraphrased in whole or in part without the written consent of the author. Proper written acknowledgement should be made for any assistance obtained from this thesis.

Notice 2

I certify that I have made all reasonable efforts to secure copyright permissions for third-party content included in this thesis and have not knowingly added copyright content to my work without the owner's permission.

Acknowledgement

In preparation of this Thesis, I gratefully acknowledge the support and assistance provided by my supervisors, Dr T. E. Hall and Dr A. Z. Tirkel, for their encouragement, insightful comments and helpful suggestions.

Abstract

In this Thesis, perfect sequences over the real quaternions are first considered. Definitions for the right and left periodic autocorrelation functions are given, and right and left perfect sequences introduced. It is shown that the right (left) perfection of any sequence implies the left (right) perfection, so concepts of right and left perfect sequences over the real quaternions are equivalent. Unitary transformations of the quaternion space $\mathbb{H}$ are then considered. Using the equivalence of the right and left perfection, it is proved that unitary transformations of the quaternion space ‘respect’ perfection of a sequence. Consequently, any symmetry transformation of the alphabet preserves perfection of a sequence.

Properties of quaternionic perfect sequences are studied. It is shown that quaternionic perfect sequences share many properties in common with perfect sequences over the complex numbers. Similar to complex perfect sequences, perfection over quaternions is preserved by shifting of a perfect sequence, multiplication by a scalar, taking conjugates of each element of a perfect sequence, taking a proper decimation of a perfect sequence. However, unlike the complex case, multiplication of the elements of a perfect sequence of length n by consecutive powers of an n-root of unity destroys perfection, in general.

To construct long sequences, this Thesis extends the well-known result about composition of two perfect sequences over complex numbers, of relatively prime lengths, into the domain of real quaternions. We introduce a concept of composition of two or more sequences with elements in the real quaternion algebra $\mathbb{H}$. Using this generalization, we construct a perfect sequence of really impressive length, in order of a few billions, over a 24-element alphabet of quaternionic 12-roots of unity. Also, a new result on composition of two sequences of even lengths is presented, and an algorithm, based on the composition two sequences of even lengths, which renders longer perfect sequences, is given.

Conditions, necessary for perfection over quaternions, are studied. The Balance Theorem for the quaternions is proved, and a few generalizations of this theorem, which are also applicable to sequences over the complex numbers, are introduced.

The left and the right quaternionic discrete Fourier transforms are introduced. It is shown that, dissimilar to the complex case, the property of having all discrete Fourier transform coefficients of equal norms is a necessary, but not sufficient, condition for perfection over quaternions.

Many examples, illustrating new concepts and results, are given in this Thesis.

Table of Contents

1. Introduction

This work initiates the study of perfect sequences over the quaternions.

A perfect sequence is a sequence with ideal periodic autocorrelation function, namely, the periodic autocorrelation function with zero values for all out-of-phase shifts. The quaternions, discovered by Sir William Rowan Hamilton in the Century XIX, can be viewed as hyper-complex numbers, representing a linear combination of one real and three imaginary parts, $\boldsymbol{q} = q_0 + q_1\boldsymbol{i} + q_2\boldsymbol{j} + q_3\boldsymbol{k}$, with the fundamental relation $\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = \boldsymbol{ijk} = -1$.

Perfect sequences have many applications in communication systems. Traditionally, perfect sequences are considered over commutative alphabets, usually complex roots of unity, and these sequences have many applications in electronic communications.

Since complex numbers are special cases of the real quaternions, perfect sequences over the quaternions can be considered as a generalization of perfect sequences over the complex numbers. Understanding of the structure and properties of quaternionic perfect sequences may provide for better insight and advances in studying perfect sequences over the complex or real numbers. Currently, a development of the theory of perfect sequences over the quaternions is still in its incipient stage, and there is no instance of an advance in the theory of the complex or real perfect sequences by application of the more general concept of perfection over the quaternions. However, it is possible, and commonly happens in science, that generalizations produce greater understanding of the more particular instances of the theory.

A beautiful and simple description of unit spheres in the 3- and 4-dimension space is achieved by using the quaternions. Over the quaternions, the unit sphere in 3 dimensions is represented by the equation $S^2 = \{\boldsymbol{q} \in \mathbb{H} : \boldsymbol{q}^2 = -1\}$, and the unit sphere in 4 dimensions has the equation $S^3 = \{\boldsymbol{q} \in \mathbb{H} : \|\boldsymbol{q}\| = 1\}$. So, if, by some reason, we want to study sequences over points on the unit sphere in the 3- or 4-dimension space, the simplest approach would be to regard such sequences as the ones over unit quaternions.

Perfect sequences over the real quaternions may have potential applications in fiber optics communication systems, when attempts are made to make use of polarization properties of the light.

Constructing perfect sequences over the quaternions is the first step towards applications.

Perfect sequences over the real quaternions do exist. Three examples of different lengths, taken at random from a set of perfect sequences obtained by a computer search over the alphabet $\boldsymbol{Q}_8 = \{\pm 1, \pm\boldsymbol{i}, \pm\boldsymbol{j}, \pm\boldsymbol{k}\}$, are listed below:

$[\,\boldsymbol{k}, \boldsymbol{i}, \boldsymbol{k}, 1, -\boldsymbol{k}, 1\,]$,

$[\,-\boldsymbol{j}, \boldsymbol{k}, -\boldsymbol{j}, 1,\ \boldsymbol{j}, \boldsymbol{k}, \boldsymbol{j}, 1\,]$,

$[\,\boldsymbol{k}, -\boldsymbol{i}, -\boldsymbol{k}, \boldsymbol{i}, -\boldsymbol{k}, -\boldsymbol{i}, \boldsymbol{k}, -\boldsymbol{i}, 1, -\boldsymbol{i}\,]$.

Unlike the complex numbers, the quaternion algebra is not commutative. Non-commutativity of the quaternions calls for defining two different autocorrelation functions: right and left autocorrelation, which, in general, have non-equal values for the given sequence (an example is given in Section 2).

In sections which follow we define the right and left autocorrelation functions, and give corresponding definitions of the right and left perfect sequences.

The present work consists of 11 major sections.

- In Section 1, Introduction, a brief overview of the material that follows is given.
- In Section 2, Notations and Definitions, some general definitions, used in the following sections, are given, and notations, adopted throughout this work, are introduced.
- In Section 3, Algebra of Quaternions, we offer a brief historic review of the invention of the quaternions, introduce operations over the quaternions, and discuss some important properties of the quaternions.
- In Section 4, Perfect Sequences over the complex field ℂ, an attempt is made to reflect the most recent state of study on perfect sequences over the complex numbers. In this

section, the known constructions of sequences are presented, conditions for perfection are introduced, properties are discussed and the question of existence of perfect sequences over $\mathbb{C}$ is briefly considered.

Together, Sections 3 and 4 can be regarded as the literature review, providing for the background necessary for understanding of the material that follows.

- In Section 5, Equivalence of Right and Left Perfection over the Real Quaternions, the concepts of left and right perfection over the quaternions are introduced. It is proved that every right perfect sequence is also left perfect, and vice versa.

- In Section 6, Transformations Preserving Perfection over the Quaternions, properties of perfect sequences over the real quaternions are studied. Also, it is shown that any unitary transformation of the real quaternion space $\mathbb{H}$ preserves perfection of a sequence. Many examples, illustrating applications of the new results, are given.

- In Section 7, Composition of Sequences over the Real Quaternions, we generalize the results on composition of perfect sequences over the complex numbers to sequences over the real quaternions, and then we use these new results for composing several perfect sequences over the quaternions, found by an exhaustive computer search. By this way, we have obtained a perfect sequence over a small alphabet of only 24 unit quaternions of quite impressive length $5{,}354{,}228{,}880$. Also, a brand new result on composition of two sequences of even lengths is presented in this section.

- In Section 8, Conditions Necessary for Perfection over the Real Quaternions, we present the Balance Theorem over the quaternions, which is an extension of the known result over the complex numbers, and consider a few generalizations of this condition. Also, we study geometrical properties of perfect sequences over the quaternions in 3-dimension Euclidean space. It is also shown that the length of a perfect sequence over the alphabet $\boldsymbol{Q}_8 = \{\pm 1, \pm \boldsymbol{i}, \pm \boldsymbol{j}, \pm \boldsymbol{k}\}$ is always an even number.

- In Section 9, Discrete Fourier Transform of a Perfect Sequence over the Quaternions, as the name suggests, we introduce the discrete Fourier transform of a quaternionic sequence. The important necessary condition for perfection over the quaternions, stating that all discrete Fourier transform coefficients of a perfect quaternionic sequence have the same norm, is proved in this section.

- In Section 10, Conclusion, we give some final remarks and list the known properties of perfect sequences over the complex numbers and over the real quaternions in Table 10.1, which facilitates a comparison between the two structures.
- Section 11, Bibliography.

The results of Section 5, stating the equivalence of left and right perfection over the real quaternions, have been presented by the author to the Fourth International Workshop on Signal Design and its Application in Communications, held in Fukuoka, Japan, 19-23 October 2009, and are published in the IEEE Proceedings [55]. The results of Section 7, construction of a perfect sequence of length 5,354,228,880, have been presented by the author to the 2010 World Congress on Mathematics and Statistics, held in Sharm El Sheikh, Egypt, 26-29 July 2010, and appear in the Online Journal on Mathematics and Statistics [56].

2. Notations and Definitions

In this section, notations, used throughout the following sections, are explained and some general definitions are given. Concepts, which are more specific to the topic of each particular section, are defined in that section.

2.1. Fonts

Throughout the present work, the quaternions, sequences and matrices over the quaternions are denoted by **bold fonts**, whereas ordinary fonts are reserved for the real and complex numbers. Three dimensional vectors are denoted by upper arrows $\vec{v}$.

2.2. Numbering

The following numbering system is adopted in the present work.

The text of the present work consists of 10 major sections. Each section has its own number implying the consecutive order of this section in the text. Some sections contain several parts, which, in turn, can be divided into more parts. The number of each part is derived by adding more digits, separated by a dot, to the number of the section in which the part is located.

Every Definition, Lemma, Proposition, Corollary, important Remark, Example and Observation is given a unique number, consisting of two digits separated by the dot. The first digit stands for the number of the section, in which the Definition, Lemma, Proposition etc appears. The second digit is the consecutive number of the Definition, Lemma, Proposition etc in this section.

Example 2.1 The title of this part reads ‘2.2. Numbering’, meaning that it is a subsection of Section 2, and the consecutive number of this subsection within Section 2 is 2. The number of this example, 2.1, means that the example is in Section 2, and it is the first example in this section.

2.3. Rounding

For positive x, $\lfloor x \rfloor$ denotes the integer not greater than x such that $x - \lfloor x \rfloor$ is minimal, $\lceil x \rceil$ denotes the integer not less than x such that $\lceil x \rceil - x$ is minimal.

2.4. Definition of a Sequence

Definition 2.1 An ordered n-tuple $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$ of elements from a set A is called a *sequence*. The set A is called an *alphabet*. The number n is called the *length* of the sequence $\boldsymbol{x}$.

Remark 2.1 For elements of a sequence of length n, the operations in indices are always assumed *modulo* n.

The following three definitions are adapted from works of Barbe and Skordev [7].

Definition 2.2 Let $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$ be a sequence. The smallest positive integer l such that $\boldsymbol{x}_t = \boldsymbol{x}_{t+l}$, for $0 \le t \le n-1$, is called the *period* of the sequence $\boldsymbol{x}$**.**

Definition 2.3 For an integer m, the m-th circular shift to the left, or simply m-shift, of the sequence $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$, denoted by ${}^{m}\boldsymbol{x}$, is the sequence ${}^{m}\boldsymbol{x} = [\boldsymbol{x}_m, \boldsymbol{x}_{m+1}, \dots, \boldsymbol{x}_{m-1}]$, that is, for every k, $0 \le k \le n-1$, $[{}^{m}\boldsymbol{x}]_k = \boldsymbol{x}_{m+k}$, where $[{}^{m}\boldsymbol{x}]_k$ denotes the k-th element of the sequence ${}^{m}\boldsymbol{x}$.

Definition 2.4 For integer numbers p and m, $0 \le p, m \le n-1$, the (p, m)*-decimation* of a sequence $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$, denoted by $Dec_p^m(\boldsymbol{x})$, is the subsequence $\left[\boldsymbol{x}_m, \boldsymbol{x}_{m+p}, \dots, \boldsymbol{x}_{m+p\left(\frac{n}{\gcd(n,p)}-1\right)}\right]$, where $\gcd(n,p)$ is the greatest common divisor of integers n and p. That is, for every k, $0 \le k \le \frac{n}{\gcd(n,p)} - 1$, $\left[Dec_p^m(\boldsymbol{x})\right]_k = \boldsymbol{x}_{m+pk}$. Where it does not cause confusion, the (p, m)-decimation is often called 'decimation by p', irrespective of m.

Observation 2.1 $Dec_p^m(\boldsymbol{x}) = {}^{m}Dec_p^0(\boldsymbol{x})$.

Definition 2.5 (Skaug and Hjelmstad [85]) Decimation $Dec_p^m(\boldsymbol{x})$ of a sequence $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$ is called *proper* if p is co-prime with n, that is, $\gcd(p, n) = 1$.

Note that the length of a decimation by p of a sequence $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$ is always a divisor of n, and equal to $\frac{n}{\gcd(n,p)}$. The length of a proper decimation by p is equal to n, the length of the original sequence.

Definition 2.6 The sum of all elements of a sequence $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$ is called the *balance* of the sequence $\boldsymbol{x}$ and is denoted by $\sum \boldsymbol{x}$.

Definition 2.7 The *norm* of a sequence $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$ is defined as the sum of the norms of all its elements: $\|\boldsymbol{x}\| = \sum_{t=o}^{n-1} \|\boldsymbol{x}_t\|$.

2.5. Roots of Unity Related Definitions

Definition 2.8 A complex number ω is called an *n-th root of unity* if $\omega^n = 1$.

Definition 2.9 An n-th root of unity ω is called *primitive* if $\omega^n = 1$ and $\omega^s \neq 1$ for all $s = 1, \dots, n-1$.

Definition 2.10 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.

3. Algebra of Quaternions

In this section, a brief introduction to quaternions is given. The exposition in this section does not attempt to cover all available information about the real quaternions, but rather emphasizes the aspects that are related to the content of the following sections.

3.1. Discovery of Quaternions

The quaternions were discovered by Sir William Rowan Hamilton on October 16th, 1843 (Van Der Waerden [92]).

Getting excited by the way the complex numbers are applied in the Euclidian plane geometry, Hamilton had spent a number of years trying to invent a bigger structure which can be similarly applied in 3-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. So, he introduced a new imaginary unit $\boldsymbol{j}$, $\boldsymbol{j}^2=-1$, and studied the new numbers in the form $\boldsymbol{x}=x_0+x_1\boldsymbol{i}+x_2\boldsymbol{j}$, where x_0, x_1, x_2 are real numbers. Addition of the new numbers presented no problem: because Hamilton wanted the new numbers, when being interpreted as points (x_0, x_1, x_2) of a 3-dimensional vector space $\mathbb{R}^3$, to preserve properties of the vector space, the only option was the ordinary vector component-wise addition $(x_0, x_1, x_2)+(y_0, y_1, y_2)=(x_0+y_0, x_1+y_1, x_2+y_2)$. However, multiplication was a much bigger concern. Because the new number system required to be closed under multiplication, the product of two imaginary units $\boldsymbol{i}$ and $\boldsymbol{j}$ must be of the form $\boldsymbol{ij}=x_0+x_1\boldsymbol{i}+x_2\boldsymbol{j}$, with x_0, x_1, x_2 real numbers. Then, the equality

$$-\boldsymbol{j}=\boldsymbol{i}^2\boldsymbol{j}=\boldsymbol{i}(\boldsymbol{ij})=\boldsymbol{i}(x_0+x_1\boldsymbol{i}+x_2\boldsymbol{j})=x_0\boldsymbol{i}+x_1\boldsymbol{i}^2+x_2\boldsymbol{ij}=x_0\boldsymbol{i}-x_1+x_2(x_0+x_1\boldsymbol{i}+x_2\boldsymbol{j})$$
$$=(x_0x_2-x_1)+(x_0+x_1x_2)\boldsymbol{i}+x_2^2\boldsymbol{j}$$

implies an inconsistent identity $x_2^2 = -1, x_2 \in \mathbb{R}$.

After many months of trial and errors, Hamilton had realized that such a number system did not present the right choice. Within the assumption of associativity, distributivity over addition and commutativity with real numbers for the multiplication, Hamilton always came to a contradiction.

In modern terms, Hamilton has been trying to construct a 3-dimensional field. Now we know that no such thing exists! This striking answer was first discovered by German mathematician Ferdinand Georg Frobenius in 1877. He proved that, for $n > 2$, $\mathbb{R}^n$ cannot be made into a field. For a short, efficient proof of this Theorem refer to Young [97].

So, a major revision of the new number system was required!

All of a sudden, while walking with his wife along the Royal Canal to a meeting of the Royal Irish Academy in Dublin, in a pure stroke of genius, Hamilton has realized that the recourse was in a higher dimension space: it was not in $\mathbb{R}^3$, but in $\mathbb{R}^4$ that one could introduce a meaningful multiplication which, moreover, was connected to rotations in $\mathbb{R}^3$ (Artmann [4]). The third imaginary unit, $\boldsymbol{k}$, has been introduced. In Hamilton's own words, 'I then and there felt the galvanic circuit of thought close; and the sparks which fell from it were the fundamental equations between $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$; exactly such as I have used them ever since' (Baez [6]).

Numbers of the form $\boldsymbol{q} = q_0 + q_1\boldsymbol{i} + q_2\boldsymbol{j} + q_3\boldsymbol{k}$, where $q_0, \dots, q_3 \in \mathbb{R}$, have been called (real) *quaternions* (De Leo [26]).

Note that, with such definition, all real and complex numbers can be considered as a special case of real quaternions. Indeed, a quaternion with zero coefficients before $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$ is equivalent to the real number $r = q_0$, while a quaternion with zero coefficients before $\boldsymbol{j}$ and $\boldsymbol{k}$ only is equivalent to the complex number $c = q_0 + q_1\boldsymbol{i}$.

3.2. Axiomatic Properties of Quaternions

In this part, a formal definition of quaternions is given, and some basic concepts related to quaternions are considered.

3.2.1. Definition of a Quaternion

Definition 3.1 (Vicci [93]) Real quaternions are defined as sums of four terms of the form

$$\boldsymbol{q} = q_0 1 + q_1 \boldsymbol{i} + q_2 \boldsymbol{j} + q_3 \boldsymbol{k}$$

where q_0, q_1, q_2, q_3 are real numbers, 1 is the multiplicative identity element, and $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$ are symbolic elements having the properties:

$$\boldsymbol{i}^2 = -1, \qquad \boldsymbol{j}^2 = -1, \qquad \boldsymbol{k}^2 = -1,$$

$$\boldsymbol{ij} = \boldsymbol{k}, \qquad \boldsymbol{ji} = -\boldsymbol{k},$$

$$\boldsymbol{jk} = \boldsymbol{i}, \qquad \boldsymbol{kj} = -\boldsymbol{i},$$

$$\boldsymbol{ki} = \boldsymbol{j}, \qquad \boldsymbol{ik} = -\boldsymbol{j}.$$

Commonly, for the sake of brevity and when it does not lead to an ambiguity, the multiplicative identity element 1 is omitted in writing of a quaternion expansion:

$$\boldsymbol{q} = q_0 + q_1 \cdot \boldsymbol{i} + q_2 \cdot \boldsymbol{j} + q_3 \cdot \boldsymbol{k}$$

By analogy with the complex numbers, elements $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$ are called *imaginary units*. The multiplication law as per Definition 3.1 is called *Hamilton's multiplication table*.

It is easy to observe that Hamilton's multiplication does not obey the commutative law.

3.2.2. Addition of Quaternions

As it has already been mentioned above, the requirement for the new number system to possess properties of a linear space over $\mathbb{R}$ determines the component-wise addition rule for the real quaternions:

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

for any real quaternions $\boldsymbol{p}=p_0+p_1\boldsymbol{i}+p_2\boldsymbol{j}+p_3\boldsymbol{k}$ and $\boldsymbol{q}=q_0+q_1\boldsymbol{i}+q_2\boldsymbol{j}+q_3\boldsymbol{k}$.

3.2.3. Multiplication of Quaternions

The requirement for the quaternion multiplication to respect distributive and associative laws implies polynomial-like multiplication rule for quaternions. This, along with Hamilton's multiplication table, provides for the following multiplication formula: for any real quaternions $\boldsymbol{p}=p_0+p_1\boldsymbol{i}+p_2\boldsymbol{j}+p_3\boldsymbol{k}$ and $\boldsymbol{q}=q_0+q_1\boldsymbol{i}+q_2\boldsymbol{j}+q_3\boldsymbol{k}$

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

Note that a pair of quaternions can multiplicatively commute, anti-commute, or neither of the two. Consider three cases below:

Example 3.1

1. *Commutative case*. Complex numbers is a special case of the real quaternions. Any two complex numbers commute with each other:

$(1+\boldsymbol{i})(-2+3\boldsymbol{i}) = -5+\boldsymbol{i}$, $(-2+3\boldsymbol{i})(1+\boldsymbol{i}) = -5+\boldsymbol{i}$.

So, $(1+\boldsymbol{i})(-2+3\boldsymbol{i}) = (-2+3\boldsymbol{i})(1+\boldsymbol{i})$.

2. *Anti-commutative case.* $\boldsymbol{ij} = \boldsymbol{k}$, $\boldsymbol{ji} = -\boldsymbol{k}$. So, $\boldsymbol{ij} = -\boldsymbol{ji}$.
3. *Neither commutative, nor anti-commutative case.* $(1+\boldsymbol{i})(\boldsymbol{j}+\boldsymbol{k}) = 2\boldsymbol{k}$, $(\boldsymbol{j}+\boldsymbol{k})(1+\boldsymbol{i}) = 2\boldsymbol{j}$.

   So, neither $(1+\boldsymbol{i})(\boldsymbol{j}+\boldsymbol{k}) = (\boldsymbol{j}+\boldsymbol{k})(1+\boldsymbol{i})$, nor $(1+\boldsymbol{i})(\boldsymbol{j}+\boldsymbol{k}) = -(\boldsymbol{j}+\boldsymbol{k})(1+\boldsymbol{i})$.

3.2.4. Quaternion Conjugates

Definition 3.2 For a quaternion $\boldsymbol{q} = q_0 + q_1\boldsymbol{i} + q_2\boldsymbol{j} + q_3\boldsymbol{k}$, the quaternion $\boldsymbol{q}^* = q_0 - q_1\boldsymbol{i} - q_2\boldsymbol{j} - q_3\boldsymbol{k}$ is called the *conjugate* of the quaternion $\boldsymbol{q}$, and is denoted by $\boldsymbol{q}^*$.

Every quaternion $\boldsymbol{q}$ commutes with its conjugate: their order of multiplication can be interchanged. Indeed, by direct calculation, $\boldsymbol{qq}^* = q_0^2 + q_1^2 + q_2^2 + q_3^2 = \boldsymbol{q}^*\boldsymbol{q}$.

Note that the product $\boldsymbol{qq}^* = \boldsymbol{q}^*\boldsymbol{q}$ is always a non-negative real number. Furthermore, we have $\boldsymbol{qq}^* = 0$ if and only if $\boldsymbol{q} = 0$.

The conjugate operation is distributive over addition, that is, $(\boldsymbol{p}+\boldsymbol{q})^* = \boldsymbol{p}^* + \boldsymbol{q}^*$. With respect to multiplication, however, $(\boldsymbol{pq})^* = \boldsymbol{q}^*\boldsymbol{p}^*$ (Artmann [4]).

3.2.5. Norm of a Quaternion

Definition 3.3 The *norm* of a quaternion $\boldsymbol{q}$, denoted by $\|\boldsymbol{q}\|$, is defined by $\|\boldsymbol{q}\| = \boldsymbol{qq}^*$. A quaternion of the norm 1 is called a *unit* quaternion.

The norm multiplication law for quaternions, $\|\boldsymbol{pq}\| = \|\boldsymbol{p}\|\|\boldsymbol{q}\|$, follows from the definition. Because quaternion multiplication preserves the norm, the set of all unit quaternions forms a group.

Since $\|\boldsymbol{q}\| = q_0^2 + q_1^2 + q_2^2 + q_3^2$, the square root $\sqrt{\|\boldsymbol{q}\|}$ is equal to the length of the vector (q_0, q_1, q_2, q_3) in $\mathbb{R}^4$.

3.2.6. Order of a Quaternion

Definition 3.4 The *order* of a quaternion $\boldsymbol{q}$ is the smallest positive integer m such that $\boldsymbol{q}^m = 1$. If no such m exists, we say that $\boldsymbol{q}$ is of infinite order.

Note that, since by the norm multiplication law for quaternions we have $\|\boldsymbol{p}^m\| = \|\boldsymbol{p}\|^m$, only unit quaternions can have a finite order.

3.2.7. Division of Quaternions

One of the most important properties of quaternions is the existence of quaternion division. That is, the equations $\boldsymbol{xq} = \boldsymbol{p}$ and $\boldsymbol{qx} = \boldsymbol{p}$ always have solutions for any quaternions $\boldsymbol{p}$ and $\boldsymbol{q}$, $\boldsymbol{q} \neq 0$. Solutions of the equation $\boldsymbol{xq} = \boldsymbol{p}$ ($\boldsymbol{qx} = \boldsymbol{p}$) are called *right* (*left*) *quotients* of the quaternions $\boldsymbol{p}$ and $\boldsymbol{q}$.

Denoting the right and left quotients by $\boldsymbol{q}_R^{-1}$ and $\boldsymbol{q}_L^{-1}$ respectively, we can easily derive explicit expressions for $\boldsymbol{q}_R^{-1}$ and $\boldsymbol{q}_L^{-1}$. Multiplying both sides of the equation $\boldsymbol{q}_R^{-1}\boldsymbol{q} = \boldsymbol{p}$ from the right and $\boldsymbol{q}\boldsymbol{q}_L^{-1} = \boldsymbol{p}$ from the left by $\frac{\boldsymbol{q}^*}{\|\boldsymbol{q}\|}$, we have $\boldsymbol{q}_R^{-1} = \frac{\boldsymbol{pq}^*}{\|\boldsymbol{q}\|}$ and $\boldsymbol{q}_L^{-1} = \frac{\boldsymbol{q}^*\boldsymbol{p}}{\|\boldsymbol{q}\|}$.

Since $\frac{\boldsymbol{p}\boldsymbol{q}^*}{\|\boldsymbol{q}\|} \neq \frac{\boldsymbol{q}^*\boldsymbol{p}}{\|\boldsymbol{q}\|}$, two distinct quotients, in general, occur. However, in the special case $\boldsymbol{p} = 1$ both left and right quotients are equal to $\frac{\boldsymbol{q}^*}{\|\boldsymbol{q}\|}$. The quaternion $\frac{\boldsymbol{q}^*}{\|\boldsymbol{q}\|}$ is called the *multiplicative inverse* of a quaternion $\boldsymbol{q}$.

3.3. Division Algebra of Quaternions

Mathematically, the remarkable property of the real quaternions is that they form a *division algebra* (many older sources use term *'skew-field'* for division algebras).

If we denote the set of all real quaternions by $\mathbb{H}$ (we use $\mathbb{H}$ because of Hamilton)

$$\mathbb{H} = \{q_0 + q_1\boldsymbol{i} + q_2\boldsymbol{j} + q_3\boldsymbol{k} \mid q_0, q_1, q_2, q_3 \in \mathbb{R}\}$$

then all the axioms of a field hold in $\mathbb{H}$, except for the commutative law of multiplication.

Note that the quaternion algebra $\mathbb{H}$ contains infinitely many complex subfields. Artmann [4] has shown that every 2-dimension plane in $\mathbb{H}$, which passes through the real axis, is isomorphic to $\mathbb{C}$, with regard to the quaternion multiplication.

The *centre* of the quaternion algebra $\mathbb{H}$, that is the subset of elements which commute with all other elements in $\mathbb{H}$, is $\mathbb{R}$ (Artmann [4]).

3.4. Quaternions and Vectors in $\mathbb{R}^3$

Every quaternion $\boldsymbol{q} = q_0 + q_1\boldsymbol{i} + q_2\boldsymbol{j} + q_3\boldsymbol{k}$ can be regarded as having a *real* ($\mathrm{Re}(\boldsymbol{q}) = q_0$) and a *pure*, or *imaginary* ($\mathrm{Im}(\boldsymbol{q}) = q_1\boldsymbol{i} + q_2\boldsymbol{j} + q_3\boldsymbol{k}$), parts. Many older sources, following the terminology used by Hamilton himself, refer to *scalar* and *vector* parts of the quaternion $\boldsymbol{q}$

respectively, and denote them as $S\boldsymbol{q} = q_0$ and $V\boldsymbol{q} = q_1\boldsymbol{i} + q_2\boldsymbol{j} + q_3\boldsymbol{k}$. Quaternions with zero real part are called *pure* quaternions.

It is easy to see that real and imaginary parts of a quaternion $\boldsymbol{q} = q_0 + q_1\boldsymbol{i} + q_2\boldsymbol{j} + q_3\boldsymbol{k}$ can be expressed as follows:

$$\mathrm{Re}(\boldsymbol{q}) = \frac{1}{2}(\boldsymbol{q} + \boldsymbol{q}^*)$$

$$\mathrm{Im}(\boldsymbol{q}) = \frac{1}{2}(\boldsymbol{q} - \boldsymbol{q}^*)$$

Hamilton regarded quaternions $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$ as basis vectors in $\mathbb{R}^3$. From this, even today, physicists call $q_1\boldsymbol{i} + q_2\boldsymbol{j} + q_3\boldsymbol{k}$ a vector in $\mathbb{R}^3$ (Artmann [4]).

For the sake of brevity, sometimes in the following sections we will denote the real and imaginary parts of a quaternion $\boldsymbol{q}$ by q and $\vec{q}$ respectively; thus, in such notations, $\boldsymbol{q} = \mathrm{Re}(\boldsymbol{q}) + \mathrm{Im}(\boldsymbol{q}) = q + \vec{q}$.

It is known (Kyrala [57]) that the product of two arbitrary quaternions $\boldsymbol{p}$ and $\boldsymbol{q}$ can be expressed as

$$\boldsymbol{pq} = pq - \langle\vec{p}, \vec{q}\rangle + p\vec{q} + q\vec{p} + \vec{p} \times \vec{q} \tag{3.1}$$

where $\langle\cdot,\cdot\rangle$ and $\times$ denote inner and cross products of two vectors in three-dimensional Euclidian space $\mathbb{R}^3$. It is clear that $pq - \langle\vec{p}, \vec{q}\rangle$ and $\mathrm{p}\vec{q} + q\vec{p} + \vec{p} \times \vec{q}$ are the scalar and vector parts of the product quaternion $\boldsymbol{pq}$ respectively.

Since vector multiplication in 3-dimensional space $\mathbb{R}^3$ is anti-commutative, $\vec{p} \times \vec{q} = -\vec{q} \times \vec{p}$, it is clear that non-commutativity of the quaternion product originates from the presence of the vector product $\vec{p} \times \vec{q}$ in the expansion (3.1).

3.5. Quaternions and Unitary Mappings in $\mathbb{R}^3$ and $\mathbb{R}^4$

Quaternions provide a convenient mathematical framework for representing rotations and reflections in 3- and 4-dimensional spaces. A connection between quaternions and rotations in 3-dimensional space $\mathbb{R}^3$ was first mentioned by British mathematician Arthur Cayley [16] as early as in 1845. Since then, the relationship between quaternions and linear transformations in 3- and 4-dimensional spaces has been established and studied. An elegant and complete description of unitary transformations in both $\mathbb{R}^3$ and $\mathbb{R}^4$ has been given by Coxeter [24] in 1946. In this part the results of Coxeter are briefly discussed.

Following Hathaway [37], we identify a point (q_0, q_1, q_2, q_3) in $\mathbb{R}^4$ with the quaternion $\boldsymbol{q} = q_0 + q_1\boldsymbol{i} + q_2\boldsymbol{j} + q_3\boldsymbol{k}$. Besides, as it was already mentioned above, a point (q_1, q_2, q_3) in $\mathbb{R}^3$ is interpreted as the pure quaternion $\boldsymbol{q} = q_1\boldsymbol{i} + q_2\boldsymbol{j} + q_3\boldsymbol{k}$.

An origin-preserving linear transformation in $\mathbb{R}^n$ is defined as follows:

Definition 3.5 Let V be a vector space over the real field $\mathbb{R}$ with an inner product $\langle\cdot,\cdot\rangle : V \times V \to \mathbb{R}$. A surjective linear transformation $T: V \to V$, satisfying $\langle x, y\rangle = \langle Tx, Ty\rangle$, for all $x, y \in V$, is called a *unitary transformation* of V.

Because a unitary transformation preserves the inner product norm,

$\|Tx\|_{\mathbb{R}^n} \overset{\text{def}}{=} < Tx, Tx >=< x, x > \overset{\text{def}}{=} \|x\|_{\mathbb{R}^n}$, for all $x \in V$,

it follows that $Tx = 0$ if and only if $x = 0$. Thus a unitary transformation maps 0 to 0, i.e. leaves the origin unchanged. Reflection in any hyperplane passing through the origin and rotations about the origin are examples of unitary transformations in the Euclidian space $\mathbb{R}^n$.

3.5.1. Unitary Transformations in $\mathbb{R}^3$

It is known (Cho [20]) that every unit quaternion $\boldsymbol{p}$ can be represented as $\boldsymbol{p} = \cos\alpha + \vec{u}\sin\alpha$, where α is a real number and $\vec{u}$ is a unit pure quaternion. Let $\vec{v}$ be an ordinary vector in 3-dimensional space $\mathbb{R}^3$, considered as a quaternion with zero real part, and let $\boldsymbol{p}$ be a unit quaternion $\boldsymbol{p} = \cos\frac{\varphi}{2} + \vec{u}\sin\frac{\varphi}{2}$. Then the triple quaternion product $\vec{v} \to \boldsymbol{p}\vec{v}\boldsymbol{p}^*$ represent the rotation (in the clockwise direction, if the line of sight points in the direction of $\vec{u}$) of the original vector $\vec{v}$ by an angle φ around the axis of $\vec{u}$. Combining rotations $\vec{v} \to \boldsymbol{p}\vec{v}\boldsymbol{p}^*$with inversions $\vec{v} \to -\vec{v}$, Coxeter [24] deduced that any unitary transformation of the ordinary 3-dimensional space $\mathbb{R}^3$ can be represented as either $\vec{v} \to \boldsymbol{p}\vec{v}\boldsymbol{p}^*$ or $\vec{v} \to -\boldsymbol{p}\vec{v}\boldsymbol{p}^*$.

3.5.2. Unitary Transformations in $\mathbb{R}^4$

Reflections and rotations in $\mathbb{R}^4$ can also be conveniently expressed by quaternion multiplication. Coxeter showed that, for unitary quaternion $\boldsymbol{p} = p_0 + p_1\boldsymbol{i} + p_2\boldsymbol{j} + p_3\boldsymbol{k}$, the reflection in the hyperplane defined by the equation $\sum_{m=0}^{3} x_m p_m = 0$ in 4-dimensional space $\mathbb{R}^4$ is represented by the transformation $\boldsymbol{x} \to -\boldsymbol{p}\boldsymbol{x}^*\boldsymbol{p}$. A rotation in $\mathbb{R}^4$ through angle φ about a plane is represented by the transformation $\boldsymbol{x} \to \boldsymbol{p}\boldsymbol{x}\boldsymbol{q}$, where $\boldsymbol{p} = p_0 + p_1\boldsymbol{i} + p_2\boldsymbol{j} + p_3\boldsymbol{k}$ and $\boldsymbol{q} = q_0 + q_1\boldsymbol{i} + q_2\boldsymbol{j} + q_3\boldsymbol{k}$ are two unit quaternions with equal real parts, $p_0 = q_0 = \cos\frac{\varphi}{2}$, and rotation is about the common plane of the two hyperplanes, defined by equations $\sum_{m=0}^{3} x_m p_m = \sum_{m=0}^{3} x_m q_m = 0$, through twice the angle between them.

The general rotation in 4-dimensional space $\mathbb{R}^4$ is expressed by the transformation $\boldsymbol{x} \to \boldsymbol{p}\boldsymbol{x}\boldsymbol{q}$, where $\boldsymbol{p}$ and $\boldsymbol{q}$ are unit quaternions. Such representation is unique for every rotation in $\mathbb{R}^4$ to the extent of changing signs $\boldsymbol{x} \to (-\boldsymbol{p})\boldsymbol{x}(-\boldsymbol{q})$.

Based on these results, Coxeter [24] has proved that every unitary transformation in $\mathbb{R}^4$ is represented as either $\boldsymbol{x} \to \boldsymbol{pxq}$, or $\boldsymbol{x} \to \boldsymbol{px}^*\boldsymbol{q}$.

3.6. Similarity of Quaternions

Definition 3.6 (Zhang [98]) Two quaternions $\boldsymbol{x}$ and $\boldsymbol{y}$ are said to be similar if there exists a nonzero quaternion $\boldsymbol{q}$ such that $\boldsymbol{q}^{-1}\boldsymbol{xq} = \boldsymbol{y}$. Similarity of two quaternions $\boldsymbol{x}$ and $\boldsymbol{y}$ is written by $\boldsymbol{x} \sim \boldsymbol{y}$.

Similarity is an equivalence relation on the real quaternion algebra $\mathbb{H}$. The equivalence class containing a quaternion $\boldsymbol{x}$ is denoted by $[\boldsymbol{x}]$.

It is known (Zhang [98]) that quaternions

$$\boldsymbol{q} = q_0 + q_1\boldsymbol{i} + q_2\boldsymbol{j} + q_3\boldsymbol{k}$$

and

$$\boldsymbol{q}' = q_0 + \boldsymbol{i}\sqrt{q_1^2 + q_2^2 + q_3^2}$$

are similar, i.e. $\boldsymbol{q} \in \left[q_0 + \boldsymbol{i}\sqrt{q_1^2 + q_2^2 + q_3^2}\right]$.

Note that the quaternion $\boldsymbol{q}'$ can be regarded as a complex number.

If $\boldsymbol{x} = x_0 + \vec{x}$ and $\boldsymbol{y} = y_0 + \vec{y}$ are two quaternions written as sums of the real and vector parts, then $\boldsymbol{x} \sim \boldsymbol{y}$ if and only if $x_0 = y_0$ and $|\vec{x}| = |\vec{y}|$, i.e. $\mathrm{Re}(\boldsymbol{x}) = \mathrm{Re}(\boldsymbol{y})$ and $|\mathrm{Im}(\boldsymbol{x})| = |\mathrm{Im}(\boldsymbol{y})|$ (Brenner [14]). From here it is readily seen that the equivalence class $[\boldsymbol{q}]$ contains infinitely many quaternions, which may be visualized as points in 4-dimension quaternion space located on a 2-sphere of radius $|\mathrm{Im}(\boldsymbol{q})|$ with the centre sitting on the real axis by $\mathrm{Re}(\boldsymbol{q})$ away from the origin. Among those infinitely many similar quaternions, there are two complex numbers which are conjugates of each other.

If $\boldsymbol{q}$ is a real number, which is a special case of a real quaternion, then the 2-sphere contracts into a single point on the real axis.

Since $|\mathrm{Im}(\boldsymbol{q})| = |\mathrm{Im}(\boldsymbol{q}^*)|$ for all $\boldsymbol{q} \in \mathbb{H}$, every quaternion $\boldsymbol{q}$ is similar to its own conjugate, $\boldsymbol{q} \sim \boldsymbol{q}^*$.

3.7. Fundamental Theorem of Algebra for the Quaternions

Unlike the complex case, where every polynomial can be represented as $f(x) = a_n x^n + \cdots + a_n x + a_n$, polynomials over the quaternions can not always be written in such a form. Due to non-commutativity of quaternion multiplication, a general form of a polynomial over the quaternions consists of terms $\boldsymbol{a}_0 \boldsymbol{x} \boldsymbol{a}_1 \boldsymbol{x} \ldots \boldsymbol{x} \boldsymbol{a}_n$ where $\boldsymbol{a}_0, \ldots, \boldsymbol{a}_n$ are quaternions.

The question of an existence of a *root* of a general polynomial over the real quaternions, that is a solution of the equation $F(\boldsymbol{x}) = \boldsymbol{a}_0 \boldsymbol{x} \boldsymbol{a}_1 \boldsymbol{x} \ldots \boldsymbol{x} \boldsymbol{a}_n + \varphi(\boldsymbol{x}) = 0$, where $\boldsymbol{a}_0, \ldots, \boldsymbol{a}_n$ are non-zero quaternions, $\boldsymbol{x}$ is a quaternion indeterminant, and $\varphi(\boldsymbol{x})$ is the sum of a finite number of monomials $\boldsymbol{b}_0 \boldsymbol{x} \boldsymbol{b}_1 \boldsymbol{x} \ldots \boldsymbol{x} \boldsymbol{b}_k$, $k < n$, has been studied by Eilenberg and Niven [27]. They have proved that $F(\boldsymbol{x}) = 0$ has at least one quaternion solution. The obvious corollary of this result, which has been, in fact, discovered before the main result became available (Niven [73]), is that $f(\boldsymbol{x}) = \boldsymbol{a}_0 \boldsymbol{x}^n + \cdots + \boldsymbol{a}_{n-1} \boldsymbol{x} + \boldsymbol{a}_n = 0$, with $\boldsymbol{a}_0, \ldots, \boldsymbol{a}_n$ quaternions, has at least one solution in $\mathbb{H}$.

It is worth noting that, unlike in the complex case, the number of solutions of the equation $F(\boldsymbol{x}) = 0$ or $f(\boldsymbol{x}) = 0$ may exceed the degree n of the polynomial.

Example 3.2 The equation $\boldsymbol{x}^2 + 1 = 0$ has infinitely many solutions.

Fan [28] has shown that the number of quaternionic solutions to $\boldsymbol{x}^2 - \boldsymbol{q} = 0$, $\boldsymbol{q} \in \mathbb{H}$, are either

(1) two quaternions, when $\boldsymbol{q} \notin \mathbb{R}$, or
(2) infinite number, when $\boldsymbol{q} \in \mathbb{R}, \boldsymbol{q} < 0$, or
(3) two real numbers, when $\boldsymbol{q} \in \mathbb{R}, \boldsymbol{q} > 0$, or
(4) 0, when $\boldsymbol{q} = 0$.

Niven [73] studied necessary and sufficient conditions for the equation of the form $f(\boldsymbol{x}) = \boldsymbol{a}_0\boldsymbol{x}^n + \cdots + \boldsymbol{a}_{n-1}\boldsymbol{x} + \boldsymbol{a}_n = 0$ to have infinitely many quaternion roots. Huang and So [47] have found an exact formula for the solutions of the quaternionic quadratic equation $\boldsymbol{x}^2 + \boldsymbol{b}\boldsymbol{x} + \boldsymbol{c} = 0$.

The number of solutions and a general explicit formula for the solutions of the general quaternionic polynomial equation $F(\boldsymbol{x}) = 0$ are still open questions.

3.8. Matrices over Quaternions

In [98], Zhang studies matrices with quaternion entries, and introduces elementary operation over them. Although most of the results would be trivial in the case of complex numbers, non-commutativity of quaternion multiplication makes properties of quaternion matrices quite dissimilar to properties of their complex counterparts. In matrix theory, the non-commutativity of quaternions needs to be treated with extreme care!

Let $M_{m\times n}(\mathbb{H})$, or simply $M_n(\mathbb{H})$ when $m = n$, denote the set of all $m \times n$ matrices with quaternion entries. Addition and multiplication of quaternion matrices are defined similarly to the complex case. The left (right) scalar multiplication is defined as follows:

for $\boldsymbol{A} = [\boldsymbol{a}_{st}] \in M_{m\times n}(\mathbb{H})$ and $\boldsymbol{q} \in \mathbb{H}$, $\boldsymbol{qA} = [\boldsymbol{q}\boldsymbol{a}_{st}]$ ($\boldsymbol{qA} = [\boldsymbol{a}_{st}\boldsymbol{q}]$).

It is clear that, in general, $\boldsymbol{qA} \neq \boldsymbol{Aq}$.

Definition 3.7 Just as for complex matrices, for every quaternion matrix $\boldsymbol{A} = [\boldsymbol{a}_{st}] \in M_{m\times n}(\mathbb{H})$ we define its *conjugate* $\overline{\boldsymbol{A}} = [\boldsymbol{a}_{st}^*] \in M_{m\times n}(\mathbb{H})$, *transpose* $\boldsymbol{A}^{\boldsymbol{T}} = [\boldsymbol{a}_{ts}] \in M_{n\times m}(\mathbb{H})$, and *conjugate transpose* $\boldsymbol{A}^* = [\boldsymbol{a}_{ts}^*] \in M_{n\times m}(\mathbb{H})$.

Zhang [98] introduces the concepts of unitary and Hermitian matrices over the real quaternions, by generalization of the complex case.

Definition 3.8 Just as for complex matrices, a square quaternion matrix $\boldsymbol{A} \in M_n(\mathbb{H})$ is said to be *normal* if $\boldsymbol{AA}^* = \boldsymbol{A}^*\boldsymbol{A}$, *Hermitian* if $\boldsymbol{A}^* = \boldsymbol{A}$, and *unitary* if $\boldsymbol{A}^*\boldsymbol{A} = \boldsymbol{I}$, where $\boldsymbol{I}$ denotes the identity matrix.

Since the equation $\boldsymbol{AB} = \boldsymbol{I}$ holds if and only if $\boldsymbol{BA} = \boldsymbol{I}$ holds ([98], Proposition 4.1), every unitary matrix $\boldsymbol{A}$ satisfies $\boldsymbol{A}^*\boldsymbol{A} = \boldsymbol{AA}^* = \boldsymbol{I}$. Like in the complex case, the product of unitary quaternion matrices is itself unitary. Also, a unitary quaternion matrix $\boldsymbol{U}$ scaled by a unit quaternion $\boldsymbol{q}$ is unitary, whether $\boldsymbol{q}$ is multiplied from the left or from the right (Sangwine and Le Bihan [79]).

3.8.1. Quaternionic Determinants

Note that since the classical definition of the determinant of a complex matrix involves summation of multiple products of the matrix entries, due to the non-commutative nature of quaternion multiplication the classical concept of matrix determinant can not be directly applied in the case of quaternion matrices.

Moore [70] was trying to avoid this problem by assigning some particular order of succession for multipliers in each term which goes in the determinant. Although used by some authors (Jacobson [51], Liebendorfer [61]), the Moore determinant has not received wide recognition. Sometimes, the concept of a *double determinant*, which, for a matrix $\boldsymbol{A}$, is the Moore determinant of the product matrix $\boldsymbol{A}^*\boldsymbol{A}$, is used instead (Chen [19], Renmin et. al. [78]). The double determinant has a nice property of being a non-negative real number.

Another approach to defining a quaternion determinant was implemented by Study [87]. The details can be found in the excellent retrospective survey paper of Aslaksen [5]. Study's idea was to transform a quaternion matrix of order n into the complex matrix of special form of order $2n$, and compute the corresponding determinant. This is the most common approach to quaternion determinants, which has been adopted and evolved in many contemporary sources (Cohen [23], Farenick and Pidkowich [30], Zhang [98]).

However, it has been accepted that quaternionic determinants present an important failure that can not be easily fixed. Fan [28] shows that there does not exist an extension for the conventional definition of matrix determinant to quaternion matrices, which preserves the multiplicative property of determinants $\det(\boldsymbol{AB}) = \det(\boldsymbol{A}) \det(\boldsymbol{B})$.

3.8.2. Matrix Inverse

Due to non-commutativity of quaternion multiplication, left and right inverses of a quaternion matrix must be treated separately. Chen [19] gives necessary and sufficient conditions for the existence of left and right quaternion matrix inverses, and presents an explicit formula for calculation. Chen's formula involves the double determinants.

Since the equations $\boldsymbol{AB} = \boldsymbol{I}$ and $\boldsymbol{BA} = \boldsymbol{I}$ can only hold simultaneously, in the case when both left and right quaternion matrix inverses exist, they are equal to each other.

Definition 3.9 A square quaternion matrix $\boldsymbol{A} \in M_n(\mathbb{H})$ is said to be *invertible* if $\boldsymbol{AB} = \boldsymbol{BA} = \boldsymbol{I}$ for some matrix $\boldsymbol{B} \in M_n(\mathbb{H})$.

Zhang ([98], Theorem 4.1) has shown that for any two invertible matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ in $M_n(\mathbb{H})$, the following identities hold:

- $(\boldsymbol{AB})^* = \boldsymbol{B}^*\boldsymbol{A}^*$,
- $(\boldsymbol{AB})^{-1} = \boldsymbol{B}^{-1}\boldsymbol{A}^{-1}$ and
- $(\boldsymbol{A}^*)^{-1} = (\boldsymbol{A}^{-1})^*$.

3.9. Eigenvalues of Matrices over the Quaternions

In this section, we briefly consider the concepts of eigenvalues and eigenvectors in application to matrices over the real quaternions. It is clear that due to non-commutativity of quaternions two distinct eigenvalue equations can be considered: $\boldsymbol{Q\xi} = \boldsymbol{\xi\lambda}$ and $\boldsymbol{Q\xi} = \boldsymbol{\lambda\xi}$.

Definition 3.10 For a quaternion matrix $\boldsymbol{Q} \in M_n(\mathbb{H})$, $\boldsymbol{\lambda} \in \mathbb{H}$ is called a *right* (*left*) *eigenvalue* of $\boldsymbol{Q}$, if it satisfies the equation $\boldsymbol{Q\xi} = \boldsymbol{\xi\lambda}$ ($\boldsymbol{Q\xi} = \boldsymbol{\lambda\xi}$) for some non-zero $\boldsymbol{\xi} \in \mathbb{H}^n$, and $\boldsymbol{\xi}$ is called a *right* (*left*) *eigenvector* of $\boldsymbol{Q}$ corresponding to the right (left) eigenvalue $\boldsymbol{\lambda}$. The set of distinct right (left) eigenvalues is called the *right* (*left*) *spectrum* of $\boldsymbol{Q}$.

3.9.1. Right Quaternionic Eigenvalues

Note that $\mathbb{H}^n$ is a full vector space over $\mathbb{R}$, but only a right vector space over $\mathbb{C}$ or $\mathbb{H}$. Indeed, every quaternion matrix $\boldsymbol{Q} \in M_n(\mathbb{H})$ acts as a transformation on the real vector space $\mathbb{H}^n$ by the usual correspondence $\boldsymbol{\xi} \to \boldsymbol{Q\xi}$ on vectors of $\mathbb{H}^n$. Because $\boldsymbol{Q}$ is a linear transformation, the following identity holds:

$$\boldsymbol{Q}(\alpha_1\boldsymbol{\xi}_1 + \alpha_2\boldsymbol{\xi}_2) = \alpha_1\boldsymbol{Q\xi}_1 + \alpha_2\boldsymbol{Q\xi}_2$$

Due to non-commutativity of quaternion multiplication, this equation only holds generally when α_1 and α_2 are real numbers, and not elements of $\mathbb{C}$ or $\mathbb{H}$. However, if we take matrices $\boldsymbol{Q} \in M_n(\mathbb{H})$ acting from the left, and quaternions $\boldsymbol{\alpha_1}, \boldsymbol{\alpha_2}$ acting from the right, the equation above transforms into

$$\boldsymbol{Q}(\boldsymbol{\xi}_1\boldsymbol{\alpha}_1 + \boldsymbol{\xi}_2\boldsymbol{\alpha}_2) = \boldsymbol{Q\xi}_1\boldsymbol{\alpha}_1 + \boldsymbol{Q\xi}_2\boldsymbol{\alpha}_2$$

which holds for all $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2 \in \mathbb{H}$. Therefore, in the quaternion context it is natural to consider the eigenvalue equation $\boldsymbol{Q\xi} = \boldsymbol{\xi\lambda}$, where $\boldsymbol{\xi} \in \mathbb{H}^n$ is non-zero and $\boldsymbol{\lambda} \in \mathbb{H}$. (Formally speaking, in the right vector space $\mathbb{H}^n$ over $\mathbb{H}$ left multiplication of vectors by quaternions, e.g. $\boldsymbol{q\xi}$, $\boldsymbol{q} \in \mathbb{H}$, $\boldsymbol{\xi} \in \mathbb{H}^n$, has no meaning!)

Before going any further, we make note of the following inevitable fact. If matrix $\boldsymbol{Q}$ has a non-real right eigenvalue $\boldsymbol{\lambda}$ (that is, $\mathrm{Im}(\boldsymbol{\lambda}) \neq 0$) , then it has infinitely many right eigenvalues. In fact, any quaternion similar to $\boldsymbol{\lambda}$ will be another non-real right eigenvalue of $\boldsymbol{Q}$. Indeed, if $\boldsymbol{\lambda}$ is a right eigenvalue of $\boldsymbol{Q}$ with corresponding eigenvector $\boldsymbol{\xi}$, then, for any non-zero quaternion $\boldsymbol{\omega}$, the following equality holds: $\boldsymbol{Q}(\boldsymbol{\xi\omega}) = (\boldsymbol{Q\xi})\boldsymbol{\omega} = (\boldsymbol{\xi\lambda})\boldsymbol{\omega} = \boldsymbol{\xi\omega\omega}^{-1}\boldsymbol{\lambda\omega} = (\boldsymbol{\xi\omega})(\boldsymbol{\omega}^{-1}\boldsymbol{\lambda\omega})$, which shows that $\boldsymbol{\omega}^{-1}\boldsymbol{\lambda\omega}$ is a right eigenvalue of $\boldsymbol{Q}$ corresponding to the non-zero eigenvector $\boldsymbol{\xi\omega}$.

Thus, the set of all right eigenvalues of a quaternion matrix breakes into a number of conjugacy classes, each class containing similar quaternions. Within each infinite conjugacy class, there are two quaternions which are complex numbers and conjugates of each other. Of those two complex numbers, the ones with non-negative imaginary part are called *standard right* *eigenvalues* of the quaternion matrix. If the right eigenvalue is a real number, then the corresponding conjugacy class contracts to a single element.

A fundamental property of quaternionic matrices is the existence result for right eigenvalues. It is known, and extensively reflected in literature (Lee [59], Brenner [14], Farenick and Pidkowich [30], Flaunt [31], Viswanath [94]), that every $\boldsymbol{Q} \in M_n(\mathbb{H})$ has a right eigenvalue. Furthermore, the number of distinct conjugacy classes of right eigenvalues of a quaternion matrix $\boldsymbol{Q}$ does not exceed n.

Similarly to the complex case, every $n \times n$ matrix $\boldsymbol{Q}$ with quaternion coefficients can be transformed into an upper triangular form (i.e. all entries are zero below the main diagonal) by a unitary transformation (Lee [59], Brenner [14], Farenick and Pidkowich [30]). That is, for an arbitrary quaternion matrix $\boldsymbol{Q}$, there always exists a unitary matrix $\boldsymbol{U}$, such that

$$\boldsymbol{U}^*\boldsymbol{Q}\boldsymbol{U} = \begin{bmatrix} \lambda_0 & * & \cdots & * \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & * \\ 0 & \cdots & 0 & \lambda_n \end{bmatrix}.$$

The diagonal elements $\lambda_0, \dots, \lambda_n$ are n right eigenvalues of $\boldsymbol{Q}$, which can be chosen as complex numbers (standard right eingenvalues), and the stars denote quaternions. The diagonal elements $\lambda_0, \dots, \lambda_n$ are indeterminate to the extent of changing to similar quaternions, and their order of succession.

If $\boldsymbol{Q}$ is a normal matrix, then its triangular form $\begin{bmatrix} \lambda_0 & * & \cdots & * \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & * \\ 0 & \cdots & 0 & \lambda_n \end{bmatrix}$ is also a normal matrix. Lee [59] proves by induction that a triangular normal matrix is necessarily a diagonal one. So, every normal quaternion matrix can be transformed into a diagonal form by a unitary transformation. Moreover, a unitary quaternion matrix can be transformed by another unitary matrix into diagonal form with the diagonal elements being complex numbers of norm 1, again indeterminate to the extent of changing to similar quaternions and their order of succession. The diagonal elements of a diagonal form of a hermitian quaternion matrix are necessarily real numbers, uniquely determined up to their order of succession.

The ‘power rule’ holds for right quaternionic eigenvalues: if $\boldsymbol{\xi}$ is a right eigenvector of $\boldsymbol{Q}$ with eigenvalue $\boldsymbol{\lambda}$, then it is a right eigenvector of $\boldsymbol{Q}^2$ with eigenvalue $\boldsymbol{\lambda}^2$. Indeed, $\boldsymbol{Q}^2\boldsymbol{\xi} = \boldsymbol{Q}(\boldsymbol{Q}\boldsymbol{\lambda}) = \boldsymbol{Q}(\xi\boldsymbol{\lambda}) = (\boldsymbol{Q}\xi)\boldsymbol{\lambda} = (\xi\boldsymbol{\lambda})\boldsymbol{\lambda} = \xi\boldsymbol{\lambda}^2$.

3.9.2. Left Quaternionic Eigenvalues

Left quaternionic *eigenvalues*, that is the solutions of the equation $\boldsymbol{Q\xi} = \boldsymbol{\xi\lambda}$, have not been extensively studied in the literature, and very few results have been obtained so far.

Note that the matrix $\boldsymbol{Q} - \boldsymbol{\lambda I}$ is singular if and only if the equation $\boldsymbol{Q\xi} = \boldsymbol{\lambda\xi}$ holds for some non-zero $\boldsymbol{\xi} \in \mathbb{H}^n$. Therefore, left eigenvalues are often called *singular eigenvalues* in the literature. Wood [95] has proved the existence of a singular eigenvalue for an arbitrary quaternion matrix $\boldsymbol{Q}$. However, Wood merely proved the non-emptiness of left spectrum for a quaternion matrix $\boldsymbol{Q}$, without providing any algorithm for computation of left eigenvalues.

De Leo and Rotelly [26] highlighted a few essential problems when dealing with left quaternionic eigenvalues. The first difficulty is represented by the impossibility to apply similarity transformations without losing the formal structure of the left eigenvalue equation. Since $\boldsymbol{qQ} \neq \boldsymbol{Qq}$ in general, two similar quaternion matrices do not necessarily satisfy the same eigenvalue equation. Consequently, we can have quaternion matrices with the same left eigenvalue spectrum, but no similarity transformation relating them. Second, as we recall from linear algebra, eigenvalues of the complex Hermitian matrix are always real numbers. As we have seen in the previous part, the same property extends to the right eigenvalues of a quaternion matrix. However, as De Leo et. al. show, the left eigenvalue problem could admit non-real quaternionic solutions. An example of a quaternion Hermitian matrix with left eigenvalues pure quaternions can be found in [98]. Another difficulty is that, as we can observe, the eigenvalue ‘power rule’ breaks for left eigenvalues, that is, if $\boldsymbol{\xi}$ is a left eigenvector of $\boldsymbol{Q}$ with eigenvalue $\boldsymbol{\lambda}$, it will not necessarily be a left eigenvector of $\boldsymbol{Q}^2$ with eigenvalue $\boldsymbol{\lambda}^2$. Indeed, $\boldsymbol{Q}^2\boldsymbol{\xi} = \boldsymbol{Q\lambda\xi} \neq \boldsymbol{\lambda Q\xi} = \boldsymbol{\lambda}^2\boldsymbol{\xi}$.

The most recent study of left quaternionic eigenvalues is by Huang et. al. [46,47]. In their two papers, they give an example of a 2×2 quaternion matrix with only two non-similar left eigenvalues and that is not diagonalizable, present an algorithm to compute all left eigenvalues of a 2×2 matrix, and study the possible number of distinct left eigenvalues of a quaternion matrix. They put forward a conjecture that finiteness of both left and right spectra implies their equality. A new proof of Huang et. al.'s results has been given by Macias-Virgos and Pereira-Saez [65].

Finding algorithms for computation of left eigenvalues of an arbitrary sized quaternion matrix is still an open problem.

3.10. Inner Products in Quaternion Space

The commutative linear vector spaces $\mathbb{C}^n$ and $\mathbb{R}^n$ possess a natural Euclidian inner product that allows an easy application of many geometrical concepts, such as orthogonality, in linear algebra. In this part, we introduce $\mathbb{H}$-, $\mathbb{C}$- and $\mathbb{R}$-inner products in $\mathbb{H}^n$, having regarded $\mathbb{H}^n$ as a right vector space over $\mathbb{H}$. We denote the $\mathbb{H}$-, $\mathbb{C}$- and $\mathbb{R}$-quaternionic inner products by $\langle\cdot,\cdot\rangle_{\mathbb{H}}$, $\langle\cdot,\cdot\rangle_{\mathbb{C}}$ or $\langle\cdot,\cdot\rangle_{\mathbb{R}}$ respectively.

Definition 3.11 A right vector space V over $\mathbb{H}$ is called a *quaternionic inner product space* if there is a function $\langle\cdot,\cdot\rangle_F : V \times V \to F$, where F can be $\mathbb{H}$, $\mathbb{C}$ or $\mathbb{R}$, such that for all $\boldsymbol{q} \in \mathbb{H}$ and $\boldsymbol{x}, \boldsymbol{x_1}, \boldsymbol{x_2} \in V$ the following identities hold:

1) $\langle \boldsymbol{x}, \boldsymbol{x}_1 + \boldsymbol{x}_2 \rangle_F = \langle \boldsymbol{x}, \boldsymbol{x}_1 \rangle_F + \langle \boldsymbol{x}, \boldsymbol{x}_2 \rangle_F$
2) $\langle \boldsymbol{x}_1, \boldsymbol{x}_2 \boldsymbol{q} \rangle_F = \langle \boldsymbol{x}_1, \boldsymbol{x}_2 \rangle_F \boldsymbol{q}$
3) $\langle \boldsymbol{x}_1, \boldsymbol{x}_2 \rangle_F = \overline{\langle \boldsymbol{x_2}, \boldsymbol{x}_1 \rangle_F}$
4) $\langle \boldsymbol{x}, \boldsymbol{x} \rangle_F \in \mathbb{R}$; $\langle \boldsymbol{x}, \boldsymbol{x} \rangle_F \geq 0$; and $\langle \boldsymbol{x}, \boldsymbol{x} \rangle_F = 0$ if and only if $\boldsymbol{x} = 0$.

Note that axioms (1) – (4) of Definition 3.11 lead to the important identity:

$$\langle \boldsymbol{x}_1\boldsymbol{q}_1, \boldsymbol{x}_2\boldsymbol{q}_2\rangle_F = \boldsymbol{q}_1^*\langle \boldsymbol{x}_1, \boldsymbol{x}_2\rangle_F \boldsymbol{q}_2$$

Definition 3.12 A norm of each vector $\boldsymbol{x} \in V$ is defined by $\|\boldsymbol{x}\|_F = \langle \boldsymbol{x}, \boldsymbol{x}\rangle_F$.

For such defined norm, the Cauchy-Schwartz inequality holds (Horwitz and Biedenharn [45]):

$$|\langle \boldsymbol{x}_1, \boldsymbol{x}_2\rangle_F| \leq \|\boldsymbol{x}_1\|_F \|\boldsymbol{x}_2\|_F$$

We now introduce the $\mathbb{H}$-valued inner product on the quaternion space $\mathbb{H}^n$, which satisfies conditions (1) – (4) of Definition 3.11.

Definition 3.13 (Farenick and Pidkowich [30]) The $\mathbb{H}$-valued inner product of two vectors $\boldsymbol{x}^T = \begin{bmatrix} \boldsymbol{x}_0 \\ \boldsymbol{x}_1 \\ \vdots \\ \boldsymbol{x}_{n-1} \end{bmatrix}$ and $\boldsymbol{y}^T = \begin{bmatrix} \boldsymbol{y}_0 \\ \boldsymbol{y}_1 \\ \vdots \\ \boldsymbol{y}_{n-1} \end{bmatrix}$ from $\mathbb{H}^n$ is defined by

$$\langle \boldsymbol{x}, \boldsymbol{y}\rangle_{\mathbb{H}} = \sum_{t=0}^{n-1} \boldsymbol{x}_t^*\boldsymbol{y}_t$$

Note that with so defined inner product, Definition 3.12 is fully compatible with Definition 2.5 (norm of the sequence), given in Section 2 of the present work: $\|\boldsymbol{x}\|_{\mathbb{H}} = \sum_{t=0}^{n-1} \boldsymbol{x}_t^*\boldsymbol{x}_t = \sum_{t=0}^{n-1}\|\boldsymbol{x}_t\| \overset{\text{def}}{=} \|\boldsymbol{x}\|$.

Horwitz and Biedenharn [45] introduced a ‘hierarchy’ of quaternionic inner products, defining $\mathbb{R}$- and $\mathbb{C}$-valued inner products on the quaternion space $\mathbb{H}^n$. For $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{H}^n$ the corresponding $\mathbb{R}$- and $\mathbb{C}$-valued inner products are defined as follows:

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle_{\mathbb{R}} \overset{\text{def}}{=} \operatorname{Re}(\langle \boldsymbol{x}, \boldsymbol{y} \rangle_{\mathbb{H}})$$

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle_{\mathbb{C}} \overset{\text{def}}{=} \operatorname{Re}(\langle \boldsymbol{x}, \boldsymbol{y} \rangle_{\mathbb{H}}) - \boldsymbol{i}\operatorname{Re}(\langle \boldsymbol{x}, \boldsymbol{y} \rangle_{\mathbb{H}} \boldsymbol{i})$$

It is easy to check that the $\mathbb{R}$- and $\mathbb{C}$-valued quaternionic inner products satisfy conditions (1) – (4) of Definition 3.11. The $\mathbb{R}$- and $\mathbb{C}$-valued quaternionic inner products have applications in construction of special tensor products used in quaternionic quantum physics. In the sections that follow we will only employ the $\mathbb{H}$-valued inner product, which is consistent with the action of $\mathbb{H}$ on $\mathbb{H}^n$ from the right, and the subscript ‘$\mathbb{H}$’ will often be omitted.

3.11. Linear Algebra over $\mathbb{H}$

Linear algebra over quaternions is very similar to the familiar linear algebra over the real or complex fields. Many concepts, such as basis, dimension, linear independency, are still applicable to quaternionic vector spaces. In applying familiar concepts, one must always take care of the non-commutative nature of the quaternions.

Exposition that follows in this part is generally adopted from the brilliant work of Farenick and Pidkowich [30].

Definition 3.14 If $V$is a nonzero right quaternion vector space $\mathbb{H}^n$ and if $X \subseteq V$ is a nonempty subset, then

1. X is a *generating set* for V if for some natural m
   $V = \{\sum_{t=0}^{m-1} \boldsymbol{x}_t \boldsymbol{q}_t \mid \boldsymbol{x}_0, \dots, \boldsymbol{x}_{m-1} \in X,\ \boldsymbol{q}_0, \dots, \boldsymbol{q}_{m-1} \in \mathbb{H}\}$.

2. X is an $\mathbb{H}$-*independent set* if, for any distinct, $\boldsymbol{x}_0, \dots, \boldsymbol{x}_{m-1} \in X$, the equation $\sum_{t=0}^{m-1} \boldsymbol{x}_t \boldsymbol{q}_t = 0$ is satisfied by $\boldsymbol{q}_0, \dots, \boldsymbol{q}_{m-1} \in \mathbb{H}$ only for $\boldsymbol{q}_0 = \cdots = \boldsymbol{q}_{m-1} = 0$.
3. X is a *basis* for V if X is the generating set and $\mathbb{H}$-independent.

Just like in the complex case, if there exist two bases for the same quaternion vector space V, they have the same cardinality n. The number of elements n in a basis is called a *dimensionality* of the quaternion vector space V. An analogue of the Gram-Schmidt Theorem holds for quaternion vector spaces.

Theorem 3.1 If V is an n-dimension quaternion vector space, then for any $\boldsymbol{x}_0 \in V$, such that $\|\boldsymbol{x}_0\| = 1$, there exist $\boldsymbol{x}_1, \dots, \boldsymbol{x}_{m-1} \in V$, such that

1. $X = \{\boldsymbol{x}_0, \dots, \boldsymbol{x}_{m-1} \in V\}$ is a basis for V.
2. $\|\boldsymbol{x}_t\| = 1$ for every $t = 1, \dots, m-1$.
3. $\langle \boldsymbol{x}_{t_1}, \boldsymbol{x}_{t_2} \rangle_{\mathbb{H}} = 0$ if $t_1 \neq t_2$.

Proof. Refer to Farenick and Pidkowich [30], Theorem 4.3, for proof.□

By establishing an isomorphism between the set of *endomorphisms* on a n-dimension right $\mathbb{H}$-vector space V, that is a function $T: V \rightarrow V$ satisfying $T(\boldsymbol{x}_1 + \boldsymbol{x}_2) = T(\boldsymbol{x}_1) + T(\boldsymbol{x}_2)$ and $T(\boldsymbol{x}\boldsymbol{q}) = T(\boldsymbol{x})\boldsymbol{q}$ for all $\boldsymbol{x}_1, \boldsymbol{x}_2 \in V$ and $\boldsymbol{q} \in \mathbb{H}$, and the set of quaternion matrices $M_n(\mathbb{H})$, Farenick and Pidkovich [30] show that, for every quaternion matrix $\boldsymbol{Q} \in M_n(\mathbb{H})$, there exists a unique quaternion matrix $\boldsymbol{P} \in M_n(\mathbb{H})$, such that $\langle \boldsymbol{Q}\boldsymbol{x}_{t_1}, \boldsymbol{x}_{t_2} \rangle_{\mathbb{H}} = \langle \boldsymbol{x}_{t_1}, \boldsymbol{P}\boldsymbol{x}_{t_2} \rangle_{\mathbb{H}}$ for all $\boldsymbol{x}_1, \boldsymbol{x}_2 \in V$. Moreover, $\boldsymbol{P} = \boldsymbol{Q}^*$.

3.12. Finite Quaternion Groups

Note that all quaternions belonging to some finite quaternion group must be of norm 1. Therefore, any finite quaternion group consists of exclusively unit quaternions.

All possible finite quaternion groups are known and classified. The first comprehensive description of all finite groups over the real quaternions has been given by Stringham [86] as early as 1881. There only exist five types of finite quaternion groups.

- Type 1 is a class of cyclic groups. These groups are of the form $\boldsymbol{C} = \{1, \boldsymbol{q}, \boldsymbol{q}^2, \dots, \boldsymbol{q}^{m-1}\}$, where $\boldsymbol{q}$ is any unit quaternion of finite order m. For every integer number m, there exists a cyclic quaternion group of order m. Groups of this type can be regarded as a kind of '2-dimensional' structures, meaning that all their elements belong to a 2-dimensional plane passing through the origin. Groups of complex roots of unity are a special case of quaternion groups of this type.

- Type 2, the *double pyramid* groups, consists of groups of the form $\boldsymbol{P} = \{1, \boldsymbol{q}, \boldsymbol{q}^2, \dots, \boldsymbol{q}^{2m-1}\} \cup \{\boldsymbol{p}, \boldsymbol{pq}, \boldsymbol{pq}^2, \dots, \boldsymbol{pq}^{2m-1}\}$, where $\boldsymbol{q}$ is any unit quaternion of even order $2m$, and $\boldsymbol{p}$ is a unit quaternion orthogonal to $\boldsymbol{q}$ with zero real part. The order of groups of this type is always a multiple of 4. The double pyramid group of order $4m$ contains a cyclic subgroup of order $2m$. The well-known *i-j-k group* $\boldsymbol{Q}_8$ of order 8, formed by unit quaternions $\pm 1, \pm\boldsymbol{i}, \pm\boldsymbol{j}, \pm\boldsymbol{k}$, is a special case of the double pyramid group, for $\boldsymbol{q} = \boldsymbol{i}$, $\boldsymbol{p} = \boldsymbol{j}$, $m = 2$.

- Type 3 consists of only one group, the *double tetrahedron* group $\boldsymbol{Q}_{24}$, of order 24. This is a group generated by two unit quaternions, $\boldsymbol{i}$ and $\frac{1+\boldsymbol{i}+\boldsymbol{j}+\boldsymbol{k}}{2}$. Elements of this group are unit quaternions $\pm 1, \pm\boldsymbol{i}, \pm\boldsymbol{j}, \pm\boldsymbol{k}$, along with unit quaternions of the form $\frac{\pm 1 \pm \boldsymbol{i} \pm \boldsymbol{j} \pm \boldsymbol{k}}{2}$ for all possible combinations of the $\pm$ signs. $\boldsymbol{Q}_8$ is a subgroup in $\boldsymbol{Q}_{24}$.

- Type 4 also consists of only one group, the *double octahedron* group $\boldsymbol{Q}_{48}$, of order 48. This group is generated by two unit quaternions, $\frac{1+\boldsymbol{i}}{\sqrt{2}}$ and $\frac{\boldsymbol{i}+\boldsymbol{j}}{\sqrt{2}}$. $\boldsymbol{Q}_8$ and $\boldsymbol{Q}_{24}$ are subgroups in $\boldsymbol{Q}_{48}$.

- Type 5 consists of two isomorphic groups, the *double icosahedron* groups $\boldsymbol{Q}_{120}$ and $\boldsymbol{Q}'_{120}$, of order 120. $\boldsymbol{Q}_{120}$ is generated by two unit quaternions, $\boldsymbol{i}$ and $\frac{e_1+\boldsymbol{i}-e_2\boldsymbol{k}}{2}$, where $e_1 = \frac{1+\sqrt{5}}{2}$, $e_2 = \frac{1-\sqrt{5}}{2}$. $\boldsymbol{Q}'_{120}$ is generated by $\boldsymbol{i}$ and $\frac{e_2+\boldsymbol{i}-e_1\boldsymbol{k}}{2}$. That is, generators of $\boldsymbol{Q}_{120}$ and $\boldsymbol{Q}'_{120}$ only differ by interchange of e_1 and e_2. Isomorphism between $\boldsymbol{Q}_{120}$ and $\boldsymbol{Q}'_{120}$ is established by the transformation $T: \boldsymbol{q} \to (\boldsymbol{1}-\boldsymbol{k})\boldsymbol{q}(\boldsymbol{1}-\boldsymbol{k})^{-1}$. $\boldsymbol{Q}_8$ and $\boldsymbol{Q}_{24}$ are subgroups in $\boldsymbol{Q}_{120}$ and $\boldsymbol{Q}'_{120}$, however, $\boldsymbol{Q}_{48}$ is not a subgroup in $\boldsymbol{Q}_{120}$ or $\boldsymbol{Q}'_{120}$.

There are no other finite groups over the real quaternions.

4. Perfect Sequences over the Complex Field $\mathbb{C}$

Definition 4.1 A non-zero sequence $a = [a_0, a_1, \dots, a_{n-1}]$ over the complex numbers is called *perfect* if its periodic autocorrelation function $ACF(m) = \frac{1}{\|a\|}\sum_{t=0}^{n-1} a_t a_{t+m}^*$ is equal to zero for all non-zero shifts m, $1 \leq m \leq n-1$.

Remark 4.1 In Definition 4.1, the normalizing factor $\frac{1}{\|\boldsymbol{a}\|}$ appears in the formula for the autocorrelation values. Due to presence of this factor, the autocorrelation function can not be defined for the sequence with all elements equal to zero. Such trivial sequences have no useful applications and, therefore, are beyond the interest of our research. In the present work, only non-trivial sequences, having at least one non-zero element, are considered.

Perfect sequences over the complex numbers have many applications in such diverse areas as spread spectrum multiple access systems, pulse compression radars, fast-startup equalization and channel estimation (Mow [71]).

Besides, studying the structure of perfect sequences, their properties, conditions for existence and finding generating algorithms would be extremely beneficial from purely a mathematical point of view.

In this section, we discuss the necessary and sufficient condition for perfection of sequences with elements in the complex field $\mathbb{C}$, consider some useful properties, and give a brief description of various known types of perfect sequences. Finally, the question of existence of perfect sequences is briefly discussed.

In the literature, when talking about complex perfect sequences, many authors are only considering sequences over the n-th complex roots of unity. Different sources call such sequences *polyphase*, *unimodular*, or *phase-shift keying (PSK)* sequences. In many cases, the results about perfect sequences over the roots of unity can without difficulty be extended to sequences over arbitrary complex numbers. In this work, we do not restrict attention to considering sequences over the roots of unity only. Most of the results listed below are applicable to sequences over arbitrary complex numbers. Where it is not the case, an explicit notice is given.

4.1. Necessary and Sufficient Condition for Perfection over Complex Numbers

We start with stating the necessary and sufficient condition for perfection over $\mathbb{C}$.

Connection between perfect polyphase sequences and special properties of their discrete Fourier transforms has been known for quite a few decades. Chung and Kumar initiated the study of bent functions, which are defined as functions $f: \mathbb{Z}_n^m \to \mathbb{Z}_n$ with the property that all discrete Fourier coefficients of the *bent sequence* $[\omega_n^{f(0)}, \dots, \omega_n^{f(n-1)}]$, where ω is a primitive n-th root of unity, have unit magnitude. Chung and Kumar [22] have made a remark that bent sequences have ideal autocorrelation properties.

In his PhD Thesis (1993), Wai Ho Mow considers constructions of perfect sequences involving bent functions. Mow has mentioned, and used in his Thesis, the fact that the polyphase sequence $y = [y_0, y_1, \dots, y_{n-1}]$ is perfect if and only if $|[DFT(y)]_t| = 1$, for all $0 \leq t \leq n-1$. Mow's Thesis became a basis for the textbook [72], published in 1995, two years after submission of the Thesis.

Fan and Darnell [29] consider conditions for perfection of a sequence $a = [a_0, \dots, a_{n-1}]$, $a_0, \dots, a_{n-1} \in \mathbb{C}$, in their paper published in the same year 1995. They have stated that the property of having all discrete Fourier transform coefficients of equal magnitude, $|A_0| = \cdots = |A_{n-1}|$, is a necessary and sufficient condition for a sequence a to be perfect.

Mow's version and Fan and Darnell's version differ only in use of normalizing factor.

Another use of the above equivalence of perfection of a sequence with its Fourier transform coefficients being of equal norm is found in works of Gabidulin [34,35] and Gabidulin and Shorin [36], where perfect sequences are also constructed.

However, none of the authors have presented a formal proof of this important condition for perfection. Here below we give a statement of this result and a formal proof.

Proposition 4.1 Let $x = [x_0, x_1, \dots, x_{n-1}]$ be a sequence with elements in the complex field $\mathbb{C}$. The sequence x is perfect if and only if all its discrete Fourier transform coefficients $X_s = \sum_{t=0}^{n-1} x_t \, e^{-\frac{2\pi i}{n}st}$, $0 \leq s \leq n-1$, are of equal norm.

Proof. (i) First, assume that $\|X_0\| = \cdots = \|X_{n-1}\| = c$. We show x is perfect.

Let $X = [X_0, \dots, X_{n-1}]$. Consider the autocorrelation function of the sequence $x = [x_0, x_1, \dots, x_{n-1}]$ for some non-zero shift m, $1 \leq m \leq n-1$.

$$ACF_x(m) = \frac{1}{\|x\|} \sum_{s=o}^{n-1} x_s^* x_{s+m} = \frac{1}{\|x\|} \sum_{s=o}^{n-1} ([DFT^{-1}(X)]_s)^* [DFT^{-1}(X)]_{s+m}$$

$$= \frac{1}{\|x\|} \sum_{s=o}^{n-1} \left(\frac{1}{n} \sum_{t_1=0}^{n-1} X_{t_1} e^{\frac{2\pi i}{n} s t_1} \right)^* \left(\frac{1}{n} \sum_{t_2=0}^{n-1} X_{t_2} e^{\frac{2\pi i}{n}(s+m)t_2} \right)$$

$$= \frac{1}{\|x\| n^2} \sum_{s=0}^{n-1} \sum_{t_1=0}^{n-1} \sum_{t_2=0}^{n-1} X_{t_1}^* X_{t_2} e^{-\frac{2\pi i}{n} s t_1 + \frac{2\pi i}{n}(s+m)t_2}$$

$$= \frac{1}{\|x\| n^2} \sum_{s=0}^{n-1} \sum_{t_1=0}^{n-1} \sum_{t_2=0}^{n-1} X_{t_1}^* X_{t_2} e^{\frac{2\pi i}{n}(s(t_2 - t_1) + m t_2)}$$

$$= \frac{1}{\|x\| n^2} \sum_{t_1=0}^{n-1} X_{t_1}^* \sum_{t_2=0}^{n-1} X_{t_2} e^{\frac{2\pi i}{n} m t_2} \sum_{s=0}^{n-1} e^{\frac{2\pi i}{n} s (t_2 - t_1)}$$

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

$$= \frac{n}{\|x\|n^2} \sum_{t_1=0}^{n-1} X_{t_1}^* X_{t_1} e^{\frac{2\pi i}{n}mt_1} = \frac{1}{\|x\|n} \sum_{t_1=0}^{n-1} \|X_{t_1}\| e^{\frac{2\pi i}{n}mt_1} = \frac{c}{\|x\|n} \sum_{t_1=0}^{n-1} e^{\frac{2\pi i}{n}mt_1} = 0$$

since $\sum_{t_1=0}^{n-1} e^{-\frac{2\pi i}{n}mt_1}$ is the sum of all n-roots of unity.

So, $ACF_x(m) = 0$, and this is true for all non-zero shifts m, $1 \le m \le n-1$. Thus, $x = [x_0, x_1, \dots, x_{n-1}]$ is perfect.

(ii) On the other hand, assuming that $x = [x_0, x_1, \dots, x_{n-1}]$ is perfect, we have

$$\begin{aligned}
\|X_m\| = X_m^* X_m &= \left(\sum_{t_1=0}^{n-1} x_{t_1} e^{-\frac{2\pi i}{n}mt_1}\right)^* \left(\sum_{t_2=0}^{n-1} x_{t_2} e^{-\frac{2\pi i}{n}mt_2}\right) \\
&= \left(\sum_{t_1=0}^{n-1} x_{t_1}^* e^{\frac{2\pi i}{n}mt_1}\right)\left(\sum_{t_2=0}^{n-1} x_{t_2} e^{-\frac{2\pi i}{n}mt_2}\right) = \sum_{t_1=0}^{n-1}\sum_{t_2=0}^{n-1} x_{t_1}^* x_{t_2} e^{\frac{2\pi i}{n}m(t_1-t_2)} \\
&= \sum_{t_1=0}^{n-1}\sum_{s=0}^{n-1} x_{t_1}^* x_{t_1-s} e^{-\frac{2\pi i}{n}ms} = \sum_{s=0}^{n-1} e^{-\frac{2\pi i}{n}ms} \sum_{t_1=0}^{n-1} x_{t_1}^* x_{t_1-s} \\
&= \sum_{s=0}^{n-1} e^{-\frac{2\pi i}{n}ms} \|x\| ACF_x(-s) = \|x\| \sum_{s=0}^{n-1} \left(ACF_x(s)\right)^* e^{-\frac{2\pi i}{n}ms} = \|x\|
\end{aligned}$$

The last equality above holds, because $ACF_x(s) = 1$ for $s = 0$ and $ACF_x(s) = 0$ otherwise.

Thus, all discrete Fourier transform coefficients of a perfect sequence have equal norm, which is exactly the norm of the original sequence x, $\|X_0\| = \cdots = \|X_{n-1}\| = \|x\|$. □

4.2. Properties of Perfect Sequences over $\mathbb{C}$

In this section, some basic properties of perfect sequences are discussed.

4.2.1. Transformations Preserving Perfection

Fan and Darnell [29] list the following properties of perfect sequences over roots of unity:

If $a = [a_t]_{0\le t\le n-1}$ is a polyphase perfect sequence, then so are

1. $[a_{t\pm m}]_{0\le t\le n-1}$, where m is any integer and the subscript is expressed $modulo\ n$;
2. $[ca_t]_{0\le t\le n-1}$, where c is any complex constant;
3. $[a_t\beta^{mt}]_{0\le t\le n-1}$, where m is any integer and β is an n-th root of 1;
4. $[a_t^*]_{0\le t\le n-1}$, where a_t^* denotes complex conjugation;
5. $[[DFT(a)]_t]_{0\le t\le n-1}$, the discrete Fourier transform of a.

Note that properties 1 – 4 hold for perfect sequences over arbitrary complex numbers. The proof of properties 1, 2 and 4 is not complicated and directly follows from the definition of perfection, therefore, omitted here; proof for property 3 is presented in Section 7 of the present work, Corollary 7.1. Property 5 is valid for any sequence with elements of equal norm, not necessarily a perfect one. Refer to Proposition 4.2 below.

<u>Proposition 4.2</u> Let $x = [x_0, x_1, \dots, x_{n-1}]$ be a sequence over the complex numbers with all elements of equal norm. Then the discrete Fourier transform $DFT(x) = [X_0, X_1, \dots, X_{n-1}]$ is perfect.

<u>Proof.</u> Assume that $\|x_0\| = \cdots . = \|x_{n-1}\| = c$. Consider the autocorrelation function of the sequence $DFT(x) = [X_0, X_1, \dots, X_{n-1}]$ for some non-zero shift m:

$$ACF_{DFT(x)}(m)=\frac{1}{\|X\|}\sum_{s=o}^{n-1}X_s^*X_{s+m}=\frac{1}{\|X\|}\sum_{s=o}^{n-1}\left(\sum_{t_1=0}^{n-1}x_{t_1}e^{-\frac{2\pi i}{n}st_1}\right)^*\left(\sum_{t_2=0}^{n-1}x_{t_2}e^{-\frac{2\pi i}{n}(s+m)t_2}\right)$$

$$=\frac{1}{\|X\|}\sum_{s=0}^{n-1}\sum_{t_1=0}^{n-1}\sum_{t_2=0}^{n-1}x_{t_1}^*e^{\frac{2\pi i}{n}st_1}x_{t_2}e^{-\frac{2\pi i}{n}(s+m)t_2}$$

$$=\frac{1}{\|X\|}\sum_{s=0}^{n-1}\sum_{t_1=0}^{n-1}\sum_{t_2=0}^{n-1}x_{t_1}^*x_{t_2}e^{\frac{2\pi i}{n}(s(t_1-t_2)-mt_2)}$$

$$=\frac{1}{\|X\|}\sum_{t_1=0}^{n-1}x_{t_1}^*\sum_{t_2=0}^{n-1}x_{t_2}e^{-\frac{2\pi i}{n}mt_2}\sum_{s=0}^{n-1}e^{\frac{2\pi i}{n}s(t_1-t_2)}$$

The last summation $\sum_{s=0}^{n-1}e^{\frac{2\pi i}{n}s(t_1-t_2)}$ represents a sum 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 it is equal to n. Therefore, the equality above continues as

$$=\frac{n}{\|X\|}\sum_{t_1=0}^{n-1}x_{t_1}^*x_{t_1}e^{-\frac{2\pi i}{n}mt_1}=\frac{n}{\|X\|}\sum_{t_1=0}^{n-1}\|x_{t_1}\|e^{-\frac{2\pi i}{n}mt_1}=\frac{nc}{\|X\|}\sum_{t_1=0}^{n-1}e^{-\frac{2\pi i}{n}mt_1}=0$$

since $\sum_{t_1=0}^{n-1}e^{-\frac{2\pi i}{n}mt_1}$ is a sum all of n-roots of unity.

Thus, $ACF_{DFT(x)}(m)=0$. Since it is true for all non-zero shifts m, $0\le m\le n-1$, we have $DFT(x)=[X_0,\dots,X_{n-1}]$ is perfect. □

The above list of properties can be appended by another one (Gabidulin and Shorin [36]): A proper decimation of a perfect sequence is perfect. That is, a sequence $a=[a_0,a_1,\dots,a_{n-1}]$ is perfect if and only if, for p relatively prime with n, its (p,m)-decimation $\left[a_m,a_{m+p},\dots,a_{m+p(n-1)}\right]$ is perfect.

4.2.2. Balance Theorem

The balance theorem, called so because it involves a *balance*, the sum of all elements of a sequence, provides a necessary condition for perfection.

A version of the balance theorem was first introduced by Bomer and Antweiler [11], for two-dimensional perfect arrays over $\mathbb{C}$. Since perfect sequences are special cases of perfect arrays (they are two-dimensional arrays of size $1 \times n$), this result is fully applicable for perfect sequences.

The balance theorem states that if $a = [a_0, a_1, \dots, a_{n-1}]$ is a perfect sequence with elements from the complex field $\mathbb{C}$, then

$$\|a_0 + a_1 + \cdots + a_{n-1}\| = \|a_0\| + \|a_1\| + \cdots + \|a_{n-1}\|$$

Refer to Section 8.1, Proposition 8.1, for a formal proof.

4.2.3. Composition of Perfect Sequences

A rule for composition of two perfect sequences, first mentioned in Ipatov's text [49], is a convenient mean to form longer perfect sequences by 'multiplying' two perfect sequences of shorter lengths.

If a sequence $a = \left[a_0, \dots, a_{n_1-1}\right]$ of length n_1 and a sequence $b = \left[b_0, \dots, b_{n_2-1}\right]$ of length n_2 are perfect and n_1 and n_2 are relatively prime numbers (that is, $\gcd(n_1, n_2) = 1$), then by repeating the sequence a n_2 times and the sequence b n_1 times, and multiplying them together element-by-element, we obtain the composition sequence $c = a * b = [a_0 b_0, \dots, a_{n_1-1} b_{n_2-1}]$ of length $n = n_1 n_2$, which is also perfect (Fan and Darnell [29]).

The rule for composition of two perfect sequences of relatively prime lengths is the direct consequence of a more general result (Luke [62]). Luke introduces the *product theorem* for autocorrelation functions, which states that the autocorrelation values of the composition of two sequences of relatively prime lengths are the products of the individual autocorrelation values. That is, if sequences $a = [a_0, \dots, a_{n_1-1}]$ and $b = [b_0, \dots, b_{n_2-1}]$ are of relatively prime lengths, then the autocorrelation function of the composition $a * b$ is expressed by $ACF_{a*b}(m) = ACF_a(m)ACF_b(m)$.

4.3. Known Constructions of Perfect Sequences

In this section, a short overview of known perfect sequences over ℂ is given.

4.3.1. Perfect Sequences over ℝ

The known perfect sequences with entries from the real field ℝ can be subdivided into three major types:

- binary perfect sequences, with elements from $\{ -1, 1 \}$;
- ternary perfect sequences, with elements from $\{ -1, 0, 1 \}$;
- multilevel perfect sequences, with elements of different absolute magnitude (which may or may not include 0 among their entries).

In this section, we briefly discuss each of these types.

4.3.1.1. Binary Perfect Sequences

Although binary perfect sequences would be particularly interesting for practical applications, the only known binary perfect sequence, up to shifting and multiplying by -1, is

$$[\,1, 1, 1, -1]$$

It is widely conjectured and proved for many cases that no binary perfect sequences of longer lengths exist, refer to Section 4.4.2 below.

4.3.1.2. Ternary Perfect Sequences

In the context of perfect sequences over $\mathbb{R}$, by ternary sequences we understand sequences with entries from the set $\{\,-1, 0, 1\}$. Such perfect sequences exist, and lengths much longer than 4 are achievable in many instances.

Example 4.1 (Ipatov [49]) The sequence

$$[\,1, 1, 1, 1, 1, -1, 1, 0, 1, 0, -1, 1, 1, -1, 0, 0, 1, -1, 0, -1, -1]$$

is a perfect ternary sequence of length 21.

Study of ternary perfect sequences was initiated in the mid 1960's by Chang [17]. By considering a relationship between the numbers of '1', '-1' and '0' among entries of a ternary perfect sequence, Chang derives a necessary condition for perfection of a ternary sequence. If we denote the number of 1's in a ternary sequence by m_+, and the number of -1's by m_-, then Chang's condition implies that the following identity necessarily holds for any perfect sequence:

$$(m_+ - m_-)^2 = m_+ + m_-$$

Chang has discovered that some sequences generated by a linear recursion relation over $\mathrm{GF}(3)$ of length $(3^n - 1)/2$ for some n's, after substitution $2 \rightarrow -1$ in their entries, satisfy this necessary condition. Manually checking for perfection those of them which satisfy the necessary condition, Chang found examples of perfect ternary sequences of lengths 13, 121, and 1093.

In his paper, Chang refers to the earlier work of Tompkins [90], who has listed all ternary perfect sequences up to length 18.

Moharir [69] continues the reasoning line of Chang, and finds more necessary conditions (he calls them *combinatorial admissibility conditions*) for perfection of a ternary sequence. Based on these results, Moharir suggests an algorithm for optimization of an exhaustive search of ternary perfect sequences of longer lengths. Application of Mohair's algorithm provides a significant reduction in computer running time for performing a search for longer perfect sequences.

Many known constructions involve certain transformations of *m-sequences*, or other *linear shift register sequences*. For a good introduction to m-sequences and linear shift register sequences refer to Simon et. al. [84].

Shedd and Sarwate [83], using the formulae of Helleseth [40] for cross-correlation functions, suggest two constructions, based on two m-sequences over $\mathrm{GF}(p)$ of a special form of length $p^n - 1$, for perfect ternary sequences of length $p^n - 1$. One of the proposed constructions is applicable in the case $p = 2$, another in the case when p is an odd prime. Shedd and Sarwate presented examples of ternary perfect sequences of length 31 and 26.

Ipatov [50] has introduced a large class of ternary sequences of length $(q^n - 1)/(q - 1)$, derived from linear shift register sequences over $\mathrm{GF}(q^n)$, for odd n and $q = p^s$, where p is an odd prime.

Using results from difference set theory, Hoholdt and Justesen [41] present a construction of ternary perfect sequences of length $(q^{2m+1} - 1)/(q - 1)$, where $q = 2^s$. Although the details of their construction are rather complicated, the suggested method for generating perfect sequences is quite simple. For $s = 1$, that is $q = 2$, their construction coincides with that of Shedd and Sarwate.

4.3.1.3. Multilevel Perfect Sequences over ℝ

Except for the special case of ternary sequences, multilevel perfect sequences have not been extensively studied in the literature.

Luke [62] introduces and studies *amplitude asymmetrical* (two-level) binary perfect sequences. Luke shows that, since the autocorrelation function of a binary m-sequence has the constant value of -1 for all non-zero shifts (refer to Sarwate and Pursley [80]), any binary m-sequence can be made into a perfect two-level sequence by substitution of all '-1' entries by a suitable (rational) number q.

<u>Example 4.2</u> The binary m-sequence $[1, 1, -1]$ over GF(2) of length $3 = 2^2 - 1$ becomes perfect after substitution $-1 \to q = -\frac{1}{2}$. It is easy to manually check that the two-level sequence $\left[1, 1, -\frac{1}{2}\right]$ is perfect.

Three-level *Legendre sequences* $x = \left[x_1, \dots, x_p\right]$, which, for every prime p and $1 \le t \le p$ are defined by

$$x_t = \begin{cases} 0, \text{ if } x_t = 0 \; mod \; p \\ 1, \text{ if } t \text{ is a quadratic residue } mod \; p \\ -1, \text{ if } t \text{ is quadratic non residue } mod \; p \end{cases},$$

can be modified in the same manner. Luke provides the following example of three-level perfect sequence derived from a Legendre sequence of length 17:

Example 4.3 (Luke [62], Table I) The following sequence, derived from a Legendre sequence of length 17 by substitution $-1 \to -0.61$ and $0 \to 0.2$, is three-level perfect of length 17:

$$[\,1, 1, -0.61, 1, -0.61, -0.61, -0.61, 1, 1, -0.61, -0.61, -0.61\,, 1, -0.61, 1, 1, 0.2]$$

A similar construction has been proposed by Darrnell and Fan [25]. Concatenating together two copies of the same m-sequence $x = [x_0, \dots, x_{n-1}]$ over $\mathrm{GF}(p)$, where p is prime and the length, given by $n = p^m - 1$, is such that $n = 2t$ with t an odd number, in the *inverse-repeat* manner (that is, the resulting sequence is an anti-symmetric sequence of length $2n$ (Tomlinson [89])), and performing the appropriate substitutions, we get a *quasi-perfect* p-level sequence $a = [a_0, \dots, a_{2n-1}]$, the autocorrelation function of which is given by

$$ACF_a(m) = \begin{cases} P, & \text{if } m = 0 \\ -P, & \text{if } m = n \\ 0, & \text{otherwise} \end{cases}, \text{ for some } P.$$

If this quasi-perfect sequence is combined with the sequence $b = [(-1)^t]$, $0 \le t \le 2n - 1$, of the same length $2n$ using the element-by-element multiplication, the resulting sequence $c = [c_0, \dots, c_{2n-1}]$ will be p-valued multilevel of length $2n$ and period n. A ‘half’ of this sequence, representing one period, will be a perfect sequence of length n.

Darrnell and Fan [25] give an example of such a perfect sequence for the values $p = 3$, $m = 3$, and $p^m - 1 = 26$. The resulting perfect sequence, shown in Example 4.4, is a ternary perfect sequence. However, different number of levels can be achieved by application of this method for different values of p.

Example 4.4 (Darnell and Fan [25]) The following sequence is two-level perfect:

$$[0, -1, 1, -1, 0, 0, -1, 0, -1, -1, -1, 1, 1]$$

Bomer and Antweiler [10] suggest another construction of three-level real valued perfect sequence. Based on an arbitrary m-sequence $x = [x_0, \dots, x_{n-1}]$ over $\mathrm{GF}(q)$ of length $n = q^m - 1$, where $q = p^s$ for some prime p, the new perfect sequence $a = [a_0, \dots, a_{n-1}]$ is defined by

$$a_t = \begin{cases} 1, & \text{if } x_t = 0 \\ b_1, & \text{if } x_t = 1 \\ b_2, & \text{else} \end{cases}, \text{ for } 0 \le t \le n-1.$$

The sequence a 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 $(4(q-2) + (q-3)^2)b_2^4 + 4(q-1)b_2^3 + \big(4c_1 - 2c_2(q-1)\big)b_2^2 - 4c_2 b_2 + c_2^2 = 0$,

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

4.3.2. Perfect Polyphase Sequences

Due to an abundance of potential applications, perfect sequences over the roots of unity are comparatively well exposed in the literature.

4.3.2.1. Frank Sequences

The first publication concerning perfect sequences over the roots of unity appeared in 1961. Heimiller [39] presents a simple method of generating polyphase perfect sequences of length p^2 for a prime p. Let $1, \omega_1, \dots, \omega_{p-1}$ be p different p-th roots of unity, that is $\omega = e^{-\frac{2\pi i}{p}t}$, $0 \le t \le p - 1$. Then the sequences, suggested by Heimiller, are formed as follows.

First, we build a matrix consisting of powers of $1, \omega_1, \dots, \omega_{p-1}$:

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_1 & \omega_1^2 & \cdots & \omega_1^{p-1} \\ 1 & \omega_2 & \omega_2^2 & \cdots & \omega_2^{p-1} \\ \vdots & & & & \vdots \\ 1 & \omega_{p-1} & \omega_{p-1}^2 & \cdots & \omega_{p-1}^{p-1} \end{bmatrix}$$

The perfect sequence is then formed by concatenating together in order all terms of the first column sequence above, then all terms of the second column sequence, etc, until all column sequences are used:

$$[\,1, 1, 1, \dots, 1, 1,\ \omega_1,\ \omega_2, \dots,\ \omega_{p-1}, 1, \omega_1^2, \omega_2^2, \dots, \omega_{p-1}^2, \dots, 1, \omega_1^{p-1}, \omega_2^{p-1}, \dots, \omega_{p-1}^{p-1}]$$

Heimiller has noted that the order of the column sequences can be changed, and also any cyclic permutation of each column sequence can be substituted for the same column sequence, without affecting perfection of the resulting sequence.

Upon publishing Heimiller’s paper, Frank [33] claimed that he had obtained the same sequences more than 9 years earlier. Being employed in the aircraft manufacturing industry, Frank could only place his results in internal reports having restricted circulation. However, the appropriate Patent[1] had been issued at that time, containing a description of synchronizing systems using special properties of perfect sequences.

Moreover, Frank has noted the restriction for p to be a prime number can be withdrawn, and the above construction yields a perfect sequence over the n-th roots of unity for any positive integer n.

Heimiller has accepted Frank’s claim (Heimiller [38]). Polyphase perfect sequences of such a form are called *Frank sequences*.

4.3.2.2. Chu Sequences

---

[1] R.L.Frank, Phase Coded Communication System, U.S. Patent No 3 099 795, July 30, 1963 (filed Nov. 27, 1957)

The lengths of Frank sequences are restricted to perfect squares. Chu [21] provides a construction of polyphase perfect sequences, which exist for every length N, $N \geq 2$.

Chu sequences of length N, $a = [a_0, \dots, a_{N-1}]$, are given by

$$a_t = \begin{cases} e^{\frac{\pi M i}{N} t^2}, \text{if } N \text{ is even} \\ e^{\frac{\pi M i}{N} t(t+1)}, \text{if } N \text{ is odd} \end{cases}$$

for $0 \leq t \leq n-1$, where M is an integer relatively prime with N.

A linear phase shifts of the form $e^{\frac{2\pi M q i}{N} t}$, where q is any integer, when introduced into the sequence will not affect perfection, by Property 3 from Section 4.2.1 of the present work. Therefore, the modified sequence $b = [b_0, \dots, b_{N-1}]$, $b_t = a_t e^{\frac{2\pi M q i}{N} t}$, is also perfect. So, a more general expression for a Chu sequence is

$$b_t = \begin{cases} e^{\frac{\pi M i}{N} (t^2 + qt)}, \text{if } N \text{ is even} \\ e^{\frac{\pi M i}{N} (t(t+1) + qt)}, \text{if } N \text{ is odd} \end{cases}$$

Some sources reference Chu sequences in this more general form (Fan and Darnell [29], Popovic [75]).

After Chu had published his paper, Frank, again, remarked [32] that the same sequences had been earlier discovered by S. Zadoff, Frank's colleague in the aircraft industry. For the same reason as Frank, Zadoff could not freely publish his findings, however, another Patent[2] comprising Zadoff's results has been issued. So, Chu sequences are often referenced as *Zadoff-Chu*, or *ZC-*, *sequences* in many sources.

4.3.2.3. Alltop Sequences

---

[2] S.Zadoff, Phase Coded Communication System, U.S. Patent No 3 099 796, July 30, 1963 (filed Nov. 27, 1957)

Alltop [2] introduces a family of quadric phase sequences of odd length, which, he noted, are similar to those of Chu. For n an odd integer greater than 2, a *quadric phase* sequence $c = [c_0, \dots, c_{n-1}]$ is defined by $c_t = e^{\frac{2\pi mi}{n}t^2}$, for $0 \leq t \leq n-1$, where m is an integer relatively prime with n.

It is easy to see that Alltop sequences correspond to Chu sequences of odd length. Indeed, if we take $M = 2m$, $q = -1$ and $N = n$ (note, since m is odd and relatively prime with n, that M is relatively prime with N) in the expression for b_t, $0 \leq t \leq N-1$, we have

$$b_t = e^{\frac{\pi Mi}{N}(t(t+1)+qt)} = e^{\frac{2\pi mi}{n}t^2} = c_t.$$

4.3.2.4. P3 and P4 Codes

Lewis and Kretschmer [60] propose two other sequences. For any positive integer N, they define *P3* and *P4 codes* as follows:

(P3): $a_t = e^{\frac{\pi i}{n}t^2}$

(P4): $a_t = e^{\frac{\pi i}{n}t^2 + \pi i t}$

It is possible to show that P3 and P4 codes are also equivalent to Chu sequences (Fan and Darnell [29]).

4.3.2.5. Golomb Sequences

Zhang and Golomb [99] define another similar class of perfect polyphase sequences, which became known as *Golomb sequences*. For each integer n, $n \geq 2$, a Golomb sequence $a = [a_0, \dots, a_{n-1}]$ of length n is defined by $a_t = e^{\frac{\pi Mi}{N}t(t-1)}$, for $0 \leq t \leq n-1$.

When n is odd, a Golomb sequence is the same as the Chu sequence of the same length (more accurately, it is the shift by 1 of the Chu sequence). Thus, it is perfect.

When n is even, the length of the Golomb sequence becomes $2n$, and the sequence is not perfect, according to definition used in this work. However, Zhang and Golomb introduce the '*window autocorrelation*' with a window of size n: $ACF_a^W(m) = \sum_{t=0}^{n-1} a_t a_{t+m}^*$. Use of their windows autocorrelation instead of traditional autocorrelation retrieves the desired ideal autocorrelation properties for subsequences of length n. However, study of such autocorrelation functions lies outside the scope of the present work.

4.3.2.6. Milewski Sequences

A new elegant construction for perfect sequences of length $n = q^{2m+1}$ over the alphabet of q^{m+1}-roots of unity, for any positive integer q and $m \geq 1$, has been suggested by Milewski [66]. His construction involves concatenating a few copies of a Chu sequence, multiplied by roots of unity in special order.

Let $a = [a_0, \dots, a_{q-1}]$ be any Chu sequence of length q. We then build a $q^{m+1} \times q^m$ matrix with entries $z_{st} = a_s \omega^{st}$, where ω is a primitive q^{m+1}-root of unity, and indices of a are implied $modulo\ q$:

$$\begin{bmatrix} a_0\omega^{0\cdot 0} & \cdots & a_{q-1}\omega^{(q-1)\cdot 0} & \cdots & a_0\omega^{(q^{m+1}-q)\cdot 0} & \cdots & a_{q-1}\omega^{(q^{m+1}-1)\cdot 0} \\ a_0\omega^{0\cdot 1} & \cdots & a_{q-1}\omega^{(q-1)\cdot 1} & \cdots & a_0\omega^{(q^{m+1}-q)\cdot 1} & \cdots & a_{q-1}\omega^{(q^{m+1}-1)\cdot 1} \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_0\omega^{0\cdot (q^m-1)} & \cdots & a_{q-1}\omega^{(q-1)\cdot (q^m-1)} & \cdots & a_0\omega^{(q^{m+1}-q)\cdot (q^m-1)} & \cdots & a_{q-1}\omega^{(q^{m+1}-1)\cdot (q^m-1)} \end{bmatrix}_{q^{m+1}\times q^m}$$

The resulting perfect sequence is obtained by concatenating together, one by one, the rows of the matrix $[z_{st}]$.

4.3.2.7. Gabidulin Sequences

Two new types of perfect sequences have been proposed by the Russian mathematician E.Gabidulin [34].

The first type consists of sequences of length p^{2m}, for p an odd prime and m any positive integer. By the Euclidian division algorithm, any integer s, $0 \leq s \leq p^{2m} - 1$ can be uniquely represented as

$$s = up^m + v,$$

where $0 \leq u \leq p^m - 1$ and $0 \leq v \leq p^m - 1$.

Let ω_{p^m} be a primitive root of unity of degree p^m. A perfect sequence $a = [a_0, \dots, a_{p^{2m}-1}]$ is then constructed by

$$a_s = z_v \omega_{p^m}^{ruv}, 0 \leq s \leq p^{2m} - 1,$$

where r is any integer relatively prime with p, u and v are defined as above, and z_t, $0 \leq t \leq p^m - 1$, are arbitrary complex numbers of norm 1.

Gabidulin has commented that if all z_t's are chosen to be equal to 1, then sequences of this type turn into well known Frank sequences.

The second type consists of sequences of length p^{2m+1}, for p an odd prime and m any positive integer. Any integer s, $0 \leq s \leq p^{2m} + 1$, can be uniquely represented as

$$s = up^{m+1} + vp^m + c,$$

where $0 \leq u \leq p^m$, $0 \leq v \leq p$ and $0 \leq c \leq p^m$.

Let $b = [b_0, \dots, b_{p-1}]$ be a perfect sequence of length p, and $\omega_{p^{m+1}}$, ω_{p^m} be primitive roots of unity of degree p^{m+1}, p^m respectively. Then a perfect sequence $a = [a_0, \dots, a_{p^{2m+1}-1}]$ is constructed by

$a_s = b_v \omega_{p^{m+1}}^{cu} \omega_{p^m}^{cv}, 0 \leq s \leq p^{2m+1} - 1,$

where integers u, v and c are defined as above.

Fan and Darnell [29] have remarked that, if we choose the sequence $b = [b_0, \dots, b_{p-1}]$ to be a Chu sequence of length p, Gabidulin sequences from the second family become equivalent to Milewski sequences.

4.3.2.8. Generalized Bent Function Sequences

Definition 4.2 (Chung and Kumar [22])[3] A *generalized bent function* $f: \mathbb{Z}_q^m \to \mathbb{Z}_q$, for a positive integer q, is a function having the property that all of the Fourier transform coefficients $DFT(\lambda)$, $\lambda \in \mathbb{Z}_q^m$, of $\left[\omega^{f(0)}, \dots, \omega^{f(q-1)}\right]$, where ω is a prime q-th root of unity, defined by $DFT(\lambda) = \frac{1}{\sqrt{q^m}} \sum_{x \in \mathbb{Z}_q^m} \omega^{f(x)}\, \omega^{-\lambda^T x}$, have unit magnitude. The sequence $\left[\omega^{f(0)}, \dots, \omega^{f(q-1)}\right]$ is called a *bent sequence*.

In the special case $m = 1$ (*one-dimensional bent function*, Mow [72]), the generalized bent function $f(\cdot)$ is a mapping from an integer $t \in \mathbb{Z}_q$ to another integer $f(t) \in \mathbb{Z}_q$.

Let $f: \mathbb{Z}_q \to \mathbb{Z}_q$ be a one dimensional bent function. Then, by Proposition 4.1, Section 4.1, the bent sequence $\left[\omega^{f(0)}, \dots, \omega^{f(q-1)}\right]$ is perfect. Bent sequences form a class of perfect sequences. It is interesting to know that this class of perfect sequences includes Frank sequences and a subset of Chu sequences as special cases (Fan and Darnell [29]).

Gabidulin [35] has obtained the complete description of one-dimensional bent functions.

---

[3] Note that in the present work the Fourier transform coefficients of sequence $x = [x_0, \dots, x_{n-1}]$ are defined by $X_m = \sum_{t=0}^{n-1} x_t e^{-\frac{2\pi i}{n} mt}$, and the inverse Fourier transform coefficients are defined by $x_m = \frac{1}{n} \sum_{t=0}^{n-1} X_t e^{\frac{2\pi i}{n} mt}$ and, therefore, differs from the definition of Chung and Kumar by the constant normalizing factor $\frac{1}{\sqrt{n}}$; the presence of this normalizing factor does not make any difference in what follows.

4.3.2.9. Unified Approach of Mow

In his published textbook [72], Mow proposes a unified construction of perfect polyphase sequences and provides an explicit formula for computing such sequences.

Mow's general result states that, for any positive integers s and m, the polyphase sequence of length $n = sm^2$, given by the expression

$$\left[e^{\frac{2\pi i}{n}f(0)}, e^{\frac{2\pi i}{n}f(1)}, \dots, e^{\frac{2\pi i}{n}f(n-1)}\right],$$

where

- for $0 \le x \le m-1$, $f(x)$ is as arbitrary rational-valued function,
- for $m \le x \le n-1$, function $f(x)$ is defined by the recursive formula $f(km+l) = \frac{m^2(s+1)}{2}\left(r_0 + n_0\frac{l(l+1)}{2}\right)k^2 + m(r_1\pi(l) + n_1) + f(l)$, where $\pi(l)$, $0 \le l \le m-1$, is an arbitrary permutation of the elements in the set $\{0, 1, \dots, m\}$, and k, r_0, n_0, r_1, n_1 are arbitrary integers such that
  - $0 \le k \le sm-1$,
  - $0 \le r_0 \le s-1$, and r_0 is co-prime with s,
  - $0 \le n_0 \le s-1$, $(s+1)n_0$ is even and $r_0 + n_0\frac{l(l+1)}{2}$ is co-prime with s for all l, $0 \le l \le m-1$,
  - $0 \le r_1 \le sm-1$, and r_0 is co-prime with m,
  - n_1 is an integer, $0 \le n_1 \le sm-1$,

is perfect.

Mow shows that all classes of perfect polyphase sequences, discussed above in this section, are special cases of his unified approach.

4.3.2.10. Modulatable Perfect Sequences

Modulatable polyphase perfect sequences are sequences with ideal autocorrelation properties, which are preserved by a *modulation process*, that is multiplication by a string of complex numbers. The modulation process can be used for information transmission in spread spectrum communication systems.

Suehiro and Hatori [88] have introduced a new class of polyphase perfect sequences of length n^2. Each of their sequence can be modulated by n complex numbers of norm 1, so that the resulting modulated sequence is also perfect.

Suehiro and Hatori sequences are closely related to Frank sequences, and therefore are often called *generalized Frank sequences*.

As with Frank sequences, we also start with the familiar $n \times n$ matrix U, consisting of powers of n-roots of unity.

$$U = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_1 & \omega_1^2 & \cdots & \omega_1^{n-1} \\ 1 & \omega_2 & \omega_2^2 & \cdots & \omega_2^{n-1} \\ \vdots & & & & \vdots \\ 1 & \omega_{n-1} & \omega_{n-1}^2 & \cdots & \omega_{n-1}^{n-1} \end{bmatrix}$$

We then multiply this matrix, from the right, by a diagonal matrix

$$B = \begin{bmatrix} b_0 & 0 & \cdots & \cdots & 0 \\ 0 & b_1 & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & b_{n-1} \end{bmatrix}$$, with $b_0, \dots, b_{n-1}$ complex numbers of norm 1.

A perfect sequence $a = [a_0, \dots, a_{n^2-1}]$ of length n^2 is obtained by concatenating the rows of the product matrix

$$UB = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_1 & \omega_1^2 & \cdots & \omega_1^{n-1} \\ 1 & \omega_2 & \omega_2^2 & \cdots & \omega_2^{n-1} \\ \vdots & & & & \vdots \\ 1 & \omega_{n-1} & \omega_{n-1}^2 & \cdots & \omega_{n-1}^{n-1} \end{bmatrix} \begin{bmatrix} b_0 & 0 & \cdots & \cdots & 0 \\ 0 & b_1 & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & b_{n-1} \end{bmatrix}$$

$$= \begin{bmatrix} b_0 & b_1 & b_2 & \cdots & b_{n-1} \\ b_0 & \omega_1 b_1 & \omega_1^2 b_2 & & \omega_1^{n-1} b_{n-1} \\ b_0 & \omega_2 b_1 & \omega_2^2 b_2 & & \omega_2^{n-1} b_{n-1} \\ \vdots & \vdots & \vdots & & 0 \\ b_0 & \omega_{n-1} b_1 & \omega_{n-1}^2 b_2 & 0 & \omega_{n-1}^{n-1} b_{n-1} \end{bmatrix}$$

Thus, sequence a can be regarded as a modulated sequence obtained by modulating the original Frank sequence with complex numbers of absolute value 1.

The general definition of a generalized Frank sequence $a = [a_0, \dots, a_{n^2-1}]$ is given by the formula $a_t = b_{t_1} e^{\frac{2\pi i}{n} r t_1 t_2}$, for $0 \le t_1, t_2 \le n-1$ and $t = t_1 n + t_2$, and r is relatively prime with n (Fan and Darnell [29]).

A similar generalization of Frank sequences has been independently proposed by Gabidulin [34]. Gabidulin sequences of the first type, discussed earlier in Section 4.3.2.7 of the present work, are a special case of generalized Frank sequences for $n = p^m$ and p being an odd prime.

A modulatable generalization of Chu sequences (called *generalized chirp-like sequences*) has been developed by Popovic [77]. The new class of perfect sequences is based on an application of Chu sequences of length $n = sm^2$, where s and m are positive integers. If $a = [a_0, \dots, a_{n-1}]$, $n = sm^2$, is a Chu sequence, and $b = [b_0, \dots, b_{m-1}]$ is a sequence of m arbitrary complex numbers of norm 1, then the generalized chirp-like (GCL) sequence $c = [c_0, \dots, c_{n-1}]$ of length n is defined by $c_t = a_t b_t$, $0 \le t \le n-1$, where indices of b are taken $modulo\, m$. After substitution of defining equations for Chu sequences, the formula for GCL sequences becomes

$$c_t = \begin{cases} b_t e^{\frac{\pi r i}{n} t^2}, \text{if } n \text{ is even} \\ b_t e^{\frac{\pi r i}{n} t(t+1)}, \text{if } n \text{ is odd} \end{cases}, 0 \le t \le n-1, \gcd(r, n) = 1.$$

Popovic has shown that P4 codes are derived as a special case of GCL sequences. Besides, it is interesting to note that GCL sequences include generalized Frank sequences and Milewski sequences as subclasses (Popovic [75,76]).

4.3.3. Bomer and Antweiler Construction

Bomer and Antweiler [10] suggest 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 $\mathrm{GF}(3)$ to three complex values. Let $x = [x_0, \dots, x_{n-1}]$ be an m-sequence over $\mathrm{GF}(3)$. Then elements of a 3-level complex sequence $a = [a_0, \dots, a_{n-1}]$ are formed by the rule

$$a_t = \begin{cases} 1, & \text{if } x_t = 0 \\ b_1, & \text{if } x_t = 1 \\ b_2, & \text{else} \end{cases}, \text{ for } 0 \le t \le n-1,$$

where $b_1 = e^{i\beta_1}$, $b_2 = e^{i\beta_2}$ with $\beta_1 = \beta_2 \pm \cos^{-1} c$, $\beta_2 = \pm \cos^{-1}(c\sqrt{\frac{2}{1+c}}) \pm \frac{1}{2}\cos^{-1} c$ and $c = \frac{1-3^{m-1}}{2\cdot 3^{m-1}}$.

Note that b_1 and b_2 are not exactly equal to the 3-roots of unity, however, the phase values of b_1 and b_2 tend to $\frac{2\pi}{3}$ and $\frac{4\pi}{3}$ for increasing length n.

4.3.4. Multilevel Perfect Sequences over $\mathbb{C}$

There are very few sources on multilevel complex perfect sequences in the literature.

Using a technique, similar to that which has been employed for obtaining multilevel real valued perfect sequences, Darrnell and Fan [25] present a method of construction of multilevel complex perfect sequences of length n, where n is any integer satisfying $n = p^m - 1$ for some prime p and some integer m, and $n = 4t$ for some odd t. There is an example of such a sequence.

Example 4.5 (Darnell and Fan [25]) The following sequence is a two-level perfect sequence of length $31 = \frac{5^3-1}{4}$:

$$[\, 0, 0, -1, -1, i, 1, i, -i, 1, 1, -1, 1, 1, 1, i, 0, -1, -i, 1, -i, 0, i, 0, i, 1, -1, i, i, 0, 1, -1 \,]$$

Recently, Boztas and Parampalli [13], based on results of Lee [58], have presented a new construction of perfect sequences over a *PSK+ alphabet*, which is the set of n-roots of unity extended by adding 0. Their construction employs m-sequences over GF(q) of length $q^m - 1$, for $m = -2 \; mod \; q$, and yields a perfect sequence over the q-roots of unity plus 0 of length $\frac{q^m-1}{q-1}$.

4.4. Existence of Perfect Sequences over $\mathbb{C}$

Note that multilevel sequences exist for arbitrary long length n. Some constructions of ternary sequences of arbitrary long length, based on m-sequences or Legendre sequences of similar length, discussed in Section 4.3.1.3 of the present work. Perhaps, the simplest example of a two-level perfect sequence, which exists for every length n, is the sequence of which all elements, except one, are zeros:

Example 4.6 Two level perfect sequence of length n, for any n,

$$[\underbrace{0, \dots, 0}_{n-1}, 1]$$

The construction, due to Bomer and Antweiler, of a perfect sequence of an arbitrary long length over the alphabet of only three complex numbers, each of norm 1, is given in Section 4.3.3.

However, the situation with perfect sequences over the n-roots of unity is rather different. It is known that such sequences do not exist for many lengths. Some recent non-existence results for perfect sequences over the roots of unity of certain lengths are presented in this section.

4.4.1. Equivalent Formulation of Perfection

The existence of a perfect sequence is equivalent to the existence of a circulant Hadamard matrix.

Definition 4.3 A matrix $C \in M_n(\mathbb{R})$ with entries from $\{-1, 1\}$ with the property that any two distinct rows are orthogonal to each other, is called a *Hadamard matrix*.

Formally, the condition of mutual column orthogonality for matrix C with entries from $\{-1, 1\}$ can be expressed as $CC^T = nI$, where I is the identity matrix.

For a comprehensive introduction to Hadamard matrices refer to Horadam [43].

Definition 4.4 (Baumert [9]) A matrix $C \in M_n(\mathbb{C})$ is said to be a *circulant* if each successive row is derived from the previous row by shifting it cyclically one position to the right.

Example 4.7 (Baumert [9]) The matrix $\begin{bmatrix} 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \end{bmatrix}$ is circulant.

It is clear that the rows of a circulant Hadamard matrix are shifted versions of a binary perfect sequence.

Arasu and De Launey [3] extend the concept of Hadamard matrix to matrices over roots of unity.

4.4.2. Non-Existence of Non-Trivial Binary Perfect Sequences

Many non-existence statements for perfect sequences are obtained by applying results from difference set theory.

Definition 4.5 (Jungnickel and Pott [52]) 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,λ)-*difference set* if its list of differences, that is $\triangle D = \{d_1 - d_2 : d_1, d_2 \in D, d_1 \neq d_2\}$, contains each non-zero element of G precisely λ times. If G is a cyclic group, D is likewise called *cyclic*.

It is well known (Baumert [9], Jungnickel and Pott [53], Hoholdt [42]) that there exists a one-to-one correspondence between binary sequences of length n with two-level autocorrelation function (that is, all autocorrelation coefficients for every non-zero shift are equal to some constant γ) and cyclic difference sets in $\mathbb{Z}_n$.

Indeed, if D is a (n,m,λ)-difference set in $\mathbb{Z}_n$, we construct a binary sequence $x = [x_0, x_1, \dots, x_{n-1}]$ by

$$x_t = \begin{cases} 1, & \text{if } t \in D \\ -1, & \text{if } t \notin D \end{cases}, \quad 0 \leq t \leq n-1.$$

The autocorrelation function of x is then given by

$$ACF_x(m) = \begin{cases} n, \text{ if } m = 0 \bmod n \\ n - 4(m - \lambda), \text{ if } m \neq 0 \bmod n \end{cases}, \; 0 \leq t \leq n - 1.$$

For a perfect binary sequence all autocorrelation coefficients for every non-zero shift are equal to zero ($\gamma = 0$), and, as shown in [9], for a difference set D to exist in $\mathbb{Z}_n$, n has to be an even square, $n = 4u^2$ 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* (Jungnickel and Pott [52]).

The only known example of Hadamard difference set is the trivial $(4,1,0)$-difference set, corresponding to the *trivial* binary perfect sequence $[1,1,1,-1]$ of length 4. It has been widely conjectured that no other Hadamard difference sets exist. The conjecture is commonly known as the *'circulant Hadamard matrix conjecture'*, due to the related concept of circulant Hadamard matrix, briefly explained above.

Many attempts have been undertaken towards finding a proof of non-existence of other Hadamard difference sets, and many important results have been obtained on the way, however, the circulant Hadamard matrix conjecture is still unsolved. The history and recent status of the circulant Hadamard matrix conjecture is as follows.

Turyn [91] has proved that if a Hadamard $(4u^2, 2u^2 - u, u^2 - u)$-difference set exists, u must be an odd number. Baumert [9] has shown that non-trivial Hadamard difference sets can only exist for $u \geq 55$. This means that there are no Hadamard difference sets for n in the range $4 < n < 12100$. Using the results of Schmidt [81], Jungnickel and Pott [53] have been able to improve the result of Baumert, demonstrating that Hadamard difference sets with u in the range $1 < u \leq 10000$ do not exist, with possible exceptions of

$u \in \{165, 231, 1155, 2145, 2805, 3255, 3905, 5115, 5187, 6699, 7161, 8151, 8645, 9867\}$.

Since then, there has not been any more progress towards proving the circulant Hadamard matrix conjecture.

A paper of Xian [96], in which the author claimed he presented a proof of the circulant Hadamard matrix conjecture, appeared in 1987. However, shortly following this publication, Mitchell [68] has commented that the proof was not correct, and gave a counter-example, which highlighted the flaw in the proof.

4.4.3. Non-Existence Results for Quaternary Sequences

The term *'quaternary sequences'* refers to sequences over the 4-roots of unity, i.e. with entries from the set $\{\pm 1, \pm i\}$. There are some results regarding the non-existence of quaternary perfect sequences.

Studying properties of bent sequences, Chung and Kumar [22] have proved that there are no perfect quaternary sequences of length 2^m, for $m > 4$.

Establishing equivalence between quaternary perfect sequences and 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, Arasu, De Launey and Ma [3] have obtained some results sufficient to prove that there are no quaternary perfect sequences for many orders. Applying these results, most of the orders are excluded as permissible length for a quaternary perfect sequence, leaving only 11 orders up to 1000 yet to be checked:

$260,\ 340,\ 442,\ 468,\ 520,\ 580,\ 680,\ 754,\ 820,\ 884,\ 890.$

Arasu, De Launey and Ma put forward the conjecture that there exist no quaternary perfect sequences of length greater than 16.

Parraud [74] has presented an alternative proof for the results of Arasu, De Launey and Ma and conjectured that there only exist perfect quaternary sequences of length 4, 8 and 16.

4.4.4. Non-Existence of p-ary Polyphase Perfect Sequences

Studying perfect sequences over the p-roots of unity, for p an odd prime, Ma and Ng [64] have shown that existence of such sequences is equivalent to the existence of certain kinds of difference sets. Using results from difference set theory, Ma and Ng have proved non-existence of perfect sequences of many lengths, including the following cases:

- p^s, for $s \geq 3$;
- $2p^s$, for $s \geq 1$;
- pq, for prime q, $q > p$.

4.4.5. Non-Existence of Almost p-ary Perfect Sequences

Chee et. al. [18] introduces *almost* p*-ary* sequences of length $n + 1$, which are defined as sequences of the form $[0, x_1, \dots, x_n]$, where $x_1, \dots, x_n$ are p-th roots of unity, for some p. They present some non-existence results for perfect almost p-ary sequences for certain combinations of n and p.

Also, it is shown (Luke [63]) that perfect almost binary sequences of length $n + 1$ do not exist for $n > 1$.

4.4.6. Conjecture on Non-Existence of Longer Polyphase Perfect Sequences

Considering the known constructions of perfect sequences over the n-roots of unity, discussed in Section 4.3.2 of the present work, it is easy to observe that alphabet size increases for longer perfect sequences. Note that none of the known constructions over n-roots of unity results in a perfect sequence longer than n^2.

Based on such observations, Mow has conjectured a relationship between the length of a polyphase perfect sequence and the minimum alphabet size.

<u>Conjecture 4.1</u> (Mow [71]) Let $L = sm^2$, for s, m positive integers and s is 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

$$N_{min} = \begin{cases} 2sm, & \text{for even } s \text{ and odd } m \\ sm, & \text{otherwise} \end{cases}.$$

In particular, Mow's conjecture means that over the alphabet of n-roots of unity, there are no perfect sequences of length above n^2. This statement is fully compatible with the conjectures of Arasu et. al. [3] and Parraud [74], refer to Section 4.4.3 of the present work.

5. Right and Left Perfection over the Real Quaternions

In this section we give definition of right and left perfection over the real quaternions, and introduce a very important property of perfect sequences over the real quaternions. We prove that the right perfection of any sequence implies the left perfection, and vise versa, so the concepts of right and left perfection over the real quaternions are equivalent. The results of this section have been presented by the author on the Fourth International Workshop on Signal Design and its Application in Communications, held in Fukuoka, Japan, 19-23 October 2009, and are published in the IEEE Proceedings [55].

5.1. Definition of Perfection over the Real Quaternions

Unlike complex numbers, the quaternion algebra is non-commutative. Non-commutativity of the quaternions calls for defining two alternative autocorrelation functions: right and left autocorrelation, which, in general, have non-equal values for the given sequence (refer to Example 5.1 below). Correspondingly, two definitions of perfect sequence are available.

<u>Definition 5.1</u> A non-zero sequence $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ over an arbitrary quaternion alphabet is called *right perfect* if its *right* periodic autocorrelation function $ACF_{\boldsymbol{a}}^{R}(m) = \frac{1}{\|\boldsymbol{a}\|}\sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_{t+m}^*$ is equal to zero for all non-zero shifts m, $1 \leq m \leq n-1$.

Definition 5.2 A non-zero sequence $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ over an arbitrary quaternion alphabet is called *left perfect* if its *left* periodic autocorrelation function $ACF_{\boldsymbol{a}}^{L}(m) = \frac{1}{\|\boldsymbol{a}\|}\sum_{t=0}^{n-1} \boldsymbol{a}_t^{*}\boldsymbol{a}_{t+m}$ is equal to zero for all non-zero shifts m, $1 \le m \le n-1$.

An alternative definition of left autocorrelation function, which may be perceived as a more natural way for defining it, is ${}_{Alt}ACF_{\boldsymbol{a}}^{L}(m) = \frac{1}{\|\boldsymbol{a}\|}\sum_{t=0}^{n-1} \boldsymbol{a}_{t+m}^{*}\boldsymbol{a}_t$. Since ${}_{Alt}ACF_{\boldsymbol{a}}^{L}(m) = (ACF_{\boldsymbol{a}}^{L}(m))^{*}$, the two definitions are equivalent. In this work, $ACF^{L}(m)$ will be used for the left autocorrelation function.

Example 5.1 For a sequence over the real quaternions, the set of right autocorrelation values can be different to the set of left autocorrelation values. For example, Table 5.1 below lists right and left autocorrelation values for the sequence $[-\boldsymbol{i}, -\boldsymbol{i}, 1, \boldsymbol{k}, -\boldsymbol{j}, \boldsymbol{i}]$ for all non-zero shifts m, $1 \le m \le 5$.

Table 5.1 Right and left autocorrelation values for the sequence $[-\boldsymbol{i}, -\boldsymbol{i}, 1, \boldsymbol{k}, -\boldsymbol{j}, \boldsymbol{i}]$.

m	$ACF^{R}(m)$	$\|ACF^{R}(m)\|$	$ACF^{L}(m)$	$\|ACF^{L}(m)\|$
1	$-2\boldsymbol{i} - 2\boldsymbol{k}$	8	0	0
2	$-1 - \boldsymbol{i} - \boldsymbol{j} + \boldsymbol{k}$	4	$-1 + \boldsymbol{i} - 3\boldsymbol{j} + \boldsymbol{k}$	12
3	0	0	0	0
4	$-1 + \boldsymbol{i} + \boldsymbol{j} - \boldsymbol{k}$	4	$-1 - \boldsymbol{i} + 3\boldsymbol{j} - \boldsymbol{k}$	12
5	$2\boldsymbol{i} + 2\boldsymbol{k}$	8	0	0

5.2. Equivalence of Right and Left Perfection over the Real Quaternions

Here we prove the equivalence of right and left perfection over the real quaternions. That is, a sequence over the real quaternions is right perfect if and only if it is left perfect.

Lemma 5.1 Let $\boldsymbol{x} = [\boldsymbol{x_0}, \boldsymbol{x_1}, \dots, \boldsymbol{x_{n-1}}]$ be any sequence with elements in the real quaternion algebra $\mathbb{H}$ and $ACF_{\boldsymbol{x}}^{R}(m) = \frac{1}{\|\boldsymbol{x}\|}\sum_{t=0}^{n-1} \boldsymbol{x_t}\boldsymbol{x_{t+m}^*}$ and $ACF_{\boldsymbol{x}}^{L}(m) = \frac{1}{\|\boldsymbol{x}\|}\sum_{t=0}^{n-1} \boldsymbol{x_t^*}\boldsymbol{x_{t+m}}$ be the right and the left autocorrelation functions of the sequence $\boldsymbol{x}$ respectively. Then

$$\sum_{m=0}^{n-1} \|ACF_{\boldsymbol{x}}^{L}(m)\| = \frac{1}{\|\boldsymbol{x}\|}\sum_{t_1=0}^{n-1}\sum_{t_2=0}^{n-1} \boldsymbol{x_{t_1}^*}(ACF_{\boldsymbol{x}}^{R}(t_2-t_1))\boldsymbol{x_{t_2}}$$

and

$$\sum_{m=0}^{n-1} \|ACF_{\boldsymbol{x}}^{R}(m)\| = \frac{1}{\|\boldsymbol{x}\|}\sum_{t_1=0}^{n-1}\sum_{t_2=0}^{n-1} \boldsymbol{x_{t_1}}(ACF_{\boldsymbol{x}}^{L}(t_2-t_1))\boldsymbol{x_{t_2}^*}$$

Proof.

$$\sum_{m=0}^{n-1} \|ACF_{\boldsymbol{x}}^{L}(m)\| = \sum_{m=0}^{n-1} \left\| \frac{1}{\|\boldsymbol{x}\|}\sum_{t=0}^{n-1} \boldsymbol{x_t^*}\boldsymbol{x_{t+m}} \right\|$$

$$= \left(\frac{1}{\|\boldsymbol{x}\|}\right)^2 \sum_{m=0}^{n-1} \left(\left(\sum_{t_1=0}^{n-1} \boldsymbol{x_{t_1}^*}\boldsymbol{x_{t_1+m}}\right) \left(\sum_{t_2=0}^{n-1} \boldsymbol{x_{t_2}^*}\boldsymbol{x_{t_2+m}}\right)^* \right)$$

$$= \frac{1}{\|\boldsymbol{x}\|^2}\sum_{m=0}^{n-1}\sum_{t_1=0}^{n-1}\sum_{t_2=0}^{n-1} \boldsymbol{x_{t_1}^*}\boldsymbol{x_{t_1+m}}\boldsymbol{x_{t_2+m}^*}\boldsymbol{x_{t_2}}$$

$$= \frac{1}{\|\boldsymbol{x}\|^2} \sum_{t_1=0}^{n-1} \sum_{t_2=0}^{n-1} \sum_{m=0}^{n-1} \boldsymbol{x}_{\boldsymbol{t_1}}^* \boldsymbol{x}_{\boldsymbol{t_1+m}} \boldsymbol{x}_{\boldsymbol{t_2+m}}^* \boldsymbol{x}_{\boldsymbol{t_2}}$$

$$= \frac{1}{\|\boldsymbol{x}\|^2} \sum_{t_1=0}^{n-1} \sum_{t_2=0}^{n-1} \boldsymbol{x}_{\boldsymbol{t_1}}^* \left(\sum_{m=0}^{n-1} \boldsymbol{x}_{\boldsymbol{t_1+m}} \boldsymbol{x}_{\boldsymbol{t_2+m}}^* \right) \boldsymbol{x}_{\boldsymbol{t_2}}$$

$$= \frac{1}{\|\boldsymbol{x}\|^2} \sum_{t_1=0}^{n-1} \sum_{t_2=0}^{n-1} \boldsymbol{x}_{\boldsymbol{t_1}}^* \big(\|\boldsymbol{x}\| ACF_{\boldsymbol{x}}^R (t_2 - t_1) \big) \boldsymbol{x}_{\boldsymbol{t_2}}$$

$$= \frac{1}{\|\boldsymbol{x}\|} \sum_{t_1=0}^{n-1} \sum_{t_2=0}^{n-1} \boldsymbol{x}_{\boldsymbol{t_1}}^* (ACF_{\boldsymbol{x}}^R (t_2 - t_1)) \boldsymbol{x}_{\boldsymbol{t_2}}$$

The second identity of Lemma 5.1 is proved in a similar way. □

Proposition 5.1 Let $\boldsymbol{a} = [\boldsymbol{a_0}, \boldsymbol{a_1}, \dots, \boldsymbol{a_{n-1}}]$ be any sequence over the real quaternion algebra $\mathbb{H}$. Then the sequence $\boldsymbol{a}$ is right perfect if and only if it is left perfect.

Proof. Assume that $\boldsymbol{a} = [\boldsymbol{a_0}, \boldsymbol{a_1}, \dots, \boldsymbol{a_{n-1}}]$ is a right perfect sequence. We will show that the sum of the norms of the left autocorrelation values $\sum_{m=1}^{n-1} \|ACF_{\boldsymbol{a}}^L(m)\|$, for all non-zero shifts m, is equal to zero.

By Lemma 5.1 we have

$$\sum_{m=0}^{n-1} \|ACF_{\boldsymbol{a}}^L(m)\| = \frac{1}{\|\boldsymbol{a}\|} \sum_{t_1=0}^{n-1} \sum_{t_2=0}^{n-1} \boldsymbol{a}_{\boldsymbol{t_1}}^* (ACF_{\boldsymbol{a}}^R (t_2 - t_1)) \boldsymbol{a}_{\boldsymbol{t_2}}$$

(4.1)

Since $\boldsymbol{a}$ is assumed right perfect, all right autocorrelation values are equal to zero for all non-zero shifts m: $ACF_{\boldsymbol{a}}^R(m) = 0,\ 1 \leq m \leq n-1$. Also, for any sequence $\boldsymbol{x}$ it is true that $ACF_{\boldsymbol{x}}^R(0) =$

$ACF_{\boldsymbol{x}}^{L}(0) = 1$. Then, $ACF_{\boldsymbol{a}}^{R}(t_2 - t_1) = 0$ for $t_1 \neq t_2$ and $ACF_{\boldsymbol{a}}^{R}(t_2 - t_1) = 1$ for $t_1 = t_2$, and the equality (4.1) above continues

$$= \frac{1}{\|\boldsymbol{a}\|} \sum_{t_1=0}^{n-1} \boldsymbol{a}_{t_1}^{*} \boldsymbol{a}_{t_1} = \frac{1}{\|\boldsymbol{a}\|} \cdot \|\boldsymbol{a}\| = 1$$

Thus,

$$1 = \sum_{m=0}^{n-1} \|ACF_{\boldsymbol{a}}^{L}(m)\| = 1 + \sum_{m=1}^{n-1} \|ACF_{\boldsymbol{a}}^{L}(m)\|$$

It follows that

$$\sum_{m=1}^{n-1} \|ACF_{\boldsymbol{a}}^{L}(m)\| = 0$$

Since the sum of non-negative real numbers is equal to zero, every summand is necessarily equal to zero too. Therefore, $ACF_{\boldsymbol{a}}^{L}(m) = 0$ for all non-zero shifts m, and $\boldsymbol{a}$ is left perfect by definition.

The inverse implication is proved similarly, by assuming that $\boldsymbol{a}$ is left perfect and showing that

$$\sum_{m=1}^{n-1} \|ACF_{\boldsymbol{a}}^{R}(m)\| = 0$$

This completes the proof of Proposition 5.1 □

Because, by Proposition 5.1, every right perfect sequence over the real quaternions is also left perfect, and vice versa, designations ‘right’ or ‘left’ perfect sequence are redundant. From now on, designations ‘right’ or ‘left’ for perfection will be omitted, and every right or left perfect sequence will simply be called perfect.

Corollary 5.1 Let $\boldsymbol{a} = [\boldsymbol{a_0}, \boldsymbol{a_1}, \dots, \boldsymbol{a_{n-1}}]$ be any sequence over the real quaternions. Then the sequence $\boldsymbol{a}$ is perfect if and only if its conjugate sequence $\boldsymbol{a}^* \overset{\text{def}}{=} [\boldsymbol{a_0^*}, \boldsymbol{a_1^*}, \dots, \boldsymbol{a_{n-1}^*}]$ is perfect.

Proof. Note that for any sequence $\boldsymbol{a}$ it is true that $ACF^R_{\boldsymbol{a}^*}(m) = ACF^L_{\boldsymbol{a}}(m)$. Therefore, left perfection of $\boldsymbol{a}$ implies right perfection of $\boldsymbol{a}^*$. □

6. Transformations Preserving Perfection over Quaternions

This section consists of two major parts. In Part 6.1, some basic operations over sequences with quaternionic entries are considered. In Part 6.2 we study how perfection over quaternions is affected by transformations of the quaternion space itself. Many examples, illustrating applications of the new results, are presented for easier understanding of the text.

Most results in this section are generalizations of the similar well known results on perfect sequences over the complex numbers. However, some results, presented in this section, are brand new.

6.1. Operations Preserving Perfection over Quaternions

Some elementary properties of perfect sequences over the complex numbers, considered in Section 4.2.1 of the present work, are generalized to perfect sequences over the real quaternions.

A new result, Proposition 6.5, is introduced in Section 6.1.5.

6.1.1. Perfection of a Shift of a Perfect Sequence

Proposition 6.1 A sequence $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ over the real quaternions is perfect if and only if any shift of this sequence is perfect.

Proof. The defining equations for (right) perfection of the shifted sequence ${}^{t}\boldsymbol{a} = [\boldsymbol{a}_t, \boldsymbol{a}_{t+1}, \dots, \boldsymbol{a}_{n-1}, \boldsymbol{a}_0, \dots, \boldsymbol{a}_{t-1}]$ are the same as the defining equations for (right) perfection of the original sequence $= [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$,

$ACF_{\boldsymbol{a}}^{R}(m) = \frac{1}{\|\boldsymbol{a}\|}\sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_{t+m}^{*} = 0$, $1 \leq m \leq n-1$,

with circularly shifted summands. □

6.1.2. Perfection of the Sequence Obtained from a Perfect Sequence by Multiplying its Elements by a Constant Factor

Proposition 6.2 Perfection of a sequence over the real quaternions is preserved by right (left) multiplication of each element of the sequence by a constant quaternion.

Proof. (i) Left or right multiplication of each element of a sequence by 0 produces the all-zero sequence, which is perfect.

(ii) For a sequence $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$, consider the (right) autocorrelation function of the product sequence $\boldsymbol{q} \cdot \boldsymbol{a} \cdot \boldsymbol{r} = [\boldsymbol{q}\boldsymbol{a}_0\boldsymbol{r}, \boldsymbol{q}\boldsymbol{a}_1\boldsymbol{r}, \dots, \boldsymbol{q}\boldsymbol{a}_{n-1}\boldsymbol{r}]$ for any non-zero quaternions $\boldsymbol{q}$ and $\boldsymbol{r}$.

$$\begin{aligned}
ACF_{\boldsymbol{qar}}^{R}(m) &= \frac{1}{\|\boldsymbol{q}\cdot\boldsymbol{a}\cdot\boldsymbol{r}\|}\sum_{t=0}^{n-1}(\boldsymbol{q}\boldsymbol{a}_t\boldsymbol{r})(\boldsymbol{q}\boldsymbol{a}_{t+m}\boldsymbol{r})^{*} = \frac{1}{\|\boldsymbol{q}\cdot\boldsymbol{a}\cdot\boldsymbol{r}\|}\sum_{t=0}^{n-1}\boldsymbol{q}\boldsymbol{a}_t\boldsymbol{r}\boldsymbol{r}^{*}\boldsymbol{a}_{t+m}^{*}\boldsymbol{q}^{*} \\
&= \frac{1}{\|\boldsymbol{q}\cdot\boldsymbol{a}\cdot\boldsymbol{r}\|}\sum_{t=0}^{n-1}\boldsymbol{q}\boldsymbol{a}_t\|\boldsymbol{r}\|\,\boldsymbol{a}_{t+m}^{*}\boldsymbol{q}^{*} = \frac{\|\boldsymbol{r}\|}{\|\boldsymbol{q}\cdot\boldsymbol{a}\cdot\boldsymbol{r}\|}\boldsymbol{q}\left(\sum_{t=0}^{n-1}\boldsymbol{a}_t\,\boldsymbol{a}_{t+m}^{*}\right)\boldsymbol{q}^{*} \\
&= \frac{\|\boldsymbol{r}\|}{\|\boldsymbol{q}\cdot\boldsymbol{a}\cdot\boldsymbol{r}\|}\boldsymbol{q}ACF_{\boldsymbol{a}}^{R}(m)\boldsymbol{q}^{*}
\end{aligned}$$

If we assume $\boldsymbol{a}$ is perfect, then $ACF_{\boldsymbol{a}}^{R}(m) = 0$ for every $1 \leq m \leq n-1$. Thus, $ACF_{\boldsymbol{q}\cdot\boldsymbol{a}\cdot\boldsymbol{r}}^{R}(m) = 0$, $1 \leq m \leq n-1$, and sequence $\boldsymbol{q}\cdot\boldsymbol{a}\cdot\boldsymbol{r}$ is perfect by definition. □

6.1.3. Perfection of the Sequence Obtained from a Perfect Sequence by Multiplying its Elements by Consecutive Powers of Roots of Unity

For a sequence over the real quaternions $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$, consider the sequence $\omega(\boldsymbol{x}) = [\boldsymbol{x}_0\omega^0, \boldsymbol{x}_1\omega^1, \boldsymbol{x}_2\omega^2, \dots, \boldsymbol{x}_{n-1}\omega^{n-1}]$, where $\omega = e^{\frac{2\pi s i}{n}}$ is any n-th complex root of unity, $1 \leq s \leq n-1$.

As shown by the example below, multiplication of elements of a sequence by consecutive powers of a root of unity can destroy perfection of the original sequence. That is, for a perfect sequence $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ over the real quaternions, the sequence $\omega(\boldsymbol{a}) = [\boldsymbol{a}_0\omega^0, \boldsymbol{a}_1\omega^1, \boldsymbol{a}_2\omega^2, \dots, \boldsymbol{a}_{n-1}\omega^{n-1}]$ is not, in general, perfect.

Example 6.1 The perfect sequence $\boldsymbol{a} = [\,1+\boldsymbol{j}, 1, 0, -\boldsymbol{j}]$, by right multiplication of its elements by $1, \omega, \omega^2$ and ω^3 respectively, where ω denotes the primitive 4-th root of unity $\omega = i$, transforms to the sequence

$$\omega(\boldsymbol{a}) = [\,1+\boldsymbol{j}, \boldsymbol{i}, 0, -\boldsymbol{k}]$$

which is not perfect. Indeed,

$$ACF^R(1) = \frac{1}{4}\big((1+\boldsymbol{j})\cdot\boldsymbol{i}^* + \boldsymbol{i}\cdot 0 + 0\cdot(-\boldsymbol{k})^* + (-\boldsymbol{k})\cdot(1+\boldsymbol{j})^*\big)$$

$$= \frac{1}{4}\big((-\boldsymbol{i}+\boldsymbol{k}) + 0 + 0 + (-\boldsymbol{i}-\boldsymbol{k})\big) = \frac{1}{4}\cdot(-2\boldsymbol{i}) \neq 0$$

However, by Proposition 6.3 below, in a special case, when elements of a perfect sequence commute with a root of unity, perfection is preserved by multiplication of elements of a sequence by consecutive powers of that root of unity.

<u>Lemma 6.1</u> Let $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$ be a sequence over the real quaternions. Then $\|\omega(\boldsymbol{x})\| = \|\boldsymbol{x}\|$.

<u>Proof.</u> $\|\omega(\boldsymbol{x})\| = \|[\boldsymbol{x}_0\omega^0, \boldsymbol{x}_1\omega^1, \dots, \boldsymbol{x}_{n-1}\omega^{n-1}]\| = \|\boldsymbol{x}_0\omega^0\| + \|\boldsymbol{x}_1\omega^1\| + \cdots + \|\boldsymbol{x}_{n-1}\omega^{n-1}\| = \|\boldsymbol{x}_0\|\|\omega^0\| + \|\boldsymbol{x}_1\|\|\omega^1\| + \cdots + \|\boldsymbol{x}_{n-1}\|\|\omega^{n-1}\| = \|\boldsymbol{x}_0\| + \|\boldsymbol{x}_1\| + \cdots + \|\boldsymbol{x}_{n-1}\| = \|\boldsymbol{x}\|$. □

<u>Proposition 6.3</u> If all elements of a perfect sequence $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ over the real quaternions commute with the n-th root of unity $\omega = e^{\frac{2\pi s i}{n}}$, for some $1 \leq s \leq n-1$, then $\omega(\boldsymbol{a}) = [\boldsymbol{a}_0\omega^0, \boldsymbol{a}_1\omega^1, \boldsymbol{a}_2\omega^2, \dots, \boldsymbol{a}_{n-1}\omega^{n-1}]$ is perfect.

<u>Proof.</u> First note that if all elements of the sequence $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ commute with ω, then they commute with every power $\omega^2, \dots, \omega^{n-1}$.

By Lemma 6.1, $\|\omega(\boldsymbol{a})\| = \|\boldsymbol{a}\|$. Then, for any non-zero shift m, $1 \leq m \leq n-1$, we have

$$\begin{aligned} ACF^R_{\omega(\boldsymbol{a})}(m) &= \frac{1}{\|\omega(\boldsymbol{a})\|}\sum_{t=0}^{n-1}(\boldsymbol{a}_t\omega^t)(\boldsymbol{a}_{t+m}\omega^{t+m})^* = \frac{1}{\|\boldsymbol{a}\|}\sum_{t=0}^{n-1}\boldsymbol{a}_t\omega^t\omega^{n-t-m}\boldsymbol{a}^*_{t+m} \\ &= \frac{1}{\|\boldsymbol{a}\|}\sum_{t=0}^{n-1}\boldsymbol{a}_t\omega^{n-m}\boldsymbol{a}^*_{t+m} \end{aligned}$$

Since every power of ω commutes with all elements of $\boldsymbol{a}$, the equality continues

$$= \frac{\omega^{n-m}}{\|\boldsymbol{a}\|}\sum_{t=0}^{n-1}\boldsymbol{a}_t\boldsymbol{a}^*_{t+m} = \frac{\omega^{n-m}}{\|\boldsymbol{a}\|}\cdot 0 = 0$$

Therefore, $\omega(\boldsymbol{a})$ is (right) perfect. □

Corollary 6.1 If $a = [a_0, a_1, \dots, a_{n-1}]$ is a perfect sequence over the complex numbers, then $\omega(a) = [a_0\omega^0, a_1\omega^1, a_2\omega^2, \dots, a_{n-1}\omega^{n-1}]$ is perfect, where ω is the same as in Proposition 6.3.

Proof. Complex numbers commute with ω, so $\omega(a)$ is perfect by Proposition 6.3. □

Corollary 6.2 If $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ is a perfect sequence over the real quaternions of an even length n, then the sequence $[\boldsymbol{a}_0, -\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, -\boldsymbol{a}_{n-1}]$ is perfect.

Proof. Since $(-1)^n = 1$ for any even power n, $\omega = -1$ is a n-th roots of unity for an even n. Because -1 is a real number, it commutes with any quaternion $\boldsymbol{q}$. Therefore, by Proposition 6.3, $[\boldsymbol{a}_0\omega^0, \boldsymbol{a}_1\omega^1, \dots, \boldsymbol{a}_{n-1}\omega^{n-1}] = [\boldsymbol{a}_0, -\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, -\boldsymbol{a}_{n-1}]$ is perfect. □

6.1.4. Perfection of a Proper Decimation of a Perfect Sequence

Proposition 6.4 below is a generalization of the known result on perfect sequences over the complex numbers (Gabidulin and Shorin [36]).

Proposition 6.4 A proper decimation of a prefect sequence over the real quaternions is perfect.

The *Euler function* $\varphi(n)$ of a positive integer n is defined as the number of positive integers not greater than n and co-prime with n. The poof of Proposition 6.4 will rely on the following Lemma 6.2.

Lemma 6.2 Let p and n be two positive integers, such that $p < n$ and $\gcd(p, n) = 1$, and let m be an arbitrary integer. Then, for any integer $0 \leq s \leq n-1$, the equation $(m + pt) \: mod \: n = s$ has the solution $t = (s - m)p^{\varphi(n)-1} mod \: n$; moreover, this solution is unique in the range $0 \leq t \leq n-1$.

Proof. Consider the equation $(m + pt) \: mod \: n = s$ with indeterminate t. By the Euler theorem (refer to Schroeder [82]), $p^{\varphi(n)} mod \: n = 1$. Then

$$(m + pt) \: mod \: n = s \; \Leftrightarrow$$

$$(m + pt) \: mod \: n = s \: mod \: n \; \Leftrightarrow$$

$$(m + pt)p^{\varphi(n)-1} \: mod \: n = sp^{\varphi(n)-1} mod \: n \; \Leftrightarrow$$

$$(mp^{\varphi(n)-1} + tp^{\varphi(n)}) \: mod \: n = sp^{\varphi(n)-1} mod \: n \; \Leftrightarrow$$

$$(mp^{\varphi(n)-1} mod \: n + tp^{\varphi(n)} mod \: n) \: mod \: n = sp^{\varphi(n)-1} mod \: n \xLeftrightarrow{p^{\varphi(n)} mod \: n = 1}$$

$$(mp^{\varphi(n)-1} mod \: n + t) \: mod \: n = sp^{\varphi(n)-1} mod \: n \xLeftrightarrow{0 \leq t \leq n-1}$$

$$t = \left(sp^{\varphi(n)-1} - mp^{\varphi(n)-1}\right) mod \: n \; \Leftrightarrow$$

$$t = (s - m)p^{\varphi(n)-1} \: mod \: n$$

Therefore, $t = (s - m)p^{\varphi(n)-1} \: mod \: n$ is a solution of $(m + pt) \: mod \: n = s$.

The uniqueness of the solution is proved by contradiction. Assume that there exist two positive integers t_1 and t_2, $t_1 \neq t_2$, $0 \leq t_1, t_2 \leq n-1$, such that $(m + pt_1) \: mod \: n = (m + pt2 \: mod \: n$. Then

$$(m + pt_1) \: mod \: n = (m + pt_2) \: mod \: n \; \Leftrightarrow$$

$$m \: mod \: n + pt_1 \: mod \: n = m \: mod \: n + pt_2 \: mod \: n \; \Leftrightarrow$$

$$pt_1 \: mod \: n = pt_2 \: mod \: n$$

The last equality implies that the remainders of pt_1 and pt_2 after division by n are equal. Therefore,

$$pt_1 - q_1 n = pt_2 - q_2 n \Leftrightarrow$$

$$p(t_1 - t_2) = n(q_1 - q_2) \Leftrightarrow$$

$$t_1 - t_2 = \frac{n(q_1 - q_2)}{p}$$

Since $t_1 \neq t_2$ by assumption, $t_1 - t_2$ is an integer not equal to zero. Because n is co-prime with p, p does not divide n, therefore, p must divide $q_1 - q_2$, that is, $q_1 - q_2 = pk$, for some k. Then

$$t_1 - t_2 = \frac{npk}{p} = nk$$

Since $t_1 - t_2 \neq 0$, $k = \frac{t_1 - t_2}{n} \neq 0$. Therefore, $t_1 - t_2 = |nk| \geq n$. However, because $0 \leq t_1, t_2 \leq n-1$ implies $|t_1 - t_2| \leq n-1$, we have the contradictory inequality $n \leq t_1 - t_2 \leq n-1$, meaning that our assumption of existence $t_1 \neq t_2$, $0 \leq t_1, t_2 \leq n-1$ was incorrect.

Thus, a solution for$(m + pt)\ mod\ n$ is unique in $0 \leq t \leq n-1$. □

We are now ready for a proof of Proposition 6.4.

Proof of Proposition 6.4 Let $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{n-1}]$ be a perfect sequence over the real quaternions of length n. Let k be an arbitrary positive integer such that $0 < k \leq n-1$. We denote $Dec_p^m(\boldsymbol{a})$ by $\boldsymbol{y} = [\boldsymbol{y}_0, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_{n-1}]$: $Dec_p^m(\boldsymbol{a}) = [\boldsymbol{y}_0, \boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_{n-1}]$, where p is co-prime to n.

Consider the (right) autocorrelation value for the k-th shift of the decimated sequence $\boldsymbol{y}$

$$ACF_{\boldsymbol{y}}^{R}(k) = \frac{1}{\|\boldsymbol{y}\|} \sum_{s=0}^{n-1} \boldsymbol{y}_s \boldsymbol{y}_{s+k}^{*}$$

Because $\boldsymbol{y} = [\boldsymbol{y}_0, \boldsymbol{y}_1, \boldsymbol{y}_2, \dots, \boldsymbol{y}_{n-1}]$ is the decimation of $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ by p, for every $\boldsymbol{y}_s$, $0 \le s \le n-1$, there exists $t, 0 \le t \le n-1$, so that $\boldsymbol{a}_{m+pt} = \boldsymbol{y}_s$. By solving the equation $(m + pt)\ mod\ n = s$ for all s, we find the 'pre-image' of every element $\boldsymbol{y}_s$ of the decimated sequence in the original sequence $\boldsymbol{a}$. The equation $(m + pt)\ mod\ n = s$ has the unique solution $t = (s - m)p^{\varphi(n)-1}\ mod\ n$ in $0 \le t \le n-1$ by Lemma 6.2. Therefore, with all indices assumed to be $modulo\ n$, the equality above is continued as

$$= \frac{1}{\|\boldsymbol{y}\|}\sum_{s=o}^{n-1} \boldsymbol{a}_{(s-m)p^{\varphi(n)-1}}\, \boldsymbol{a}^*_{(s+k-m)p^{\varphi(n)-1}} = \frac{1}{\|\boldsymbol{y}\|}\sum_{s=o}^{n-1} \boldsymbol{a}_{(s-m)p^{\varphi(n)-1}} \boldsymbol{a}^*_{(s-m)p^{\varphi(n)-1}+kp^{\varphi(n)-1}}$$

$$= \frac{1}{\|\boldsymbol{y}\|}\sum_{s=o}^{n-1} \boldsymbol{a}_{u_s}\boldsymbol{a}^*_{u_s+v}$$

where $u_s = (s-m)p^{\varphi(n)-1} mod\ n$, $v = kp^{\varphi(n)-1}\ mod\ n$.

Notice that the magnitude of v does not depend on s, the position in the sequence. Moreover, because the equation $(m + pt)\ mod\ n = s$ has a unique solution t such that $0 \le t \le n-1$, namely $t = (s-m)p^{\varphi(n)-1} mod\ n$ for any integer $0 \le s \le n-1$, the correspondence $t \leftrightarrow s$ is 'one-to-one'. Therefore, the set of indices $\{u_0, u_1, \dots, u_{n-1}\}$ is a permutation of the set of integers $\{0,1, \dots, n-1\}$, and $\{\boldsymbol{a}_{u_0}, \boldsymbol{a}_{u_1}, \dots, \boldsymbol{a}_{u_{n-1}}\}$ is a permutation of $\{\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}\}$. It means that every element of the sequence $\boldsymbol{a}$ necessarily appears in a proper decimated version of $\boldsymbol{a}$, and appears only once. Thus, the last summation is in fact the sum of products of every element of the sequence $\boldsymbol{a}$ by the conjugate of another element located 'v elements apart'. Up to the order of summation, it is exactly the v-th right autocorrelation value of the sequence $\boldsymbol{a}$. Therefore, by commutativity of quaternion addition, the equality is continued as

$$= \frac{1}{\|\boldsymbol{a}\|}\sum_{s=o}^{n-1} \boldsymbol{a}_s\boldsymbol{a}^*_{s+v} = ACF^R_{\boldsymbol{a}}(v) = 0$$

Because k has been chosen as an arbitrary integer $0 < k \le n-1$, the equality above holds for every non-zero shift k of the sequence $\boldsymbol{y} = Dec^m_p(\boldsymbol{a})$. Thus, the sequence $\boldsymbol{y} = Dec^m_p(\boldsymbol{a})$ is (right) perfect. □

Corollary 6.3 A sequence $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ over the real quaternions is perfect if and only if its reverse sequence, $[\boldsymbol{a}_{n-1}, \boldsymbol{a}_{n-2}, \dots, \boldsymbol{a}_0]$, is perfect.

Proof. The reverse of a sequence $\boldsymbol{a}$ is exactly the decimation of $\boldsymbol{a}$ by $n-1$:

$$[\boldsymbol{a}_{n-1}, \boldsymbol{a}_{n-2}, \dots, \boldsymbol{a}_0] = Dec_{n-1}^{n-1}[\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$$

Since $\boldsymbol{a}$ is assumed perfect, its reverse sequence is perfect by Proposition 6.4 □

Example 6.2 Consider the perfect sequence $\boldsymbol{a} = [\,-\boldsymbol{k}, 1, -\boldsymbol{k}, -\boldsymbol{i}, \boldsymbol{j}, -1, -\boldsymbol{j}, -1, \boldsymbol{j}, -\boldsymbol{i}\,]$ of length 10 (found by an exhaustive computer search). There are three integers co-prime with 10 in the range between 1 and 10: 3, 7 and 9. By Proposition 6.4, sequences

$$Dec_3^0(\boldsymbol{a}) = [\,-\boldsymbol{k}, -\boldsymbol{i}, -\boldsymbol{j}, -\boldsymbol{i}, -\boldsymbol{k}, -1, \boldsymbol{j}, 1, \boldsymbol{j}, -1\,]$$

$$Dec_7^0(\boldsymbol{a}) = [\,-\boldsymbol{k}, -1, \boldsymbol{j}, 1, \boldsymbol{j}, -1, -\boldsymbol{k}, -\boldsymbol{i}, -\boldsymbol{j}, -\boldsymbol{i}\,]$$

$$Dec_9^0(\boldsymbol{a}) = [\,-\boldsymbol{k}, -\boldsymbol{i}, \boldsymbol{j}, -1, -\boldsymbol{j}, -1, \boldsymbol{j}, -\boldsymbol{i}, -\boldsymbol{k}, 1\,]$$

are perfect. Checking these sequences with a computer confirms their perfection.

6.1.5. Perfection of a Sequence of Balances of Decimations of a Perfect Sequence

For a sequence $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$, we denote the sum of all elements by $\sum \boldsymbol{x}$:

$$\sum \boldsymbol{x} \overset{\text{def}}{=} \sum_{t=0}^{n-1} \boldsymbol{x}_t$$

The sum of all elements of a sequence is called the *balance* of the sequence.

<u>Proposition 6.5</u> Let $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ be a perfect sequence over the real quaternions and n_1, n_2 be two integers such that $n_1, n_2 \geq 2$ and $n = n_1 n_2$. Then the sequence

$$\left[\sum Dec_{n_2}^{0}(\boldsymbol{a}), \sum Dec_{n_2}^{1}(\boldsymbol{a}), \dots, \sum Dec_{n_2}^{n_2-1}(\boldsymbol{a})\right]$$

of length n_2 is perfect.

<u>Proof.</u> Note that all indices of $\boldsymbol{a}$ are understood $modulo\ n$. Let

$$\begin{aligned}\boldsymbol{A} &= \left[\sum Dec_{n_2}^{0}(\boldsymbol{a}), \sum Dec_{n_2}^{1}(\boldsymbol{a}), \dots, \sum Dec_{n_2}^{n_1-1}(\boldsymbol{a})\right] \\ &= \left[\sum_{t=0}^{n_1-1} \boldsymbol{a}_{n_2 t}, \sum_{t=0}^{n_1-1} \boldsymbol{a}_{n_2 t+1}, \dots, \sum_{t=0}^{n_1-1} \boldsymbol{a}_{n_2 t+n_2-1}\right]\end{aligned}$$

Consider the (right) autocorrelation function of sequence $\boldsymbol{A}$ for any non-zero shift m, $0 < m \leq n_2 - 1$.

$$ACF_{\boldsymbol{A}}^{R}(m) = \sum_{l=0}^{n_2-1} \sum Dec_{n_2}^{l}(\boldsymbol{a}) \left(\sum Dec_{n_2}^{l+m}(\boldsymbol{a})\right)^{*}$$

$$= \sum_{l=0}^{n_2-1} \left(\left(\sum_{t_1=0}^{n_1-1} \boldsymbol{a}_{n_2 t_1+l}\right)\left(\sum_{t_2=0}^{n_1-1} \boldsymbol{a}_{n_2 t_2+l+m}\right)^{*}\right) = \sum_{l=0}^{n_2-1} \sum_{t_1=0}^{n_1-1} \sum_{t_2=0}^{n_1-1} \boldsymbol{a}_{n_2 t_1+l} \boldsymbol{a}_{n_2 t_2+l+m}^{*}$$

$$= \sum_{t_1=0}^{n_1-1} \sum_{t_2=0}^{n_1-1} \sum_{l=0}^{n_2-1} \boldsymbol{a}_{n_2 t_1+l} \boldsymbol{a}_{n_2 t_2+l+m}^{*} = \sum_{t_1=0}^{n_1-1} \sum_{s=0}^{n_1-1} \sum_{l=0}^{n_2-1} \boldsymbol{a}_{n_2 t_1+l} \boldsymbol{a}_{n_2 (t_1+s)+l+m}^{*}$$

$$= \sum_{s=0}^{n_1-1} \sum_{t_1=0}^{n_1-1} \sum_{l=0}^{n_2-1} \boldsymbol{a}_{n_2 t_1+l} \boldsymbol{a}_{n_2 t_1+l+(n_2 s+m)}^{*} = \sum_{s=0}^{n_1-1} \sum_{t_1=0}^{n_1-1} \sum_{l=0}^{n_2-1} \boldsymbol{a}_{n_2 t_1+l} \boldsymbol{a}_{n_2 t_1+l+(n_2 s+m)}^{*}$$

$$= \sum_{s=0}^{n_1-1} ACF_{\boldsymbol{a}}^{R}(n_2 s + m)$$

Since $0 \leq s \leq n_1 - 1$, then, multiplying this inequality by the positive integer n_2 and adding the integer m, we have $m < n_2 s + m \leq n_1 n_2 - n_2 + m = n - (n_2 - m)$. Since $0 < m \leq n_2 - 1$, then $n_2 - m > 0$, and $n - (n_2 - m) < n$. Thus, $0 < n_2 s + m < n$, and $n_2 s + m \neq 0 \; mod \; n$.

Since a is assumed perfect, all its (right) autocorrelation values for any non-zero shift are zero, that is $ACF_{\boldsymbol{a}}^{R}(n_2 s + m) = 0$ for all $0 \leq s \leq n_1 - 1$ and $0 < m \leq n_2 - 1$.

The equality above continues as

$$= \sum_{s=0}^{n_1 - 1} 0 = 0$$

Thus, $ACF_{\boldsymbol{A}}^{R}(m) = 0$ for all $0 < m \leq n_2 - 1$, and the sequence $\boldsymbol{A}$ is (right) perfect. □

Example 6.3 If $[\boldsymbol{a}_0, \boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \boldsymbol{a}_4, \boldsymbol{a}_5]$ is a perfect sequence of length 6 over the real quaternions, then the sequences

$$[\boldsymbol{a}_0 + \boldsymbol{a}_3,\ \boldsymbol{a}_1 + \boldsymbol{a}_4,\ \boldsymbol{a}_2 + \boldsymbol{a}_5]$$

and

$$[\boldsymbol{a}_0 + \boldsymbol{a}_2 + \boldsymbol{a}_4,\ \boldsymbol{a}_1 + \boldsymbol{a}_3 + \boldsymbol{a}_5]$$

are both perfect.

For instance, since the sequence $\boldsymbol{a} = [\,\boldsymbol{k}, \boldsymbol{i}, \boldsymbol{k}, 1, -\boldsymbol{k}, 1\,]$ is perfect (found by an exhaustive computer search), it follows that the sequences

$$[\,1 + \boldsymbol{k}, \boldsymbol{i} - \boldsymbol{k}, 1 + \boldsymbol{k}\,]$$

and

$$[\,\boldsymbol{k}, 2 + \boldsymbol{i}\,]$$

are also perfect.

6.2. Transformations of the Quaternion Space Preserving Perfection

In the previous part of this section, we considered some transformations of quaternionic sequences preserving perfection. Such simple transformations as shifting, multiplying by a constant, decimation etc, are like elementary arithmetical operations over perfect sequences, and do not involve a transformation of the quaternion space $\mathbb{H}$ itself.

In this part, we study how transformations of the quaternion space $\mathbb{H}$ itself affect perfection of sequences with elements from $\mathbb{H}$.

<u>Proposition 6.6</u> Let $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ be a sequence with elements in the real quaternion space $\mathbb{H}$, and T be any unitary transformation of the quaternion space $\mathbb{H}$. Then the sequence $\boldsymbol{a}$ is perfect if and only if the transformed sequence $T(\boldsymbol{a}) \overset{\text{def}}{=} [T(\boldsymbol{a}_0), T(\boldsymbol{a}_1), \dots, T(\boldsymbol{a}_{n-1})]$ is perfect.

<u>Proof.</u> It is known (Coxeter [24]) that, for any unitary transformation T of the real quaternion space $\mathbb{H}$, there exist two unit quaternions $\boldsymbol{p}$ and $\boldsymbol{q}$, so that the transformation T is represented as either $T(\boldsymbol{x}) = \boldsymbol{p}\boldsymbol{x}\boldsymbol{q}$, or $T(\boldsymbol{x}) = \boldsymbol{p}\boldsymbol{x}^*\boldsymbol{q}$.

Assume $\boldsymbol{a}$ is perfect. By Corollary 5.1 the conjugate sequence $\boldsymbol{a}^*$ is perfect. Then, by Proposition 6.2, sequences $\boldsymbol{p}\boldsymbol{a}$ and $\boldsymbol{p}\boldsymbol{a}^*$are perfect for any quaternion $\boldsymbol{p}$. Then sequences $\boldsymbol{p}\boldsymbol{a}\boldsymbol{q}$ and $\boldsymbol{p}\boldsymbol{a}^*\boldsymbol{q}$ are perfect for any quaternion $\boldsymbol{q}$. Therefore, $T(\boldsymbol{a})$ is perfect.

Conversely, assume that the sequence $T(\boldsymbol{a})$ is perfect. Consider the inverse transformation T^{-1}, given by either $T^{-1}(\boldsymbol{x}) = \boldsymbol{p}^*\boldsymbol{x}\boldsymbol{q}^*$, or $T^{-1}(\boldsymbol{x}) = \boldsymbol{q}\boldsymbol{x}^*\boldsymbol{p}$. Thus T^{-1} is also a unitary transformation of the real quaternion space $\mathbb{H}$. Since $\boldsymbol{a} = T^{-1}(T(\boldsymbol{a}))$, and since $T(\boldsymbol{a})$ is assumed perfect, we have $\boldsymbol{a}$ is perfect. □

Definition 6.1 A unitary transformation T of the real quaternion space $\mathbb{H}$ is called a *symmetry transformation* of a finite alphabet A if it maps alphabet A onto itself, $T\colon A \to A$.

Example 6.4 If elements of an alphabet A represent vertices of a regular polytope, then any transformation of this polytope by rotation, reflection or inversion is a symmetry transformation of alphabet A.

Corollary 6.4 A symmetry transformation of the alphabet preserves perfection of a sequence over the real quaternions.

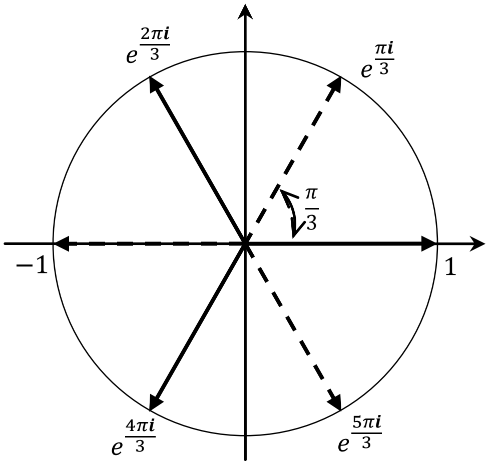
Proof. Any symmetry transformation of the alphabet is a special case of the unitary transformations of the quaternion space $\mathbb{H}$. □

Example 6.5 Consider a reflection T of the quaternion space $\mathbb{H}$ in the hyperplane passing through the origin and orthogonal to the real axis. Such a reflection T changes a sign of the real part q of every quaternion $\boldsymbol{q} = q + \vec{q} \in \mathbb{H}$, leaving its vector part $\vec{q}$ unchanged. The perfect sequence $\boldsymbol{a} = [\,-\boldsymbol{k}, 1, -\boldsymbol{k}, -\boldsymbol{i}, \boldsymbol{j}, -1, -\boldsymbol{j}, -1, \boldsymbol{j}, -\boldsymbol{i}\,]$, taken from Example 6.2 above, will transform to $T(\boldsymbol{a}) = [\,-\boldsymbol{k}, -1, -\boldsymbol{k}, -\boldsymbol{i}, \boldsymbol{j}, 1, -\boldsymbol{j}, 1, \boldsymbol{j}, -\boldsymbol{i}\,]$ by this transformation, which is also perfect.

.

Example 6.6 Consider the perfect sequence $a = [\,1, \omega, \omega\,]$ over the 3-roots of unity $\{1, \omega, \omega^2\}$, where $\omega = e^{\frac{2\pi \boldsymbol{i}}{3}}$. Since complex numbers are a special case of the real quaternions, sequences over the complex numbers will possess all properties of sequences over the quaternions. In particular, any unitary transformation of the complex space $\mathbb{C}$ preserves perfection of a sequence. Consider a transformation T of the complex space by rotation about the origin by angle $\frac{\pi}{3}$ (refer to Figure 6.1). The transformation T maps the set of 3-roots of unity into the set of 6-th roots of unity: $T(1) = e^{\frac{\pi i}{3}}$, $T(\omega) = -1$, $T(\omega^2) = e^{\frac{5\pi i}{3}}$. Proposition 6.6 ensures that the sequence $T(a) = [\, e^{\frac{\pi i}{3}}, -1, -1\,]$ over 6-th roots of unity is perfect.

Figure 6.1 Transformation of the complex space by rotation about the origin by angle $\frac{\pi}{3}$



7. Composition of Sequences over Quaternions

Some methods for building longer perfect sequences over the real quaternions are introduced in this section. The main idea behind the considered methods is a use of shorter perfect sequences, or other sequences of a special form, as ‘building blocks’ for compounding longer perfect sequences. The shorter sequences are generally found by an exhaustive computer search over some alphabet.

Two main results of this section are

- Proposition 7.1 on compounding two sequences of relatively prime length, and
- Proposition 7.2, which considers methods of compounding two sequences of even lengths.

It has been conjectured that there are no perfect sequences longer than n^2 over the n-complex roots of unity (Mow’s conjecture, refer to Section 4.4.6 of the present work). This conjecture, if true, imposes significant limits for the lengths of perfect sequences over the roots of unity, restricting a potential for practical applications which require longer sequences. In this section we demonstrate that there is no equivalent restriction for quaternion sequences. Example 7.3 shows a perfect sequence of quite impressive length, in order of a few billions, over an alphabet of 24 unit quaternions, which are quaternionic 12-roots of unity.

Proposition 7.2 introduces a brand new method for compounding two sequences of even lengths. A use of this new method for constructing new sequences of length 12 and 20 over an alphabet of 24 unit quaternions is demonstrated in Examples 7.4 and 7.5.

7.1. Composition of Sequences of Relatively Prime Lengths

Definition 7.1 Let $\boldsymbol{a} = \left[\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n_1-1}\right]$ and $\boldsymbol{b} = \left[\boldsymbol{b}_0, \boldsymbol{b}_1, \dots, \boldsymbol{b}_{n_2-1}\right]$ be two sequences over the real quaternions. The sequence $\boldsymbol{a} * \boldsymbol{b} = [\boldsymbol{a}_t \boldsymbol{b}_t]$, $t = 0, \dots, \mathrm{lcm}(n_1, n_2) - 1$, where indices of sequences $\boldsymbol{a}$ and $\boldsymbol{b}$ are understood $modulo\, n_1$ and $modulo\, n_2$ respectively, is called the *composition* of sequences $\boldsymbol{a}$ and $\boldsymbol{b}$.

If sequences $\boldsymbol{a}$ and $\boldsymbol{b}$ are of relatively prime length, then the length of the composition sequence is equal to the product of lengths of the original sequences.

Note that, dissimilar to the complex case, the product theorem for autocorrelation functions, briefly discussed in Section 4.2.3 of the present work, does not hold for sequences over quaternions. That is, the autocorrelation function of the composition sequence is not, in general, equal to the product of autocorrelations functions of the original sequences. Consider the example below:

Example 7.1 Consider two sequences $\boldsymbol{a} = [0,1,\boldsymbol{i}]$ and $\boldsymbol{b} = [0,\boldsymbol{j}]$ of relatively prime lengths. The composition of these sequences $\boldsymbol{a} * \boldsymbol{b} = [0,\boldsymbol{j},0,0,0,\boldsymbol{k}]$. Calculating autocorrelation function for shift 2, we have

$$ACF_{\boldsymbol{a}*\boldsymbol{b}}(2) = \boldsymbol{k}^*\boldsymbol{j} = \boldsymbol{i}$$

$$ACF_{\boldsymbol{a}}(2) = \boldsymbol{i}^*1 = -\boldsymbol{i}$$

$$ACF_{\boldsymbol{b}}(2) = \boldsymbol{j}^*\boldsymbol{j} = 1$$

and

$$ACF_{\boldsymbol{a}*\boldsymbol{b}}(2) \neq ACF_{\boldsymbol{a}}(2) \cdot ACF_{\boldsymbol{b}}(2).$$

As the following proposition states, the composition of two perfect sequences over the real quaternions will be perfect. However, over the quaternions, this statement is not a simple consequence of the product theorem for autocorrelation functions.

Proposition 7.1 Let $\boldsymbol{a} = \left[\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n_1-1}\right]$ and $\boldsymbol{b} = \left[\boldsymbol{b}_0, \boldsymbol{b}_1, \dots, \boldsymbol{b}_{n_2-1}\right]$ be two perfect sequences over the real quaternions so that their lengths n_1 and n_2 are relatively prime numbers. Then their composition $\boldsymbol{a} * \boldsymbol{b} = \left[\boldsymbol{a}_0\boldsymbol{b}_0, \boldsymbol{a}_1\boldsymbol{b}_1, \dots, \boldsymbol{a}_{n_1-1}\boldsymbol{b}_{n_2-1}\right]$ is perfect.

Proof. Indices of sequences $\boldsymbol{a}$ and $\boldsymbol{b}$ are understood $modulo\ n_1$ and $modulo\ n_2$ respectively.

Consider the (right) autocorrelation function of the product sequence $\boldsymbol{a} * \boldsymbol{b}$ for any non-zero shift m, $1 \le m \le (n_1 - 1)(n_2 - 1)$:

$$ACF^R_{\boldsymbol{a}*\boldsymbol{b}}(m) = \frac{1}{\|\boldsymbol{a} * \boldsymbol{b}\|} \sum_{t=0}^{n_1 n_2 - 1} \boldsymbol{a}_t \boldsymbol{b}_t (\boldsymbol{a}_{t+m} \boldsymbol{b}_{t+m})^* = \frac{1}{\|\boldsymbol{a} * \boldsymbol{b}\|} \sum_{t=0}^{n_1 n_2 - 1} \boldsymbol{a}_t \boldsymbol{b}_t \boldsymbol{b}^*_{t+m} \boldsymbol{a}^*_{t+m}$$

$$= \frac{1}{\|\boldsymbol{a} * \boldsymbol{b}\|} \sum_{t_1=0}^{n_1-1} \sum_{t_2=0}^{n_2-1} \boldsymbol{a}_{t_1} \boldsymbol{b}_{t_2} \boldsymbol{b}^*_{t_2+m} \boldsymbol{a}^*_{t_1+m}$$

$$= \frac{1}{\|\boldsymbol{a} * \boldsymbol{b}\|} \sum_{t_1=0}^{n_1-1} \boldsymbol{a}_{t_1} \left(\sum_{t_2=0}^{n_2-1} \boldsymbol{b}_{t_2} \boldsymbol{b}^*_{t_2+m} \right) \boldsymbol{a}^*_{t_1+m}$$

If $m \ne 0\ mod\ n_2$ then $\sum_{t_2=0}^{n_2-1} \boldsymbol{b}_{t_2} \boldsymbol{b}^*_{t_2+m} = 0$, since $\boldsymbol{b}$ is perfect.

If $m = 0\ mod\ n_2$ then $\sum_{t_2=0}^{n_2-1} \boldsymbol{b}_{t_2} \boldsymbol{b}^*_{t_2+m} = \sum_{t_2=0}^{n_2-1} \boldsymbol{b}_{t_2} \boldsymbol{b}^*_{t_2} = \|\boldsymbol{b}\|$.

The assumption that n_1 and n_2 are relatively prime numbers assures the condition that m, $1 \le m \le (n_1 - 1)(n_2 - 1)$, can not be equal to $0\ mod\ n_1$ and $0\ mod\ n_2$ simultaneously. Since $\boldsymbol{a}$ is perfect, its only non-zero autocorrelation values are for shifts $m = 0\ mod\ n_1$.

Therefore, the equality above continues as

$$= \begin{cases} \dfrac{1}{\|\boldsymbol{a} * \boldsymbol{b}\|} \displaystyle\sum_{t_1=0}^{n_1-1} \boldsymbol{a}_{t_1} \cdot 0 \cdot \boldsymbol{a}^*_{t_1+m} = 0, \text{if } m \neq 0 \; mod \; n_2 \\ \dfrac{1}{\|\boldsymbol{a} * \boldsymbol{b}\|} \displaystyle\sum_{t_1=0}^{n_1-1} \boldsymbol{a}_{t_1} \cdot \|\boldsymbol{b}\| \cdot \boldsymbol{a}^*_{t_1+m} = \dfrac{\|\boldsymbol{b}\|}{\|\boldsymbol{a} * \boldsymbol{b}\|} \displaystyle\sum_{t_1=0}^{n_1-1} \boldsymbol{a}_{t_1} \boldsymbol{a}^*_{t_1+m} = \dfrac{\|\boldsymbol{b}\|}{\|\boldsymbol{a} * \boldsymbol{b}\|} \cdot 0 = 0, \text{if } m = 0 \; mod \; n_2 \end{cases}$$

Thus, $ACF^R_{\boldsymbol{a}*\boldsymbol{b}}(m) = 0$ for all non-zero shifts m, $1 \leq m \leq (n_1 - 1)(n_2 - 1)$, and the composition sequence $\boldsymbol{a} * \boldsymbol{b}$ is (right) perfect by definition. □

Example 7.2 Consider perfect sequences over the *double-tetrahedron group* $\boldsymbol{Q}_{24}$ (Stringham [86]). This group of order 24 contains integer and half-integer quaternions of norm 1, i.e. $\pm\boldsymbol{1}, \pm\boldsymbol{i}, \pm\boldsymbol{j}, \pm\boldsymbol{k}$ and quaternions of the form $\frac{\pm\boldsymbol{1}\pm\boldsymbol{i}\pm\boldsymbol{j}\pm\boldsymbol{k}}{2}$ for all possible combinations of '$+$' and '$-$' signs. An exhaustive computer search for perfect sequences over $\boldsymbol{Q}_{24}$ shows that this group is remarkable in a sense that perfect sequences of both odd and even lengths over $\boldsymbol{Q}_{24}$ exist. It is possible to choose two sequences over $\boldsymbol{Q}_{24}$ of co-prime lengths, for example, lengths 5 and 6. Here are two examples, taken at random from a set of perfect sequences generated by computer search:

$$\boldsymbol{a} = [\, \frac{\boldsymbol{1} + \boldsymbol{i} + \boldsymbol{j} + \boldsymbol{k}}{2}, -\boldsymbol{i}, -\boldsymbol{j}, -\boldsymbol{j}, -\boldsymbol{i} \,]$$

$$\boldsymbol{b} = [\, \boldsymbol{k}, \boldsymbol{i}, \boldsymbol{k}, 1, -\boldsymbol{k}, 1 \,]$$

Because $\boldsymbol{Q}_{24}$ is a group, it is closed under multiplication, so the composition of two sequences above will be another sequence over the same alphabet $\boldsymbol{Q}_{24}$:

$$\boldsymbol{a} * \boldsymbol{b} = [\, \frac{-1 + \boldsymbol{i} - \boldsymbol{j} + \boldsymbol{k}}{2}, 1, -\boldsymbol{i}, -\boldsymbol{j}, -\boldsymbol{j}, \frac{1 + \boldsymbol{i} + \boldsymbol{j} + \boldsymbol{k}}{2}, \boldsymbol{j}, \boldsymbol{k}, -\boldsymbol{i}, -\boldsymbol{i}, \frac{1 - \boldsymbol{i} + \boldsymbol{j} - \boldsymbol{k}}{2}, -\boldsymbol{i}, -\boldsymbol{i}, \boldsymbol{k}, \boldsymbol{j},$$

$$\frac{1 + \boldsymbol{i} + \boldsymbol{j} + \boldsymbol{k}}{2}, -\boldsymbol{j}, -\boldsymbol{j}, -\boldsymbol{i}, 1, \frac{-1 + \boldsymbol{i} - \boldsymbol{j} + \boldsymbol{k}}{2}, -\boldsymbol{i}, \boldsymbol{i}, -\boldsymbol{j}, \boldsymbol{j}, \frac{-1 + \boldsymbol{i} + \boldsymbol{j} - \boldsymbol{k}}{2}, \boldsymbol{j}, -\boldsymbol{j}, \boldsymbol{i}, -\boldsymbol{i} \,]$$

By Proposition 7.1, $\boldsymbol{a} * \boldsymbol{b}$ is a perfect sequence of length 30.

Definition of the composition of two sequences can be generalized for an arbitrary number of sequences.

<u>Definition 7.2</u> If $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n_1-1}]$, $\boldsymbol{b} = [\boldsymbol{b}_0, \boldsymbol{b}_1, \dots, \boldsymbol{b}_{n_2-1}]$, …, $\boldsymbol{z} = [\boldsymbol{z}_0, \boldsymbol{z}_1, \dots, \boldsymbol{z}_{n_m-1}]$ are m sequences over the real quaternion algebra $\mathbb{H}$, then the sequence

$\boldsymbol{a} * \boldsymbol{b} * \dots * \boldsymbol{z} = [\boldsymbol{a}_t \boldsymbol{b}_t \dots \boldsymbol{z}_t]$, $t = 0, \dots, \mathrm{lcm}(n_1, n_2, \dots, n_m) - 1$,

where indices of $\boldsymbol{a}$ are taken $modulo\ n_1$, indices of $\boldsymbol{b}$ are taken $modulo\ n_2$, and so on, indices of $\boldsymbol{z}$ are taken $modulo\ n_m$, is called the *composition* of m sequences $\boldsymbol{a}$, $\boldsymbol{b}$, …, $\boldsymbol{z}$.

Note that if sequences $\boldsymbol{a}, \boldsymbol{b}, \dots, \boldsymbol{z}$ are of co-prime lengths, then the length of the composition sequence is equal to the product of lengths of the original sequences.

It is clear that composition of any finite number of perfect sequences of relatively prime lengths is perfect. Therefore, composing several perfect sequences of relatively prime lengths may be considered as a convenient instrument for obtaining much longer perfect sequences. Consider Example 7.3 below.

<u>Example 7.3</u> Using an exhaustive computer search over the double-tetrahedron group $\boldsymbol{Q}_{24}$, perfect sequences of relatively prime lengths $5, 7, 9, 11, 13, 17, 19$ and 23 have been found. Note that our search was restricted to *palindromic* (that is, sequences which have an elements starting with which they read the same forwards and backwards), sequences of the special form $[\, 1, \boldsymbol{j}, \boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_t, \boldsymbol{x}_t, \dots, \boldsymbol{x}_1, \boldsymbol{x}_0, \boldsymbol{j}, 1, \boldsymbol{q}\,]$, where $\boldsymbol{x}_0, \dots, \boldsymbol{x}_t \in \boldsymbol{Q}_8$ and $\boldsymbol{q} \in \boldsymbol{Q}_{24}$.

Here are examples of perfect sequences for each length:

Length 23: $\boldsymbol{a}_{23} = [\, 1, \boldsymbol{j}, -\boldsymbol{i}, -\boldsymbol{i}, \boldsymbol{i}, -\boldsymbol{k}, \boldsymbol{j}, -1, \boldsymbol{i}, \boldsymbol{k}, 1, 1, \boldsymbol{k}, \boldsymbol{i}, -1, \boldsymbol{j}, -\boldsymbol{k}, \boldsymbol{i}, -\boldsymbol{i}, -\boldsymbol{i}, \boldsymbol{j}, 1, \frac{-1-\boldsymbol{i}+\boldsymbol{j}-\boldsymbol{k}}{2}\,]$

Length 19: $\boldsymbol{a}_{19} = [\, 1, \boldsymbol{j}, -\boldsymbol{i}, -\boldsymbol{i}, \boldsymbol{i}, -1, -\boldsymbol{k}, -1, 1, 1, -1, -\boldsymbol{k}, -1, \boldsymbol{i}, -\boldsymbol{i}, -\boldsymbol{i}, \boldsymbol{j}, 1, \frac{1-\boldsymbol{i}+\boldsymbol{j}-\boldsymbol{k}}{2}\,]$

Length 17: $\boldsymbol{a}_{17} = [\,1, \boldsymbol{j}, -\boldsymbol{i}, \boldsymbol{j}, -\boldsymbol{k}, -\boldsymbol{j}, -1, 1, 1, -1, -\boldsymbol{j}, -\boldsymbol{k}, \boldsymbol{j}, -\boldsymbol{i}, \boldsymbol{j}, 1, \frac{1+\boldsymbol{i}+\boldsymbol{j}+\boldsymbol{k}}{2}\,]$

Length 13: $\boldsymbol{a}_{13} = [\,1, \boldsymbol{j}, -\boldsymbol{i}, -\boldsymbol{j}, 1, \boldsymbol{i}, \boldsymbol{i}, 1, -\boldsymbol{j}, -\boldsymbol{i}, \boldsymbol{j}, 1, \frac{-1-\boldsymbol{i}+\boldsymbol{j}-\boldsymbol{k}}{2}\,]$

Length 11: $\boldsymbol{a}_{11} = [\,1, \boldsymbol{j}, -\boldsymbol{i}, -\boldsymbol{j}, -\boldsymbol{k}, -\boldsymbol{k}, -\boldsymbol{j}, -\boldsymbol{i}, \boldsymbol{j}, 1, \frac{-1+\boldsymbol{i}+\boldsymbol{j}-\boldsymbol{k}}{2}\,]$

Length 9: $\boldsymbol{a}_{9} = [\,1, \boldsymbol{j}, -\boldsymbol{i}, -\boldsymbol{j}, -\boldsymbol{j}, -\boldsymbol{i}, \boldsymbol{j}, 1, \frac{-1-\boldsymbol{i}+\boldsymbol{j}-\boldsymbol{k}}{2}\,]$

Length 7: $\boldsymbol{a}_{7} = [\,1, \boldsymbol{j}, -\boldsymbol{i}, -\boldsymbol{i}, \boldsymbol{j}, 1, \frac{-1+\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}\,]$

Length 5: $\boldsymbol{a}_{5} = [\,1, \boldsymbol{j}, \boldsymbol{j}, 1, \frac{-1+\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}\,]$

We can append this list with one more perfect sequence,

$$\boldsymbol{a}_{16} = [\,1, 1, 1, 1, 1, \boldsymbol{i}, -1, -\boldsymbol{i}, 1, -1, 1, -1, 1, -\boldsymbol{i}, -1, \boldsymbol{i}\,]$$

which is the well-known Frank sequence over the 4-roots of unity of length 16 (refer to Section 4.3.2.1 of the present work). We regard entries of this sequence as quaternions and elements of the group $\boldsymbol{Q}_{24}$. Length 16 is a relatively prime number to lengths of all sequences from the list above.

The composition of all the above sequences,

$$\boldsymbol{a}_5 * \boldsymbol{a}_7 * \dots * \boldsymbol{a}_{23} = [\,1,1, \boldsymbol{k}, -\boldsymbol{i}, \frac{-1+\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}, \dots, \frac{1+\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}\,]$$

is perfect of length $5 \cdot 7 \cdot 9 \cdot 11 \cdot 13 \cdot 16 \cdot 17 \cdot 19 \cdot 23 = \mathbf{5,354,228,880}$.

Note that elements of the group $\boldsymbol{Q}_{24}$ can be regarded as quaternionic 12-roots of unity. Indeed, $x^{12} = 1$, for all $x \in \boldsymbol{Q}_{24}$. So, the sequence of length 5,354,228,880, obtained in Example 7.3, is in fact over the quaternionic 12-roots of unity.

7.2. Composition of Two Sequences of Even Lengths

The result of this part, Proposition 7.2, is a new result on composition of two sequences of even lengths. We give several applications of this result to perfect sequences over the real quaternions, where new perfect sequences are obtained. However, we have not found new perfect sequences over complex roots of unity by using Proposition 7.2, because we were unable to find any sequences satisfying properties 3 – 5 of Proposition 7.2 over complex roots of unity by an exhaustive search on our ordinary desktop computer.

Definition 7.3 The *(right) cross correlation function* between non-zero sequences $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$ and $\boldsymbol{y} = [\boldsymbol{y}_0, \boldsymbol{y}_1, \dots, \boldsymbol{y}_{n-1}]$ is defined as

$$CCF^R_{\boldsymbol{xy}}(m) = \frac{1}{\sqrt{\|\boldsymbol{x}\|\|\boldsymbol{y}\|}} \sum_{t=0}^{n-1} \boldsymbol{x}_t \boldsymbol{y}^*_{t+m}$$

for $0 \le m \le n-1$.

Proposition 7.2 Let $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n_1-1}]$, $\boldsymbol{b} = [\boldsymbol{b}_0, \boldsymbol{b}_1, \dots, \boldsymbol{b}_{n_2-1}]$ be two sequences of even lengths n_1 and n_2 over unit quaternions, so that the following conditions are satisfied:

1. n_2 is not a multiple or a divisor of n_1,
2. Sequence $\boldsymbol{a}$ is perfect,
3. The subsequences $Dec_2^0(\boldsymbol{b})$ and $Dec_2^1(\boldsymbol{b})$ of $\boldsymbol{b}$ are both perfect,
4. $CCF^R_{Dec_2^0(\boldsymbol{b}),Dec_2^1(\boldsymbol{b})}(m-1) = CCF^R_{Dec_2^1(\boldsymbol{b}),Dec_2^0(\boldsymbol{b})}(m)$ for every m, $1 \le m \le \left\lceil \frac{n_2}{4} \right\rceil$,
5. $CCF^R_{Dec_2^1(\boldsymbol{b}),Dec_2^0(\boldsymbol{b})}(m)$ are real numbers for every m, $1 \le m \le \left\lfloor \frac{n_2}{4} \right\rfloor$.

Then the composition sequence $\boldsymbol{a} * \boldsymbol{b} = [\boldsymbol{a}_t \boldsymbol{b}_t]$, $t = 0, \dots, \mathrm{lcm}(n_1, n_2) - 1$, is perfect.

Some Lemmas will be required for the proof of Proposition 7.2.

Lemma 7.1 Let $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$ and $\boldsymbol{y} = [\boldsymbol{y}_0, \boldsymbol{y}_1, \dots, \boldsymbol{y}_{n-1}]$ be sequences of length n over the real quaternions. Then, for $1 \leq m \leq n$, the following identity is true:

$$\left(CCF_{\boldsymbol{xy}}^{R}(m)\right)^{*} = CCF_{\boldsymbol{yx}}^{R}(n-m)$$

Proof.

$\left(CCF_{\boldsymbol{xy}}^{R}(m)\right)^{*} = \left(\frac{1}{\sqrt{\|\boldsymbol{x}\|\|\boldsymbol{y}\|}} \sum_{t=0}^{n-1} \boldsymbol{x}_t \boldsymbol{y}_{t+m}^{*}\right)^{*} = \frac{1}{\sqrt{\|\boldsymbol{x}\|\|\boldsymbol{y}\|}} \sum_{t=0}^{n-1} \boldsymbol{y}_{t+m} \boldsymbol{x}_t^{*} = \frac{1}{\sqrt{\|\boldsymbol{x}\|\|\boldsymbol{y}\|}} \sum_{s=0}^{n-1} \boldsymbol{y}_s \boldsymbol{x}_{s-m}^{*} =$ $CCF_{\boldsymbol{yx}}^{R}(n-m)$. □

Lemma 7.2 Let $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$ and $\boldsymbol{y} = [\boldsymbol{y}_0, \boldsymbol{y}_1, \dots, \boldsymbol{y}_{n-1}]$ be sequences of length n over the real quaternions. If the condition $CCF_{\boldsymbol{xy}}^{R}(m-1) = CCF_{\boldsymbol{yx}}^{R}(m)$ holds for every m in the range $1 \leq m \leq \left\lceil \frac{n}{2} \right\rceil$, then it holds for every integer m.

Proof. By taking conjugates of both parts of the equality $CCF_{\boldsymbol{xy}}^{R}(m-1) = CCF_{\boldsymbol{yx}}^{R}(m)$, we have $CCF_{\boldsymbol{yx}}^{R}(n-m+1) = CCF_{\boldsymbol{xy}}^{R}(n-m)$, by Lemma 7.1. Since, by assumption, this is true for every m in the interval $1 \leq m \leq \left\lceil \frac{n}{2} \right\rceil$, it follows that, after substitution $t = n - m + 1$, we have $CCF_{\boldsymbol{xy}}^{R}(t-1) = CCF_{\boldsymbol{yx}}^{R}(t)$ for $\left\lfloor \frac{n}{2} \right\rfloor + 1 \leq t \leq n$. Therefore, $CCF_{\boldsymbol{xy}}^{R}(m-1) = CCF_{\boldsymbol{yx}}^{R}(m)$ for every m in

$$\left\{m: 1 \leq m \leq \left\lceil \frac{n}{2} \right\rceil\right\} \cup \left\{m: \left\lfloor \frac{n}{2} \right\rfloor + 1 \leq m \leq n\right\} = \{m: 1 \leq m \leq n\},$$

and, since arithmetic $modulo\ n$ applies for m, for any integer m. □

Lemma 7.3 Let $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$ and $\boldsymbol{y} = [\boldsymbol{y}_0, \boldsymbol{y}_1, \dots, \boldsymbol{y}_{n-1}]$ be sequences of length n over the real quaternions, so that the condition of Lemma 7.2 holds: $CCF_{\boldsymbol{xy}}^{R}(m-1) = CCF_{\boldsymbol{yx}}^{R}(m)$ for

$1 \leq m \leq \left\lceil \frac{n}{2} \right\rceil$. If $CCF_{\boldsymbol{yx}}^{R}(m)$ are real numbers for $1 \leq m \leq \left\lfloor \frac{n}{2} \right\rfloor$, then $CCF_{\boldsymbol{yx}}^{R}(m)$ are real numbers for every integer m.

<u>Proof.</u> Note that, by Lemma 7.2, the assumed condition $CCF_{\boldsymbol{xy}}^{R}(m-1) = CCF_{\boldsymbol{yx}}^{R}(m)$ holds for all integers m. Since $CCF_{\boldsymbol{yx}}^{R}(m)$ are real numbers for $1 \leq m \leq \left\lfloor \frac{n}{2} \right\rfloor$, implying they are equal to their conjugates, then, making use of Lemma 7.1 and the assumed condition $CCF_{\boldsymbol{xy}}^{R}(m-1) = CCF_{\boldsymbol{yx}}^{R}(m)$, we have

$$CCF_{\boldsymbol{yx}}^{R}(m) = CCF_{\boldsymbol{xy}}^{R}(m-1) = \left(CCF_{\boldsymbol{yx}}^{R}(n-m+1)\right)^{*} = CCF_{\boldsymbol{yx}}^{R}(n-m+1).$$

Therefore, $CCF_{\boldsymbol{yx}}^{R}(n-m+1)$ are also real for $1 \leq m \leq \left\lfloor \frac{n}{2} \right\rfloor$, or, after the substitution $t = n - m + 1$, $CCF_{\boldsymbol{yx}}^{R}(t)$ are real for $\left\lceil \frac{n}{2} \right\rceil + 1 \leq t \leq n$. Thus, $CCF_{\boldsymbol{yx}}^{R}(m)$ are real for every m in

$$\left\{m\colon 1 \leq m \leq \left\lfloor \frac{n}{2} \right\rfloor\right\} \cup \left\{m\colon \left\lceil \frac{n}{2} \right\rceil + 1 \leq m \leq n\right\}.$$

If n is an even number, then $\left\lfloor \frac{n}{2} \right\rfloor = \left\lceil \frac{n}{2} \right\rceil$ and

$$\left\{m\colon 1 \leq m \leq \left\lfloor \frac{n}{2} \right\rfloor\right\} \cup \left\{m\colon \left\lceil \frac{n}{2} \right\rceil + 1 \leq m \leq n\right\} = \{m\colon 1 \leq m \leq n\}.$$

If n is an odd number, then

$$CCF_{\boldsymbol{yx}}^{R}\left(\left\lceil \frac{n}{2} \right\rceil\right) = CCF_{\boldsymbol{xy}}^{R}\left(\left\lceil \frac{n}{2} \right\rceil - 1\right) = \left(CCF_{\boldsymbol{yx}}^{R}\left(n - \left\lceil \frac{n}{2} \right\rceil + 1\right)\right)^{*} = \left(CCF_{\boldsymbol{yx}}^{R}\left(\left\lceil \frac{n}{2} \right\rceil\right)\right)^{*}.$$

Therefore, for an odd n, $CCF_{\boldsymbol{yx}}^{R}\left(\left\lceil \frac{n}{2} \right\rceil\right)$ is always a real number. Then, $CCF_{\boldsymbol{yx}}^{R}(m)$ are real for every m in

$$\left\{m\colon 1 \leq m \leq \left\lfloor \frac{n}{2} \right\rfloor\right\} \cup \left\{m\colon \left\lceil \frac{n}{2} \right\rceil + 1 \leq m \leq n\right\} \cup \left\{\left\lceil \frac{n}{2} \right\rceil\right\} = \{m\colon 1 \leq m \leq n\}.$$

Thus, $CCF_{\boldsymbol{yx}}^{R}(m)$ is real for every m in $1 \leq m \leq n$, irrespective of the parity of n. The arithmetic *modulo* n applies to m, therefore, $CCF_{\boldsymbol{yx}}^{R}(m)$ is a real number for every integer m. □

We are now ready to proceed with a proof of Proposition 7.2.

Proof of Proposition 7.2 Let $\boldsymbol{x} = Dec_2^0(\boldsymbol{b})$, $\boldsymbol{y} = Dec_2^1(\boldsymbol{b})$ and $n = \frac{n_2}{2}$.

Note that, by Lemmas 7.2 and 7.3, conditions 4 and 5 of Proposition 7.2 are, in fact, equivalent to the conditions

4′. $CCF^R_{Dec_2^0(\boldsymbol{b}),Dec_2^1(\boldsymbol{b})}(m-1) = CCF^R_{Dec_2^1(\boldsymbol{b}),Dec_2^0(\boldsymbol{b})}(m)$ for all integer m,

and

5′. $CCF^R_{Dec_2^0(\boldsymbol{b}),Dec_2^1(\boldsymbol{b})}(m)$ is a real number for all integers m.

We now consider the (right) autocorrelation value of the composition of two sequences $\boldsymbol{a}$ and $\boldsymbol{b}$ for an arbitrary shift m, $1 \le m \le \operatorname{lcm}(n_1, n_2) - 1$ and show that, with the assumptions of Proposition 7.2, it is equal to zero.

Consider two cases: the first, $m \neq 0 \; mod \; n_2$, and the second, $m = 0 \; mod \; n_2$.

Case 1. $m \neq 0 \; mod \; n_2$.

$$ACF^R_{\boldsymbol{a}*\boldsymbol{b}}(m) = \frac{1}{\|\boldsymbol{a}*\boldsymbol{b}\|} \sum_{t=0}^{\operatorname{lcm}(n_1,n_2)-1} \boldsymbol{a}_t \boldsymbol{b}_t (\boldsymbol{a}_{t+m} \boldsymbol{b}_{t+m})^* = \frac{1}{\|\boldsymbol{a}*\boldsymbol{b}\|} \sum_{t=0}^{\operatorname{lcm}(n_1,n_2)-1} \boldsymbol{a}_t \boldsymbol{b}_t \boldsymbol{b}^*_{t+m} \boldsymbol{a}^*_{t+m} \tag{7.1}$$

Since indices of $\boldsymbol{a}$ are taken $modulo \; n_1$, in the summation above, every $\boldsymbol{a}_t$ and $\boldsymbol{a}^*_{t+m}$ will repeat itself $\frac{\operatorname{lcm}(n_1,n_2)}{n_1}$ times in every n_1-th term, and, since indices of $\boldsymbol{b}$ are taken $modulo \; n_2$, every time they will meet $\boldsymbol{b}_t$ and $\boldsymbol{b}^*_{t+m}$ which are exactly $(n_1 - n_2) \; mod \; n_2$ elements apart from the $\boldsymbol{b}_t$ and $\boldsymbol{b}^*_{t+m}$, so the summation above is partitioned as follows:

$$= \frac{1}{\|\boldsymbol{a} * \boldsymbol{b}\|} \sum_{t_1=0}^{n_1-1} \boldsymbol{a}_{t_1} \left(\sum_{s=0}^{\frac{\mathrm{lcm}(n_1,n_2)}{n_1}-1} \boldsymbol{b}_{t_1+(n_1-n_2)s} \boldsymbol{b}^*_{t_1+(n_1-n_2)s+m} \right) \boldsymbol{a}^*_{t_1+m}$$

Since n_1 and n_2 are even numbers, $n_1 - n_2$ is an even number too. Moreover, because n_1 and n_2 are not multiples of each other, $\frac{\mathrm{lcm}(n_1,n_2)}{n_1} = \frac{n_2}{2}$. Since indices of all summands in the brackets above are assumed *modulo* n_2, the sum in the brackets can be expanded as follows:

$$\sum_{s=0}^{\frac{\mathrm{lcm}(n_1,n_2)}{n_1}-1} \boldsymbol{b}_{t_1+(n_1-n_2)s} \boldsymbol{b}^*_{t_1+(n_1-n_2)s+m} = \sum_{s=0}^{\frac{n_2}{2}-1} \boldsymbol{b}_{t_1+(n_1-n_2)s} \boldsymbol{b}^*_{t_1+(n_1-n_2)s+m}$$

$$= \begin{cases} \|Dec_2^0(\boldsymbol{b})\| \cdot ACF^R_{Dec_2^0(\boldsymbol{b}),Dec_2^0(\boldsymbol{b})}\left(\frac{m}{2}\right), & \text{if both } m \text{ and } t_1 \text{ are even} \\ \|Dec_2^1(\boldsymbol{b})\| \cdot ACF^R_{Dec_2^1(\boldsymbol{b}),Dec_2^1(\boldsymbol{b})}\left(\frac{m}{2}\right), & \text{if } m \text{ is even and } t_1 \text{ is odd} \\ \sqrt{\|Dec_2^0(\boldsymbol{b})\|\|Dec_2^1(\boldsymbol{b})\|} \cdot CCF^R_{Dec_2^0(\boldsymbol{b}),Dec_2^1(\boldsymbol{b})}(m-1), & \text{if } m \text{ is odd and } t_1 \text{ is even} \\ \sqrt{\|Dec_2^0(\boldsymbol{b})\|\|Dec_2^1(\boldsymbol{b})\|} \cdot CCF^R_{Dec_2^1(\boldsymbol{b}),Dec_2^0(\boldsymbol{b})}(m), & \text{if both } m \text{ and } t_1 \text{ are odd} \end{cases}$$

Note that since sequences $\boldsymbol{a}$ and $\boldsymbol{b}$ are assumed over unit quaternions, that is, all their elements have norm 1, and both $Dec_2^0(\boldsymbol{b})$ and $Dec_2^1(\boldsymbol{b})$ are of the same length $\frac{n_2}{2}$, then $\|Dec_2^0(\boldsymbol{b})\| = \|Dec_2^1(\boldsymbol{b})\| = \frac{n_2}{2}$ and $\sqrt{\|Dec_2^0(\boldsymbol{b})\|\|Dec_2^1(\boldsymbol{b})\|} = \frac{n_2}{2}$.

$$= \begin{cases} \frac{n_2}{2} \cdot ACF^R_{Dec_2^0(\boldsymbol{b}),Dec_2^0(\boldsymbol{b})}\left(\frac{m}{2}\right), & \text{if both } m \text{ and } t_1 \text{ are even} \\ \frac{n_2}{2} \cdot ACF^R_{Dec_2^1(\boldsymbol{b}),Dec_2^1(\boldsymbol{b})}\left(\frac{m}{2}\right), & \text{if } m \text{ is even and } t_1 \text{ is odd} \\ \frac{n_2}{2} \cdot CCF^R_{Dec_2^0(\boldsymbol{b}),Dec_2^1(\boldsymbol{b})}(m-1), & \text{if } m \text{ is odd and } t_1 \text{ is even} \\ \frac{n_2}{2} \cdot CCF^R_{Dec_2^1(\boldsymbol{b}),Dec_2^0(\boldsymbol{b})}(m), & \text{if both } m \text{ and } t_1 \text{ are odd} \end{cases}$$

Equality (7.1) continues:

$$= \frac{1}{\|\boldsymbol{a} * \boldsymbol{b}\|} \sum_{t_1=0}^{n_1-1} \boldsymbol{a}_{t_1} \left(\sum_{s=0}^{\frac{n_2}{2}-1} \boldsymbol{b}_{t_1+(n_1-n_2)s} \boldsymbol{b}^*_{t_1+(n_1-n_2)s+m} \right) \boldsymbol{a}^*_{t_1+m}$$

$$= \frac{1}{\|\boldsymbol{a} * \boldsymbol{b}\|} \left(\sum_{\substack{t_1=0 \\ even\, t_1}}^{n_1-2} \boldsymbol{a}_{t_1} \left(\boldsymbol{b}_{t_1+(n_1-n_2)s} \boldsymbol{b}^*_{t_1+(n_1-n_2)s+m} \right) \boldsymbol{a}^*_{t_1+m} + \sum_{\substack{t_1=1 \\ odd\, t_1}}^{n_1-1} \boldsymbol{a}_{t_1} \left(\boldsymbol{b}_{t_1+(n_1-n_2)s} \boldsymbol{b}^*_{t_1+(n_1-n_2)s+m} \right) \boldsymbol{a}^*_{t_1+m} \right)$$

$$= \begin{cases} \frac{n_2}{2\|\boldsymbol{a} * \boldsymbol{b}\|} \left(\sum_{\substack{t_1=0 \\ even\, t_1}}^{n_1-2} \boldsymbol{a}_{t_1} \left(ACF^R_{Dec_2^0(\boldsymbol{b}),Dec_2^0(\boldsymbol{b})} \left(\frac{m}{2} \right) \right) \boldsymbol{a}^*_{t_1+m} + \sum_{\substack{t_1=1 \\ odd\, t_1}}^{n_1-1} \boldsymbol{a}_{t_1} \left(ACF^R_{Dec_2^1(\boldsymbol{b}),Dec_2^1(\boldsymbol{b})} \left(\frac{m}{2} \right) \right) \boldsymbol{a}^*_{t_1+m} \right), \text{even } m \\ \frac{n_2}{2\|\boldsymbol{a} * \boldsymbol{b}\|} \left(\sum_{\substack{t_1=0 \\ even\, t_1}}^{n_1-2} \boldsymbol{a}_{t_1} \left(CCF^R_{Dec_2^0(\boldsymbol{b}),Dec_2^1(\boldsymbol{b})} (m-1) \right) \boldsymbol{a}^*_{t_1+m} + \sum_{\substack{t_1=1 \\ odd\, t_1}}^{n_1-1} \boldsymbol{a}_{t_1} \left(CCF^R_{Dec_2^1(\boldsymbol{b}),Dec_2^0(\boldsymbol{b})} (m) \right) \boldsymbol{a}^*_{t_1+m} \right), \text{odd } m \end{cases}$$

$$(7.2)$$

Since $m \neq 0\, mod\, n_2$ by the assumption of this case, $\frac{m}{2} \neq 0\, mod\, \frac{n_2}{2}$. Because $Dec_2^0(\boldsymbol{b})$ and $Dec_2^1(\boldsymbol{b})$ are both perfect of length $\frac{n_2}{2}$, then $ACF^R_{Dec_2^0(\boldsymbol{b}),Dec_2^0(\boldsymbol{b})} \left(\frac{m}{2} \right) = 0$ and $ACF^R_{Dec_2^1(\boldsymbol{b}),Dec_2^1(\boldsymbol{b})} \left(\frac{m}{2} \right) = 0$.

Let $r = CCF^R_{Dec_2^0(\boldsymbol{b}),Dec_2^1(\boldsymbol{b})}(m-1)$. By conditions $4'$ and $5'$, r is a real number, and $r = CCF^R_{Dec_2^1(\boldsymbol{b}),Dec_2^0(\boldsymbol{b})}(m)$. Then, equality (7.2) continues

$$= \begin{cases} \frac{n_2}{2\|\boldsymbol{a} * \boldsymbol{b}\|} \left(\sum_{\substack{t_1=0 \\ even\, t_1}}^{n_1-2} \boldsymbol{a}_{t_1} \cdot 0 \cdot \boldsymbol{a}^*_{t_1+m} + \sum_{\substack{t_1=1 \\ odd\, t_1}}^{n_1-1} \boldsymbol{a}_{t_1} \cdot 0 \cdot \boldsymbol{a}^*_{t_1+m} \right), \text{even } m \\ \frac{n_2}{2\|\boldsymbol{a} * \boldsymbol{b}\|} \left(\sum_{\substack{t_1=0 \\ even\, t_1}}^{n_1-2} \boldsymbol{a}_{\boldsymbol{t_1}} \cdot r \cdot \boldsymbol{a}^*_{t_1+m} + \sum_{\substack{t_1=1 \\ odd\, t_1}}^{n_1-1} \boldsymbol{a}_{t_1} \cdot r \cdot \boldsymbol{a}^*_{t_1+m} \right), \text{odd } m \end{cases}$$

$$= \begin{cases} \frac{n_2 \cdot 0}{2\|\boldsymbol{a} * \boldsymbol{b}\|} \sum_{t_1=0}^{n_1-1} \boldsymbol{a}_{t_1} \boldsymbol{a}^*_{t_1+m}, \text{even } m \\ \frac{n_2 \cdot r}{2\|\boldsymbol{a} * \boldsymbol{b}\|} \sum_{t_1=0}^{n_1-1} \boldsymbol{a}_{t_1} \boldsymbol{a}^*_{t_1+m}, \text{odd } m \end{cases} = \begin{cases} \frac{n_2 \cdot 0}{2\|\boldsymbol{a} * \boldsymbol{b}\|} \|\boldsymbol{a}\| AC^R_{\boldsymbol{a}}(m), \text{even } m \\ \frac{n_2 \cdot r}{2\|\boldsymbol{a} * \boldsymbol{b}\|} \|\boldsymbol{a}\| ACF^R_{\boldsymbol{a}}(m), \text{odd } m \end{cases}$$

Note that $\frac{n_2 \cdot 0}{2\|\boldsymbol{a}*\boldsymbol{b}\|}\|\boldsymbol{a}\| ACF_{\boldsymbol{a}}^{R}(m)$ is always equal to zero irrespective of m, due to 0 in the numerator; $ACF_{\boldsymbol{a}}^{R}(m)$ is equal to zero for every $m \neq 0 \; mod \; n_1$, and therefore, since n_1 is an even number by assumption, for every odd m.

$$= \begin{cases} \dfrac{n_2 \cdot 0}{2\|\boldsymbol{a}*\boldsymbol{b}\|} \cdot 0, \text{even } m \\ \dfrac{n_2 \cdot r}{2\|\boldsymbol{a}*\boldsymbol{b}\|} \cdot 0, \text{odd } m \end{cases} = 0$$

Case 2. $m = 0 \; mod \; n_2$. We have

$$ACF_{\boldsymbol{a}*\boldsymbol{b}}^{R}(m) = \frac{1}{\|\boldsymbol{a}*\boldsymbol{b}\|} \sum_{t=0}^{\mathrm{lcm}(n_1,n_2)-1} \boldsymbol{a}_t \boldsymbol{b}_t (\boldsymbol{a}_{t+m}\boldsymbol{b}_{t+m})^* = \frac{1}{\|\boldsymbol{a}*\boldsymbol{b}\|} \sum_{t=0}^{\mathrm{lcm}(n_1,n_2)-1} \boldsymbol{a}_t \boldsymbol{b}_t \boldsymbol{b}_{t+m}^* \boldsymbol{a}_{t+m}^*$$

$$= \frac{1}{\|\boldsymbol{a}*\boldsymbol{b}\|} \sum_{t_1=0}^{n_1-1} \boldsymbol{a}_{t_1} \left(\sum_{s=0}^{\frac{\mathrm{lcm}(n_1,n_2)}{n_1}-1} \boldsymbol{b}_{t_1+(n_1-n_2)s} \boldsymbol{b}_{t_1+(n_1-n_2)s+m}^* \right) \boldsymbol{a}_{t_1+m}^*$$

$$= \frac{1}{\|\boldsymbol{a}*\boldsymbol{b}\|} \sum_{t_1=0}^{n_1-1} \boldsymbol{a}_{t_1} \left(\sum_{s=0}^{\frac{n_2}{2}-1} \boldsymbol{b}_{t_1+(n_1-n_2)s} \boldsymbol{b}_{t_1+(n_1-n_2)s+m}^* \right) \boldsymbol{a}_{t_1+m}^*$$

Summation in indices of $\boldsymbol{b}$ is taken $modulo \; n_2$, therefore $\boldsymbol{b}_{t_1+(n_1-n_2)s+m}^* = \boldsymbol{b}_{t_1+(n_1-n_2)s}^*$. So the equality continues

$$= \frac{1}{\|\boldsymbol{a}*\boldsymbol{b}\|} \sum_{t_1=0}^{n_1-1} \boldsymbol{a}_{t_1} \left(\sum_{s=0}^{\frac{n_2}{2}-1} \boldsymbol{b}_{t_1+(n_1-n_2)s} \boldsymbol{b}_{t_1+(n_1-n_2)s}^* \right) \boldsymbol{a}_{t_1+m}^*$$

$$= \frac{1}{\|\boldsymbol{a}*\boldsymbol{b}\|} \sum_{t_1=0}^{n_1-1} \boldsymbol{a}_{t_1} \left(\sum_{s=0}^{\frac{n_2}{2}-1} \left\|\boldsymbol{b}_{t_1+(n_1-n_2)s}\right\| \right) \boldsymbol{a}_{t_1+m}^*$$

Sequence $\boldsymbol{b}$ is over unit quaternions by assumption, meaning all its elements have norm 1.

$$= \frac{1}{\|\boldsymbol{a} * \boldsymbol{b}\|} \sum_{t_1=0}^{n_1-1} \boldsymbol{a}_{t_1} \left(\sum_{s=0}^{\frac{n_2}{2}-1} 1 \right) \boldsymbol{a}^*_{t_1+m} = \frac{1}{\|\boldsymbol{a} * \boldsymbol{b}\|} \sum_{t_1=0}^{n_1-1} \boldsymbol{a}_{t_1} \frac{n_2}{2} \boldsymbol{a}^*_{t_1+m} = \frac{n_2}{2\|\boldsymbol{a} * \boldsymbol{b}\|} \|\boldsymbol{a}\| ACF^R_{\boldsymbol{a}}(m)$$

$$= 0$$

The autocorrelation function $ACF^R_{\boldsymbol{a}}(m)$ has a non-zero value only for $m = 0 \, mod \, n_1$. Because n_1 and n_2 are assumed not to be multiples of each other, it is impossible to have $m = 0 \, mod \, n_1$ and $m = 0 \, mod \, n_2$ at the same time in the interval $1 \le m \le \mathrm{lcm}(n_1, n_2) - 1$. Since, in this case we assumed $m = 0 \, mod \, n_2$, then, $m \ne 0 \, mod \, n_1$, and $ACF^R_{\boldsymbol{a}}(m) = 0$.

Thus, in both above cases $ACF^R_{\boldsymbol{a*b}}(m) = 0$. This means that $ACF^R_{\boldsymbol{a*b}}(m) = 0$ for all m, $1 \le m \le \mathrm{lcm}(n_1, n_2) - 1$, and the composition sequence $\boldsymbol{a} * \boldsymbol{b}$ is perfect. □

<u>Example 7.4</u> By an exhaustive search for sequences of length 6 over $\boldsymbol{Q}_{24}$, using the computational software package Magma, developed by the University of Sydney [12], some examples of sequences satisfying conditions 3 – 5 of Proposition 7.2 have been found. One example of such sequence is

$$\boldsymbol{b} = [\, 1 \,, \frac{-1 - \boldsymbol{i} - \boldsymbol{j} - \boldsymbol{k}}{2} \,, 1 \,, 1, \frac{-1 - \boldsymbol{i} - \boldsymbol{j} - \boldsymbol{k}}{2} \,, 1 \,]$$

Indeed, it is not difficult to check that

$$Dec^0_2(\boldsymbol{b}) \; = [\, 1 \,, 1 \,, \frac{-1 - \boldsymbol{i} - \boldsymbol{j} - \boldsymbol{k}}{2}]$$

and

$$Dec^1_2(\boldsymbol{b}) \; = [\; \frac{-1 - \boldsymbol{i} - \boldsymbol{j} - \boldsymbol{k}}{2} \,, 1 \,, 1 \,]$$

are both perfect. Therefore, condition 3 is satisfied.

For a sequence $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_5]$ of length 6, condition 4 means that

$m = 1$: $\boldsymbol{x}_0\boldsymbol{x}^*_1 + \boldsymbol{x}_2\boldsymbol{x}^*_3 + \boldsymbol{x}_4\boldsymbol{x}^*_5 = \boldsymbol{x}_1\boldsymbol{x}^*_2 + \boldsymbol{x}_3\boldsymbol{x}^*_4 + \boldsymbol{x}_5\boldsymbol{x}^*_0$,

$m = 2$: $\boldsymbol{x}_0\boldsymbol{x}^*_3 + \boldsymbol{x}_2\boldsymbol{x}^*_5 + \boldsymbol{x}_4\boldsymbol{x}^*_1 = \boldsymbol{x}_1\boldsymbol{x}^*_4 + \boldsymbol{x}_3\boldsymbol{x}^*_0 + \boldsymbol{x}_5\boldsymbol{x}^*_2$.

Condition 5 implies that all these sums are real numbers.

Direct calculation shows that conditions 4 – 5 are met for sequence $\boldsymbol{b}$:

$m = 1$:

$$\boldsymbol{b}_0 b_1^* + \boldsymbol{b}_2\boldsymbol{b}_3^* + \boldsymbol{b}_4\boldsymbol{b}_5^* = 1\cdot\left(\frac{-1-\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}\right)^* + 1\cdot(1)^* + \frac{-1-\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}\cdot(1)^* = \frac{-1+\boldsymbol{i}+\boldsymbol{j}+\boldsymbol{k}}{2} + 1 + \frac{-1-\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2} = 0$$

$$\boldsymbol{b}_1\boldsymbol{b}_2^* + \boldsymbol{b}_3\boldsymbol{b}_4^* + \boldsymbol{b}_5\boldsymbol{b}_0^* = \frac{-1-\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}\cdot(1)^* + 1\cdot\left(\frac{-1-\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}\right)^* + 1\cdot(1)^* = \frac{-1-\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2} + \frac{-1+\boldsymbol{i}+\boldsymbol{j}+\boldsymbol{k}}{2} + 1 = 0$$

$m = 2$:

$$\boldsymbol{b}_0\boldsymbol{b}_3^* + \boldsymbol{b}_2\boldsymbol{b}_5^* + \boldsymbol{b}_4\boldsymbol{b}_1^* = 1\cdot(1)^* + 1\cdot(1)^* + \frac{-1-\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}\cdot\left(\frac{-1-\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}\right)^* = 1+1+1 = 3$$

$$\boldsymbol{b}_1\boldsymbol{b}_4^* + \boldsymbol{b}_3\boldsymbol{b}_0^* + \boldsymbol{b}_5\boldsymbol{b}_2^* = \frac{-1-\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}\cdot\left(\frac{-1-\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}\right)^* + 1\cdot(1)^* + 1\cdot(1)^* = 1+1+1 = 3$$

Thus, sequence $\boldsymbol{b}$ satisfies conditions 3 – 5, and according to Proposition 7.2, the composition of any perfect sequence, whose length is not a multiple or a divisor of 6, with the sequence $\boldsymbol{b}$ will be a perfect sequence.

For example, consider the composition of the well known Frank perfect sequence of length 4 (refer to Section 4.3.2.1 of the Present work), $\boldsymbol{a} = [\,1, 1, 1, -1\,]$, with the sequence $\boldsymbol{b}$:

$$\boldsymbol{a} * \boldsymbol{b} = [\,1,1,1,-1\,] * \left[\,1\,, \frac{-1-\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}\,, 1\,, 1, \frac{-1-\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}\,, 1\,\right] =$$

$$[\,1, \frac{-1-\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}, 1, -1, \frac{-1-\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}, 1, 1, \frac{1+\boldsymbol{i}+\boldsymbol{j}+\boldsymbol{k}}{2}, 1, 1, \frac{-1-\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}, -1\,]$$

The resulting sequence of length 12 is perfect over $\boldsymbol{Q}_{24}$.

Finding sequences satisfying conditions 3 – 5 of Proposition 7.2 by an exhaustive search may be a very time consuming process, which often exceeds the computational power of an average desktop computer. As an alternative to the exhaustive search, one may try to construct a sequence with the required properties, making use of already known perfect sequences of shorter length as building blocks. A sketch of an algorithm which can be used for construction of compounded perfect sequences over the quaternions is presented below. In some cases, this algorithm allows finding sequences satisfying conditions 3 – 5 of Proposition 7.2 in a fraction of the time required for finding perfect sequences of the same length by the exhaustive search.

Before we proceed with the description of the algorithm, we define a new operation, interlacing, on two sequences of equal lengths.

<u>Definition 7.4</u> Let S_n^A and S_{2n}^A denote the sets of all sequences of lengths n and $2n$ over some alphabet A respectively. The *interlace* of two sequences $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$ and $\boldsymbol{y} = [\boldsymbol{y}_0, \boldsymbol{y}_1, \dots, \boldsymbol{y}_{n-1}]$ from S_n^A, denoted by $\mathrm{int}(\boldsymbol{x}, \boldsymbol{y})$, is defined as the operation $S_n^A \times S_n^A \to S_{2n}^A$ such that, for $0 \le t \le 2n-1$, $[\mathrm{int}(\boldsymbol{x}, \boldsymbol{y})]_t = \begin{cases} \boldsymbol{x}_{\frac{t}{2}}, \text{if } t \text{ is even} \\ \boldsymbol{y}_{\frac{t-1}{2}}, \text{if } t \text{ is odd} \end{cases}$, where $[\cdot]_t$ denotes the t-th element of the sequence in brackets, and operations in indices of $\boldsymbol{x}$ and $\boldsymbol{y}$ are assumed *modulo* n.

In plain language, the interlace of a pair of sequences of equal length is constructed by the following rule: we take the first element of the first sequence in the pair and insert it as the first entry of the interlace sequence, then we take the first element of the second sequence in the pair and append it as the second entry of the interlace sequence, then take the second element of the first sequence in the pair and append it as the third entry of the interlace sequence, and so on, until all elements of both sequences in the pair have been appended to the interlace sequence. The length of the interlace sequence is double the length of the original sequences.

<u>Algorithm 7.1</u> (constructing a sequence over the real quaternions, satisfying conditions 3 – 5 of Proposition 7.2, by interlacing two perfect sequences)

Input: Integer n; A finite set of quaternions A (alphabet)

Output: A set of sequences of length $2n$ satisfying conditions 3 – 5 of Proposition 7.2

Step 1. By an exhaustive computer search[4] over S_n^A, construct the set P_n^A of all perfect sequences of length n over A:

- 1.1 Define an empty set P_n^A;
- 1.2 Generate the first sequence of length n with elements from the set A;
- 1.3 Check the sequence generated in the previous step for perfection: if it is perfect, append it to the set P_n^A;
- 1.4 While there exists a sequence of length n with elements from the set A still unchecked for perfection in the previous steps, generate this sequence and start over from step 1.3;

Step 2. For every pair of sequences from the set P_n^A, construct the interlace sequence and check it for conditions 4 – 5 of Proposition 7.2.

- 2.1 Define an empty set R_{2n}^A;
- 2.2 Pick up the first sequence from the set P_n^A, $\boldsymbol{x} \in P_n^A$;
- 2.3 Pick up the second sequence from the set P_n^A, $\boldsymbol{y} \in P_n^A$;
- 2.4 Compute the interlace $\mathrm{int}(\boldsymbol{x}, \boldsymbol{y})$ and check[5] if it satisfies conditions 4 – 5 of Proposition 7.2: if yes, append it to the set R_{2n}^A;
- 2.5 While there is a sequence in the set P_n^A, not yet taken in step 2.4, replace $\boldsymbol{y}$ with this sequence and go to step 2.4;

---

[4] In the absence of sufficient computer power, the search in this step can be restricted to sequences with special properties, e.g. palindromic. However, restricting the search would possibly decrease the total number of perfect sequences, found in this step (the size of the set P_n^A), which, in turn, reduces the probability of successful outcome (non-empty output) of Algorithm 7.1.

[5] If we have restricted the search in step1 by considering only sequences of a special form, the list of perfect sequences in the set P_n^A may not be exhaustive. In this case, in order to maximize chances of non-empty output of Algorithm 7.1, we recommend also trying to check $\mathrm{int}(\boldsymbol{x}, \boldsymbol{y})$ obtained after the substitution of sequences $\boldsymbol{x}$ and $\boldsymbol{y}$ by perfect sequences derived by performing all shifts, proper decimations and, in the case when alphabet A is a finite quaternion group, multiplication of all elements of the original sequence by elements of the same group, of sequences $\boldsymbol{x}$ and $\boldsymbol{y}$ respectively.

2.6 While there is a sequence in the set P_n^A, not yet taken in step 2.3, replace $\boldsymbol{x}$ with this sequence and go to step 2.3;

2.7 Stop.

For many particular combinations of an integer n and an alphabet A, the output of Algorithm 7.1 will be the empty set, meaning that there exist no sequences of length $2n$ over A, satisfying conditions 3 – 5 of Proposition 7.2

When Algorithm 7.1 retrieves a non-empty set R_{2n}^A, the composition of any perfect sequence, length of which is not equal to, or a divisor or a multiple of, $2n$, with any sequence from this set is a perfect sequence of a longer length. The compositions of the same perfect sequence with different sequences from the resulting set R_{2n}^A will produce different perfect sequences.

<u>Example 7.5</u> This example demonstrates use of Algorithm 7.1 for finding sequences over $\boldsymbol{Q}_{24}$.

Step 1. We have run an exhaustive search for finding perfect sequences of length 5 of the following form:

$\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{x}_4]$, where $\boldsymbol{x}_0, \boldsymbol{x}_1, \boldsymbol{x}_3 \in \boldsymbol{Q}_8$ and $\boldsymbol{x}_2, \boldsymbol{x}_4 \in \boldsymbol{Q}_{24}$.

On our ordinary desktop computer (Intel Pentium 4 2.80GHz, 1.00 GB of RAM, with the computational software package Magma [12] running under Windows XP), the complete exhaustive search over all available sequences of such form was running for about 2 minutes, and has yielded 384 perfect sequences. All found sequences have been stored in a set named *P5Q24*.

Step 2. For every pair of perfect sequences from set *P5Q24*, we constructed the interlace sequence of length 10 by taking the first element of the first sequence in the pair and adding it to the new interlace sequence, then taking the first element of the second sequence in the pair and adding it at the end of the new interlace sequence, and so on, until all elements of both sequences have been exhausted and appeared in the interlace sequence.

Then we performed a check of the interlace sequence for conditions 4 – 5 of Proposition 7.2. Sequences, satisfying the conditions, we placed it in a set named *R10Q24*, otherwise, we started over step 2 and chose another pair of sequences from the set *P5Q24*.

In total, 384 interlace sequences satisfying conditions 3 – 5 of Proposition 7.2 have been found and put in the set *R10Q24*. The computer time required for performing this part of the algorithm was about 2 minutes again.

The compositions of any perfect sequence, whose length not a multiple or a divisor of 10, with any sequence from the set *R10Q24* give perfect sequences of longer length.

For example, sequences $[\,-\boldsymbol{i}, 1, \frac{-1+\boldsymbol{i}+\boldsymbol{j}+\boldsymbol{k}}{2}, 1, -\boldsymbol{i}\,]$ and $[\,-1, \boldsymbol{i}, \boldsymbol{i}, -1, \frac{1-\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}\,]$ were found to be perfect and belonged to the set *P5Q24*. The interlace sequence, the sequence of length 10, is $\operatorname{int}\left([\,-\boldsymbol{i}, 1, \frac{-1+\boldsymbol{i}+\boldsymbol{j}+\boldsymbol{k}}{2}, 1, -\boldsymbol{i}\,], [\,-1, \boldsymbol{i}, \boldsymbol{i}, -1, \frac{1-\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}\,]\right) = [\,-\boldsymbol{i}, -1, 1, \boldsymbol{i}, \frac{-1+\boldsymbol{i}+\boldsymbol{j}+\boldsymbol{k}}{2}, \boldsymbol{i}, 1, -1, -\boldsymbol{i}, \frac{1-\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}\,]$. This sequence satisfies conditions 3 – 5 of Proposition 7.2, therefore, the composition of any perfect sequence of any length, except a multiple or a divisor of 10, with this sequence is a perfect sequence.

For instance, the composition of the perfect sequence $\boldsymbol{a} = [\,1, 1, 1, -1\,]$ of length 4 with this sequence gives the sequence of length 20

$$[\,-\boldsymbol{i}, -1, 1, -\boldsymbol{i}, \frac{-1+\boldsymbol{i}+\boldsymbol{j}+\boldsymbol{k}}{2}, \boldsymbol{i}, 1, 1, -\boldsymbol{i}, \frac{1-\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{k}}{2}, -\boldsymbol{i}, 1, 1, \boldsymbol{i}, \frac{-1+\boldsymbol{i}+\boldsymbol{j}+\boldsymbol{k}}{2}, -\boldsymbol{i}, 1, -1, -\boldsymbol{i}, \frac{-1+\boldsymbol{i}+\boldsymbol{j}+\boldsymbol{k}}{2}\,],$$

which is perfect.

Note that there exist more than $4 \cdot 10^{28}$ sequences of length 20 over $\boldsymbol{Q}_{24}$. So, finding a perfect sequence by an exhaustive search is well beyond the computational power of a desktop computer!

8. Conditions Necessary for Perfection over Quaternions

Conditions, which can be deduced from perfection of a sequence over the real quaternions, are studied in this section.

8.1. Balance Theorem over Quaternions

The Balance Theorem for complex perfect sequences was briefly overviewed in Section 4.2.2 of the present work. A generalization of this theorem for quaternions is introduced in this part.

Proposition 8.1 (The Balance Theorem) Let $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ be a perfect sequence over the real quaternions. Then

$$\left\| \sum_{t=0}^{n-1} \boldsymbol{a}_t \right\| = \sum_{t=0}^{n-1} \| \boldsymbol{a}_t \|$$

Proof. Consider the (right) autocorrelation function for any non-zero shift m, $0 \leq m \leq n-1$:

$$ACF_{\boldsymbol{a}}^{R}(m) = \frac{1}{\|\boldsymbol{a}\|} \sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_{t+m}^{*} = 0$$

This is equivalent to

$$\sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_{t+m}^* = 0$$

(8.1)

Summing up equations (8.1) for $1 \leq m \leq n-1$, and adding the equation

$$\sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_t^* = \sum_{t=0}^{n-1} \|\boldsymbol{a}_t\|$$

we have

$$\sum_{m=0}^{n-1} \sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_{t+m}^* = \sum_{t=0}^{n-1} \left(\boldsymbol{a}_t \sum_{m=0}^{n-1} \boldsymbol{a}_{t+m}^* \right) = \sum_{t=0}^{n-1} \left(\boldsymbol{a}_t \sum_{t_1=0}^{n-1} \boldsymbol{a}_{t_1}^* \right) = \left(\sum_{t=0}^{n-1} \boldsymbol{a}_t \right) \left(\sum_{t=0}^{n-1} \boldsymbol{a}_t^* \right)$$

$$= \left(\sum_{t=0}^{n-1} \boldsymbol{a}_t \right) \left(\sum_{t=0}^{n-1} \boldsymbol{a}_t \right)^* = \left\| \left(\sum_{t=0}^{n-1} \boldsymbol{a}_t \right) \right\|$$

Since the (right) autocorrelation values of a perfect sequence for all non-zero shifts m are equal to zero, the only summand in the sum above which is not equal to zero is for $m = 0$, and hence

$$\sum_{m=0}^{n-1} \sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_{t+m}^* = \sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_t^* = \sum_{t=0}^{n-1} \|\boldsymbol{a}_t\|$$

Thus,

$$\left\| \left(\sum_{t=0}^{n-1} \boldsymbol{a}_t \right) \right\| = \sum_{t=0}^{n-1} \|\boldsymbol{a}_t\| \,. \square$$

Example 8.1 Consider the perfect sequence $\boldsymbol{a} * \boldsymbol{b}$ of length 30 from Example 7.2. Because all elements of $\boldsymbol{a} * \boldsymbol{b}$ have norm 1, $\|\boldsymbol{a} * \boldsymbol{b}\| = \sum_{t=0}^{29} \|\boldsymbol{a}_t \boldsymbol{b}_t\| = \sum_{t=0}^{29} 1 = 30$. Then,

$$\begin{aligned}\left\|\sum_{t=0}^{29}\boldsymbol{a}_t\boldsymbol{b}_t\right\| &= \left\|\frac{-1+\boldsymbol{i}-\boldsymbol{j}+\boldsymbol{k}}{2}+1-\boldsymbol{i}-\boldsymbol{j}-\boldsymbol{j}+\frac{1+\boldsymbol{i}+\boldsymbol{j}+\boldsymbol{k}}{2}+\boldsymbol{j}+\boldsymbol{k}-\boldsymbol{i}-\boldsymbol{i}\right.\\ &\quad+\frac{1-\boldsymbol{i}+\boldsymbol{j}-\boldsymbol{k}}{2}-\boldsymbol{i}-\boldsymbol{i}+\boldsymbol{k}+\boldsymbol{j}+\frac{1+\boldsymbol{i}+\boldsymbol{j}+\boldsymbol{k}}{2}-\boldsymbol{j}-\boldsymbol{j}-\boldsymbol{i}+1\\ &\quad\left.+\frac{-1+\boldsymbol{i}-\boldsymbol{j}+\boldsymbol{k}}{2}-\boldsymbol{i}+\boldsymbol{i}-\boldsymbol{j}+\boldsymbol{j}+\frac{-1+\boldsymbol{i}+\boldsymbol{j}-\boldsymbol{k}}{2}+\boldsymbol{j}-\boldsymbol{j}+\boldsymbol{i}-\boldsymbol{i}\right\|\\ &= \|2-4\boldsymbol{i}-\boldsymbol{j}+3\boldsymbol{k}\| = 30 = \|\boldsymbol{a}*\boldsymbol{b}\,\|\end{aligned}$$

8.2. Generalizations of the Balance Theorem

As the Balance Theorem in Section 8.1 suggests, perfect sequences possess some special statistical properties. In this part some new results, revealing more similar properties, are introduced. These new results, given in Propositions 8.2 and 8.3, may be regarded as generalizations of the Balance Theorem.

Proposition 8.2 Let $\boldsymbol{a}=[\boldsymbol{a}_0,\boldsymbol{a}_1,\dots,\boldsymbol{a}_{n-1}]$ be a perfect sequence over the real quaternions and $n=lm$ for some positive integers l and m. Then

$$\sum_{t_1=0}^{l-1}\left\|\sum_{t_2=0}^{m-1}\boldsymbol{a}_{t_1+lt_2}\right\|=\sum_{t=0}^{n-1}\|\boldsymbol{a}_t\|$$

Proof. The sequence

$$\boldsymbol{A}=\left[\sum_{t=0}^{m-1}\boldsymbol{a}_{lt}\,,\sum_{t=0}^{m-1}\boldsymbol{a}_{1+lt}\,,\dots,\sum_{t=0}^{m-1}\boldsymbol{a}_{(l-1)+lt}\right]$$

is perfect by Proposition 6.5. Then, by Proposition 8.1,

$$\left\| \sum_{t_1=0}^{l-1} \sum_{t_2=0}^{m-1} \boldsymbol{a}_{t_1+lt_2} \right\| = \sum_{t_1=0}^{l-1} \left\| \sum_{t_2=0}^{m-1} \boldsymbol{a}_{t_1+lt_2} \right\|$$

Note that

$$\left\| \sum_{t_1=0}^{l-1} \sum_{t_2=0}^{m-1} \boldsymbol{a}_{t_1+lt_2} \right\| = \left\| \sum_{t=0}^{n-1} \boldsymbol{a}_t \right\|$$

Since $\boldsymbol{a}$ is assumed perfect,

$$\left\| \sum_{t=0}^{n-1} \boldsymbol{a}_t \right\| = \sum_{t=0}^{n-1} \|\boldsymbol{a}_t\|$$

This proves Proposition 8.2. □

Example 8.2 If $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \boldsymbol{a}_4, \boldsymbol{a}_5]$ is a perfect sequence of length 6, then, by Proposition 8.2,

$$\|\boldsymbol{a}_0 + \boldsymbol{a}_2 + \boldsymbol{a}_4\| + \|\boldsymbol{a}_1 + \boldsymbol{a}_3 + \boldsymbol{a}_5\| = \|\boldsymbol{a}\|$$

and

$$\|\boldsymbol{a}_0 + \boldsymbol{a}_3\| + \|\boldsymbol{a}_1 + \boldsymbol{a}_4\| + \|\boldsymbol{a}_2 + \boldsymbol{a}_5\| = \|\boldsymbol{a}\|$$

Consider the perfect sequence $\boldsymbol{a} = [\,-\boldsymbol{i},\ \boldsymbol{j},\ -\boldsymbol{i}, -\boldsymbol{j}, -1, -\boldsymbol{j}\,]$ of length 6.

$$\|\boldsymbol{a}\| = \sum_{t=0}^{n-1} \|\boldsymbol{a}_t\| = 6$$

Then,

$$\|-\boldsymbol{i} - \boldsymbol{i} - 1\| + \|\boldsymbol{j} - \boldsymbol{j} - \boldsymbol{j}\| = 5 + 1 = 6$$

and

$$\|-\boldsymbol{i} - \boldsymbol{j}\| + \|\boldsymbol{j} - 1\| + \|-\boldsymbol{i} - \boldsymbol{j}\| = 2 + 2 + 2 = 6$$

Proposition 8.3 Let $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ be a perfect sequence over the real quaternions, and l,m be positive integers satisfying

1. $1 \le l, m \le n-1$ and
2. $\gcd(l,n) = 1$

Then the following identity holds

$$\sum_{t=0}^{n-1} \left\| \sum_{t_1=0}^{m-1} \boldsymbol{a}_{t+lt_1} \right\| = m\|\boldsymbol{a}\|$$

Proof. Consider the set of defining equations for a (right) perfect sequence over the real quaternions:

$$\begin{cases} \sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_t^* = \|\boldsymbol{a}\| \\ \sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_{t+1}^* = 0 \\ \quad \dots \\ \sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_{t+n-1}^* = 0 \end{cases}$$

Consider the sum of the following equations from this set:

- the first equation taken m times;
- the l -th equation taken $(m-1)$ times;
- the $2l$ -th equation taken $(m-2)$ times;
- …
- the $(m-1)l$ -th equation taken 1 time;
- the $(n-(m-1)l)$ -th equation taken 1 time;
- …

- $(n-2l)$ -th equation taken $(m-2)$ times;
- $(n-l)$ -th equations taken $(m-1)$ times.

Note that the total number of the equations in this sum is $m+(m-1)+\cdots+1+1+\cdots+(m-1)=m^2$. Conditions 1 and 2 ensure that $sl \neq 0 \; mod \; n$ for any $s, 1 \leq s \leq n-1$, implying that the first equation $\sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_t^* = \|\boldsymbol{a}\|$ is taken exactly m times.

$$m\sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_t^* + (m-1)\sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_{t+l}^* + \cdots + \sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_{t+(m-1)l}^* + \sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_{t+n-(m-1)l}^* + \cdots$$
$$+ (m-1)\sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_{t+n-l}^*$$

Using the commutativity of addition, re-arrange the order of summation in some equations, shifting the summands circularly:

$$= \underbrace{\sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_t^* + \sum_{t=0}^{n-1} \boldsymbol{a}_{t+l} \boldsymbol{a}_{t+l}^* + \cdots + \sum_{t=0}^{n-1} \boldsymbol{a}_{t+(m-1)l} \boldsymbol{a}_{t+(m-1)l}^*}_{m}$$
$$+ \underbrace{\sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_{t+l}^* + \sum_{t=0}^{n-1} \boldsymbol{a}_{t+l} \boldsymbol{a}_{t+2l}^* + \cdots + \sum_{t=0}^{n-1} \boldsymbol{a}_{t+(m-1)l} \boldsymbol{a}_{t+(m-1)l+l}^*}_{m-1} + \cdots$$
$$+ \sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_{t+(m-1)l}^* + \sum_{t=0}^{n-1} \boldsymbol{a}_{t+(m-1)l} \boldsymbol{a}_t^* + \cdots$$
$$+ \underbrace{\sum_{t=0}^{n-1} \boldsymbol{a}_{t+l} \boldsymbol{a}_t^* + \sum_{t=0}^{n-1} \boldsymbol{a}_{t+2l} \boldsymbol{a}_{t+l}^* + \cdots + \sum_{t=0}^{n-1} \boldsymbol{a}_{t+(m-1)l+l} \boldsymbol{a}_{t+(m-1)l}^*}_{m-1}$$

$$= \sum_{t=0}^{n-1} \big(\boldsymbol{a}_t \boldsymbol{a}_t^* + \boldsymbol{a}_{t+l} \boldsymbol{a}_{t+l}^* + \cdots + \boldsymbol{a}_{t+(m-1)l} \boldsymbol{a}_{t+(m-1)l}^* + \boldsymbol{a}_t \boldsymbol{a}_{t+l}^* + \boldsymbol{a}_{t+l} \boldsymbol{a}_{t+2l}^* + \cdots$$
$$+ \boldsymbol{a}_{t+(m-1)l} \boldsymbol{a}_{t+(m-1)l+l}^* + \cdots + \boldsymbol{a}_t \boldsymbol{a}_{t+(m-1)l}^* + \boldsymbol{a}_{t+(m-1)l} \boldsymbol{a}_t^* + \cdots + \boldsymbol{a}_{t+l} \boldsymbol{a}_t^*$$
$$+ \boldsymbol{a}_{t+2l} \boldsymbol{a}_{t+l}^* + \cdots + \boldsymbol{a}_{t+(m-1)l+l} \boldsymbol{a}_{t+(m-1)l}^* \big)$$

$$= \sum_{t=0}^{n-1} \left(\boldsymbol{a}_t + \boldsymbol{a}_{t+l} + \cdots + \boldsymbol{a}_{t+(m-1)l}\right)\left(\boldsymbol{a}_t^* + \boldsymbol{a}_{t+l}^* + \cdots + \boldsymbol{a}_{t+(m-1)l}^*\right)$$

$$= \sum_{t=0}^{n-1} \left\| \sum_{t_1=0}^{m-1} \boldsymbol{a}_{t+lt_1} \right\|$$

The sum of the right hand parts of the equations is

$$m\|\boldsymbol{a}\| + (m-1)\cdot 0 + (m-2)\cdot 0 + \cdots + 0 + 0 + \cdots + (m-2)\cdot 0 + (m-1)\cdot 0 = m\|\boldsymbol{a}\|.$$

Thus,

$$m\|\boldsymbol{a}\| = \sum_{t=0}^{n-1} \left\| \sum_{t_1=0}^{m-1} \boldsymbol{a}_{t+lt_1} \right\|$$

This proves Proposition 8.3 □

Example 8.3 For a perfect sequence of length 6 over unit quaternions, Proposition 8.3 states that whatever positive integers l and m we choose, both not greater than 6, and l is relatively prime with 6, the identity $\sum_{t=0}^{5}\left\|\sum_{t_1=0}^{m-1} \boldsymbol{a}_{t+lt_1}\right\| = 6m$ holds. Let's illustrate this identity for the perfect sequence $\boldsymbol{a} = [\,-\boldsymbol{i}, \boldsymbol{j}, -\boldsymbol{i}, -\boldsymbol{j}, -1, -\boldsymbol{j}\,]$ from Example 8.2, for several different combinations of l and m.

$l = 5, m = 2$:

$$\sum_{t=0}^{5} \left\| \sum_{t_1=0}^{1} \boldsymbol{a}_{t+5t_1} \right\|$$

$$= \|\boldsymbol{a}_0 + \boldsymbol{a}_5\| + \|\boldsymbol{a}_1 + \boldsymbol{a}_0\| + \|\boldsymbol{a}_2 + \boldsymbol{a}_1\| + \|\boldsymbol{a}_3 + \boldsymbol{a}_2\| + \|\boldsymbol{a}_4 + \boldsymbol{a}_3\|$$
$$+ \|\boldsymbol{a}_5 + \boldsymbol{a}_4\|$$
$$= \|-\boldsymbol{i} - \boldsymbol{j}\| + \|\boldsymbol{j} - \boldsymbol{i}\| + \|-\boldsymbol{i} + \boldsymbol{j}\| + \|-\boldsymbol{j} - \boldsymbol{i}\| + \|-1 - \boldsymbol{j}\| + \|-\boldsymbol{j} - 1\|$$
$$= 2 + 2 + 2 + 2 + 2 + 2 = 12 = 6 \cdot 2$$

$l = 1, m = 4$:

$$\sum_{t=0}^{5}\left\|\sum_{t_1=0}^{3}\boldsymbol{a}_{t+t_1}\right\|$$

$$= \|\boldsymbol{a}_0 + \boldsymbol{a}_1 + \boldsymbol{a}_2 + \boldsymbol{a}_3\| + \|\boldsymbol{a}_1 + \boldsymbol{a}_2 + \boldsymbol{a}_3 + \boldsymbol{a}_4\| + \|\boldsymbol{a}_2 + \boldsymbol{a}_3 + \boldsymbol{a}_4 + \boldsymbol{a}_5\|$$
$$+ \|\boldsymbol{a}_3 + \boldsymbol{a}_4 + \boldsymbol{a}_5 + \boldsymbol{a}_0\| + \|\boldsymbol{a}_4 + \boldsymbol{a}_5 + \boldsymbol{a}_0 + \boldsymbol{a}_1\| + \|\boldsymbol{a}_5 + \boldsymbol{a}_0 + \boldsymbol{a}_1 + \boldsymbol{a}_2\|$$
$$= \|-\boldsymbol{i} + \boldsymbol{j} - \boldsymbol{i} - \boldsymbol{j}\| + \|\boldsymbol{j} - \boldsymbol{i} - \boldsymbol{j} - 1\| + \|-\boldsymbol{i} - \boldsymbol{j} - 1 - \boldsymbol{j}\| + \|-\boldsymbol{j} - 1 - \boldsymbol{j} - \boldsymbol{i}\|$$
$$+ \|-1 - j - \boldsymbol{i} + \boldsymbol{j}\| + \|-\boldsymbol{j} - \boldsymbol{i} + \boldsymbol{j} - \boldsymbol{i}\| = 4 + 2 + 6 + 6 + 2 + 4 = 24 = 6 \cdot 4$$

$l = 5, m = 5$:

$$\sum_{t=0}^{5}\left\|\sum_{t_1=0}^{4}\boldsymbol{a}_{t+5t_1}\right\|$$

$$= \|\boldsymbol{a}_0 + \boldsymbol{a}_5 + \boldsymbol{a}_4 + \boldsymbol{a}_3 + \boldsymbol{a}_2\| + \|\boldsymbol{a}_1 + \boldsymbol{a}_0 + \boldsymbol{a}_5 + \boldsymbol{a}_4 + \boldsymbol{a}_3\|$$
$$+ \|\boldsymbol{a}_2 + \boldsymbol{a}_1 + \boldsymbol{a}_0 + \boldsymbol{a}_5 + \boldsymbol{a}_4\| + \|\boldsymbol{a}_3 + \boldsymbol{a}_2 + \boldsymbol{a}_1 + \boldsymbol{a}_0 + \boldsymbol{a}_5\|$$
$$+ \|\boldsymbol{a}_4 + \boldsymbol{a}_3 + \boldsymbol{a}_2 + \boldsymbol{a}_1 + \boldsymbol{a}_0\| + \|\boldsymbol{a}_5 + \boldsymbol{a}_4 + \boldsymbol{a}_3 + \boldsymbol{a}_2 + \boldsymbol{a}_1\|$$
$$= \|-\boldsymbol{i} - \boldsymbol{j} - 1 - \boldsymbol{j} - \boldsymbol{i}\| + \|\boldsymbol{j} - \boldsymbol{i} - \boldsymbol{j} - 1 - \boldsymbol{j}\| + \|-\boldsymbol{i} + \boldsymbol{j} - \boldsymbol{i} - \boldsymbol{j} - 1\|$$
$$+ \|-\boldsymbol{j} - \boldsymbol{i} + \boldsymbol{j} - \boldsymbol{i} - \boldsymbol{j}\| + \|-1 - \boldsymbol{j} - \boldsymbol{i} + \boldsymbol{j} - \boldsymbol{i}\| + \|-\boldsymbol{j} - 1 - \boldsymbol{j} - \boldsymbol{i} + \boldsymbol{j}\|$$
$$= 9 + 3 + 5 + 5 + 5 + 3 = 30 = 6 \cdot 5$$

8.3. Perfection over Quaternions and the Geometry of $\mathbb{R}^3$

Some interesting properties, relating perfection over the quaternions and the geometry of Euclidean space $\mathbb{R}^3$, are studied in this part.

Proposition 8.4 Let $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ be a perfect sequence over the real quaternions.

(A) If each element $\boldsymbol{a}_t, 0 \le t \le n-1$, is expanded as the sum of scalar and vector parts, $\boldsymbol{a}_t = a_t + \overrightarrow{a_t}$, then for each $1 \le m \le n-1$ the following identity holds:

$$\sum_{t=0}^{n-1} \overrightarrow{a_t} \times \overrightarrow{a_{t+m}} = 0$$

where ‘×’ stands for the vector cross product in three-dimensional Euclidian space.

(B) If $\boldsymbol{a}_t, 0 \le t \le n-1$, are expanded as in (A) above, then for each $1 \le m \le n-1$ the following identity holds:

$$\sum_{t=0}^{n-1} (a_{t+m} - a_{t-m})\overrightarrow{a_t} = 0$$

(C) If each element $\boldsymbol{a}_t, 0 \le t \le n-1$, is expanded as $\boldsymbol{a}_t = a_t + b_t i + c_t j + d_t k$, then for each $1 \le m \le n-1$ the following identities hold:

$$\sum_{t=0}^{n-1} \begin{vmatrix} a_t & a_{t+m} \\ b_t & b_{t+m} \end{vmatrix} = 0, \qquad \sum_{t=0}^{n-1} \begin{vmatrix} a_t & a_{t+m} \\ c_t & c_{t+m} \end{vmatrix} = 0, \qquad \sum_{t=0}^{n-1} \begin{vmatrix} a_t & a_{t+m} \\ d_t & d_{t+m} \end{vmatrix} = 0$$

where $\begin{vmatrix} \cdot & \cdot \\ \cdot & \cdot \end{vmatrix}$ stands for the determinant of a 2 × 2 matrix.

(D) If $\boldsymbol{a}_t, 0 \le t \le n-1$, are expanded as in (C) above, then for each $1 \le m \le n-1$ the following identities hold:

$$\sum_{t=0}^{n-1} \begin{vmatrix} b_t & b_{t+m} \\ c_t & c_{t+m} \end{vmatrix} = 0, \qquad \sum_{t=0}^{n-1} \begin{vmatrix} c_t & c_{t+m} \\ d_t & d_{t+m} \end{vmatrix} = 0, \qquad \sum_{t=0}^{n-1} \begin{vmatrix} b_t & b_{t+m} \\ d_t & d_{t+m} \end{vmatrix} = 0$$

(E) Let $[\boldsymbol{a}, \boldsymbol{b}] = \boldsymbol{ab} - \boldsymbol{ba}$ denote the *commutator* of two quaternions $\boldsymbol{a}$ and $\boldsymbol{b}$. Then for each $1 \le m \le n-1$ the following identity holds:

$$\sum_{t=0}^{n-1} [\boldsymbol{a}_t, \boldsymbol{a}_{t+m}] = 0$$

Proof.

(A) Since $\boldsymbol{a}$ is assumed perfect, implying it is both right and left perfect by Proposition 5.1, the following is true for any non-zero shift m, $0 \leq m \leq n-1$:

$$0 = ACF_{\boldsymbol{a}}^{R}(m) = \frac{1}{\|\boldsymbol{a}\|}\sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_{t+m}^{*}$$

$$= \frac{1}{\|\boldsymbol{a}\|}\sum_{t=0}^{n-1}\left(a_t a_{t+m} - \langle \overrightarrow{a_t}, \overrightarrow{a_{t+m}} \rangle - a_t\overrightarrow{a_{t+m}} + a_{t+m}\overrightarrow{a_t} - \overrightarrow{a_t} \times \overrightarrow{a_{t+m}}\right)$$

$$= \frac{1}{\|\boldsymbol{a}\|}\sum_{t=0}^{n-1}\left(a_t a_{t+m} - \langle \overrightarrow{a_t}, \overrightarrow{a_{t+m}} \rangle\right) + \frac{1}{\|\boldsymbol{a}\|}\sum_{t=0}^{n-1}\left(-a_t\overrightarrow{a_{t+m}} + a_{t+m}\overrightarrow{a_t} - \overrightarrow{a_t} \times \overrightarrow{a_{t+m}}\right)$$

and

$$0 = ACF_{\boldsymbol{a}}^{L}(m) = \frac{1}{\|\boldsymbol{a}\|}\sum_{t=0}^{n-1} \boldsymbol{a}_t^{*} \boldsymbol{a}_{t+m}$$

$$= \frac{1}{\|\boldsymbol{a}\|}\sum_{t=0}^{n-1}\left(a_t a_{t+m} - \langle \overrightarrow{a_t}, \overrightarrow{a_{t+m}} \rangle + a_t\overrightarrow{a_{t+m}} - a_{t+m}\overrightarrow{a_t} - \overrightarrow{a_t} \times \overrightarrow{a_{t+m}}\right)$$

$$= \frac{1}{\|\boldsymbol{a}\|}\sum_{t=0}^{n-1}\left(a_t a_{t+m} - \langle \overrightarrow{a_t}, \overrightarrow{a_{t+m}} \rangle\right) + \frac{1}{\|\boldsymbol{a}\|}\sum_{t=0}^{n-1}\left(a_t\overrightarrow{a_{t+m}} - a_{t+m}\overrightarrow{a_t} - \overrightarrow{a_t} \times \overrightarrow{a_{t+m}}\right)$$

A quaternion is equal to zero if and only if its scalar and vector parts are both equal to zero. Therefore,

$$\sum_{t=0}^{n-1}\left(-a_t\overrightarrow{a_{t+m}} + a_{t+m}\overrightarrow{a_t} - \overrightarrow{a_t} \times \overrightarrow{a_{t+m}}\right) = 0 \tag{8.2}$$

and

$$\sum_{t=0}^{n-1}\left(a_t\overrightarrow{a_{t+m}} - a_{t+m}\overrightarrow{a_t} - \overrightarrow{a_t} \times \overrightarrow{a_{t+m}}\right) = 0$$

(8.3)

By summing up equations (8.2) and (8.3), we have

$$\sum_{t=0}^{n-1}\overrightarrow{a_t} \times \overrightarrow{a_{t+m}} = 0$$

This proves the validity of statement (A).

(B) From equations (8.2) and (8.3) it follows that

$$\sum_{t=0}^{n-1}\left(a_t\overrightarrow{a_{t+m}} - a_{t+m}\overrightarrow{a_t}\right) = 0$$

This, after gathering together the terms with equal vector parts, gives the identity of statement (B).

(C) Note that if $\boldsymbol{a_1} = a_1 + b_1\boldsymbol{i} + c_1\boldsymbol{j} + d_1\boldsymbol{k}$ and $\boldsymbol{a_2} = a_2 + b_2\boldsymbol{i} + c_2\boldsymbol{j} + d_2\boldsymbol{k}$ are arbitrary quaternions, then

$$\boldsymbol{a_1}\boldsymbol{a_2^*} - \boldsymbol{a_1^*}\boldsymbol{a_2} = 2(-a_1b_2 + b_1a_2)\boldsymbol{i} + 2(-a_1c_2 + c_1a_2)\boldsymbol{j} + 2(-a_1d_2 + d_1a_2)\boldsymbol{k}$$

Since the sequence $\boldsymbol{a}$ is both right and left perfect, then for any non-zero shift m, $0 \le m \le n - 1$, we have

$$\sum_{t=0}^{n-1}\boldsymbol{a}_t\boldsymbol{a}_{t+m}^* = 0$$

and

$$\sum_{t=0}^{n-1}\boldsymbol{a}_t^*\boldsymbol{a}_{t+m} = 0$$

Subtracting the latter from the former, we have:

$$0=\sum_{t=0}^{n-1}\boldsymbol{a}_t\boldsymbol{a}_{t+m}^{*}-\sum_{t=0}^{n-1}\boldsymbol{a}_t^{*}\boldsymbol{a}_{t+m}=\sum_{t=0}^{n-1}(\boldsymbol{a}_t\boldsymbol{a}_{t+m}^{*}-\boldsymbol{a}_t^{*}\boldsymbol{a}_{t+m})$$

$$=2\boldsymbol{i}\sum_{t=0}^{n-1}(-a_tb_{t+m}+b_ta_{t+m})+2\boldsymbol{j}\sum_{t=0}^{n-1}(-a_tc_{t+m}+c_ta_{t+m})+2\boldsymbol{k}\sum_{t=0}^{n-1}(-a_tc_{t+m}+c_ta_{t+m})$$

$$=-2\boldsymbol{i}\sum_{t=0}^{n-1}\begin{vmatrix}a_t & a_{t+m}\\ b_t & b_{t+m}\end{vmatrix}-2\boldsymbol{j}\sum_{t=0}^{n-1}\begin{vmatrix}a_t & a_{t+m}\\ c_t & c_{t+m}\end{vmatrix}-2\boldsymbol{k}\sum_{t=0}^{n-1}\begin{vmatrix}a_t & a_{t+m}\\ c_t & c_{t+m}\end{vmatrix} \tag{8.4}$$

Since a quaternion is only equal to zero when each of its components is equal to zero, from (8.4) we get all the identities of statement (C):

$$\sum_{t=0}^{n-1}\begin{vmatrix}a_t & a_{t+m}\\ b_t & b_{t+m}\end{vmatrix}=0,\sum_{t=0}^{n-1}\begin{vmatrix}a_t & a_{t+m}\\ c_t & c_{t+m}\end{vmatrix}=0,\sum_{t=0}^{n-1}\begin{vmatrix}a_t & a_{t+m}\\ c_t & c_{t+m}\end{vmatrix}=0$$

(D) The cross-product of two vectors $\overrightarrow{a_1}=b_1\boldsymbol{i}+c_1\boldsymbol{j}+d_1\boldsymbol{k}$ and $\overrightarrow{a_2}=b_2\boldsymbol{i}+c_2\boldsymbol{j}+d_2\boldsymbol{k}$ can be expanded as $\overrightarrow{a_1}\times\overrightarrow{a_2}=(c_1d_2-d_1c_2)\boldsymbol{i}+(d_1b_2-b_1d_2)\boldsymbol{j}+(b_1c_2-c_1b_2)\boldsymbol{k}$ (Kyrala [57]). If a sequence $\boldsymbol{a}$ is perfect, then, by part (A) of this Proposition,

$$0=\sum_{t=0}^{n-1}\overrightarrow{a_t}\times\overrightarrow{a_{t+m}}=\sum_{t=0}^{n-1}\big((c_1d_2-d_1c_2)\boldsymbol{i}(d_1b_2-b_1d_2)\boldsymbol{j}+(d_1b_2-b_1d_2)\boldsymbol{j}\big)$$

$$=\sum_{t=0}^{n-1}(c_1d_2-d_1c_2)\boldsymbol{i}+\sum_{t=0}^{n-1}(d_1b_2-b_1d_2)\boldsymbol{j}+\sum_{t=0}^{n-1}(b_1c_2-c_1b_2)\boldsymbol{k}$$

$$=\boldsymbol{i}\sum_{t=0}^{n-1}\begin{vmatrix}c_t & c_{t+m}\\ d_t & d_{t+m}\end{vmatrix}+\boldsymbol{j}\sum_{t=0}^{n-1}\begin{vmatrix}d_t & d_{t+m}\\ b_t & b_{t+m}\end{vmatrix}+\boldsymbol{k}\sum_{t=0}^{n-1}\begin{vmatrix}b_t & b_{t+m}\\ c_t & c_{t+m}\end{vmatrix}$$

Since a quaternion is only equal to zero when each of its components is equal to zero, from (8.4) we get all the identities of statement (D):

$$\sum_{t=0}^{n-1}\begin{vmatrix} c_t & c_{t+m} \\ d_t & d_{t+m} \end{vmatrix} = 0, \sum_{t=0}^{n-1}\begin{vmatrix} d_t & d_{t+m} \\ b_t & b_{t+m} \end{vmatrix} = 0, \sum_{t=0}^{n-1}\begin{vmatrix} b_t & b_{t+m} \\ c_t & c_{t+m} \end{vmatrix} = 0$$

(E) Since the product of two arbitrary quaternions $\boldsymbol{p}$ and $\boldsymbol{q}$ can be expanded as $\boldsymbol{pq} = pq - \langle \vec{p}, \vec{q} \rangle + p\vec{q} + q\vec{p} + \vec{p} \times \vec{q}$ (Kyrala [57]), it follows that $\vec{p} \times \vec{q} = \frac{1}{2}(\boldsymbol{pq} - \boldsymbol{qp})$. With this identity, statement (E) becomes a simple consequence of statement (A). □

<u>Example 8.4</u> For the perfect sequence $\boldsymbol{a} = [\,-\boldsymbol{k}, 1, -\boldsymbol{k}, -\boldsymbol{i}, \boldsymbol{j}, -1, -\boldsymbol{j}, -1, \boldsymbol{j}, -\boldsymbol{i}\,]$ from Example 6.2, the sum of commutators, for $m = 1$, is given by

$$\sum_{t=o}^{9}[\boldsymbol{a}_t, \boldsymbol{a}_{t+m}] = [-\boldsymbol{k}, 1] + [1, -\boldsymbol{k}] + [-\boldsymbol{k}, -\boldsymbol{i}] + [-\boldsymbol{i}, \boldsymbol{j}] + [\boldsymbol{j}, -1] + [-1, -\boldsymbol{j}] + [-\boldsymbol{j}, -1]$$
$$+ [-1, \boldsymbol{j}] + [\boldsymbol{j}, -\boldsymbol{i}] + [-\boldsymbol{i}, -\boldsymbol{k}] = 0 + 0 + 2\boldsymbol{j} - 2\boldsymbol{k} + 0 + 0 + 0 + 0 + 2\boldsymbol{k} - 2\boldsymbol{j}$$
$$= 0$$

8.4. Length of a Perfect Sequence over Q_8

In the next Proposition 8.5 we restrict our attention to considering sequences over the ***i-j-k*** *group* $\boldsymbol{Q}_8$ (Stringham [86]), sometimes called a *quaternion group*. It is a non-abelian multiplicative group of order 8 formed by the unit quaternions $\pm 1, \pm \boldsymbol{i}, \pm \boldsymbol{j}, \pm \boldsymbol{k}$.

<u>Proposition 8.5</u> Let $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ be a perfect sequence with elements from $\boldsymbol{Q}_8$. Then its length n is an even number.

<u>Proof.</u> The multiplicative inverse of a unit quaternion $\boldsymbol{q}$ is unique and equal to its conjugate $\boldsymbol{q}^*$. Therefore, being a multiplicative group, the set of elements $\boldsymbol{Q}_8$ is closed in respect to multiplication and taking conjugates.

As it has been shown earlier, perfection of a sequence $\boldsymbol{a}$ is equivalent to $\sum_{t=0}^{n-1} \boldsymbol{a}_t \boldsymbol{a}_{t+m}^* = 0$ (Equations (8.1)).

The terms in the left hand part of (8.1) are products of elements in the group $\boldsymbol{Q}_8$.

Note that the sum of two quaternions from $\boldsymbol{Q}_8$ can only be equal to zero if they are a pair of additive inverses. For any element $\boldsymbol{x}$ of the group $\boldsymbol{Q}_8$ its additive inverse, $-\boldsymbol{x}$, is also in $\boldsymbol{Q}_8$. This additive inverse is unique and can not be represented as a sum of elements of $\boldsymbol{Q}_8$. Therefore, in order to be equal to zero, the sum of finitely many elements of the group $\boldsymbol{Q}_8$ must only contain pairs of quaternions and their additive inverses. That is, for any quaternion $\boldsymbol{x} \in \boldsymbol{Q}_8$ the number $n_{\boldsymbol{x}}$ of its appearances in the sum should be equal to number $n_{-\boldsymbol{x}}$ of appearances of $-\boldsymbol{x}$.

We have $n_{-1} + n_1 + n_{-\boldsymbol{i}} + n_{\boldsymbol{i}} + n_{-\boldsymbol{j}} + n_{\boldsymbol{j}} + n_{-\boldsymbol{k}} + n_{\boldsymbol{k}} = n$.

However, from (8.1), $n_{-1} = n_1, n_{-\boldsymbol{i}} = n_{\boldsymbol{i}}\,, n_{-\boldsymbol{j}} = n_{\boldsymbol{j}}, n_{-\boldsymbol{k}} = n_{\boldsymbol{k}}$.

Therefore, $n = 2n_1 + 2n_{\boldsymbol{i}} + 2n_{\boldsymbol{j}} + 2n_{\boldsymbol{k}} = 2\left(n_1 + n_{\boldsymbol{i}} + n_{\boldsymbol{j}} + n_{\boldsymbol{k}}\right)$.

Thus n is an even number. □

9. Discrete Fourier Transform of a Perfect Sequence over Quaternions

Most of the properties of perfect sequences over the real quaternions, discussed in the previous sections, coincide with similar properties of perfect sequences over the complex numbers. The following statements are true for perfect sequences over the real quaternions and over the complex numbers:

- Left and right perfection are equivalent;
- Multiplication of a perfect sequence by a scalar (either from the left, or from the right) preserves perfection;
- The conjugate sequence of a perfect sequence is perfect;
- Any shift of a perfect sequence is perfect;
- A proper decimation of a perfect sequence is perfect;
- The composition of two or more perfect sequences of co-prime lengths is perfect.

One might be tempted to think that perfect sequences over the quaternions have all the properties of complex perfect sequences. However, this is not true. A difference appears when we consider the discrete Fourier transform of a perfect sequence.

In this section, we introduce the discrete Fourier transform of a sequence over the real quatenions, and discuss a difference between perfect sequences over the real quaternions and the complex numbers.

9.1. Quaternionic Discrete Fourier Transform

We define the discrete Fourier transform over the quaternions by analogy with the discrete Fourier transform over the complex numbers. However, due to non-commutativity of the quaternions, it is possible to consider two distinct discrete Fourier transforms: left and right discrete Fourier transforms.

<u>Definition 9.1</u> We call the sequence $DFT^L(\boldsymbol{x}) = \boldsymbol{X}^L = [\boldsymbol{X}_0^L, \boldsymbol{X}_1^L, \dots, \boldsymbol{X}_{n-1}^L]$ over the real quaternions the *left discrete Fourier transform* (*left DFT*) of a sequence $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$ over the real quaternions if

$$\boldsymbol{X}_s^L = \sum_{t=0}^{n-1} e^{-\frac{2\pi i}{n}st}\boldsymbol{x}_t$$

where $e^{\frac{2\pi i}{n}}$ is the principal n-th complex root of unity. The elements $\boldsymbol{X}_0^L, \boldsymbol{X}_1^L, \dots, \boldsymbol{X}_{n-1}^L$ of the left DFT are called the *left discrete Fourier transform coefficients*.

<u>Definition 9.2</u> We call the sequence $DFT^R(\boldsymbol{x}) = \boldsymbol{X}^R = [\boldsymbol{X}_0^R, \boldsymbol{X}_1^R, \dots, \boldsymbol{X}_{n-1}^R]$ over the real quaternions the *right discrete Fourier transform* (*right DFT*) of a sequence $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$ over the real quaternions if

$$\boldsymbol{X}_s^R = \sum_{t=0}^{n-1} \boldsymbol{x}_t e^{-\frac{2\pi i}{n}st}$$

where $e^{\frac{2\pi i}{n}}$ is the principal n-th complex root of unity. The elements $\boldsymbol{X}_0^R, \boldsymbol{X}_1^R, \dots, \boldsymbol{X}_{n-1}^R$ of the right DFT are called the *right discrete Fourier transform coefficients*.

Also, we define left and right inverse discrete Fourier transforms.

Definition 9.3 We call the sequence $IDFT^L(\boldsymbol{X}) = \boldsymbol{x}^L = [\boldsymbol{x}_0^L, \boldsymbol{x}_1^L, \dots, \boldsymbol{x}_{n-1}^L]$ over the real quaternions the *left inverse discrete Fourier transform* (*left IDFT*) of a sequence $\boldsymbol{X} = [\boldsymbol{X}_0, \boldsymbol{X}_1, \dots, \boldsymbol{X}_{n-1}]$ over the real quaternions if

$$\boldsymbol{x}_s^L = \frac{1}{n}\sum_{t=0}^{n-1} e^{\frac{2\pi i}{n}st}\boldsymbol{X}_t$$

where $e^{\frac{2\pi i}{n}}$ is the principal n-th complex root of unity. The elements $\boldsymbol{x}_0^L, \boldsymbol{x}_1^L, \dots, \boldsymbol{x}_{n-1}^L$ of the left DFT are called the *left inverse discrete Fourier transform coefficients*.

Definition 9.4 We call the sequence $IDFT^R(\boldsymbol{X}) = \boldsymbol{x}^R = [\boldsymbol{x}_0^R, \boldsymbol{x}_1^R, \dots, \boldsymbol{x}_{n-1}^R]$ over the real quaternions the *right inverse discrete Fourier transform* (*right IDFT*) of a sequence $\boldsymbol{X} = [\boldsymbol{X}_0, \boldsymbol{X}_1, \dots, \boldsymbol{X}_{n-1}]$ over the real quaternions if

$$\boldsymbol{x}_s^R = \frac{1}{n}\sum_{t=0}^{n-1} \boldsymbol{X}_t e^{\frac{2\pi i}{n}st}$$

where $e^{\frac{2\pi i}{n}}$ is the principal n-th complex root of unity. The elements $\boldsymbol{x}_0^R, \boldsymbol{x}_1^R, \dots, \boldsymbol{x}_{n-1}^R$ of the right DFT are called the *right inverse discrete Fourier transform coefficients*.

The left and the left inverse discrete Fourier transforms, so defined, possess an important property: they are the inverse functions of each other, and likewise for the right and the right inverse discrete Fourier transforms. Refer to Proposition 9.1 below.

Proposition 9.1 Let $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$ be a sequence over the real quaternions. Then $\boldsymbol{x} = IDFT^R\big(DFT^R(\boldsymbol{x})\big)$ and $\boldsymbol{x} = IDFT^L\big(DFT^L(\boldsymbol{x})\big)$.

Proof. Let $DFT^R(\boldsymbol{x}) = [\boldsymbol{X}_0^R, \boldsymbol{X}_1^R, \dots, \boldsymbol{X}_{n-1}^R]$. If we denote the s-th element of the sequence $IDFT^R\big(DFT^R(\boldsymbol{x})\big)$ by $\big[IDFT^R\big(DFT^R(\boldsymbol{x})\big)\big]_s$, we have

$$\big[IDFT^R\big(DFT^R(\boldsymbol{x})\big)\big]_s = \frac{1}{n}\sum_{t=0}^{n-1} \boldsymbol{X}_t^R e^{\frac{2\pi i}{n}st} = \frac{1}{n}\sum_{t=0}^{n-1}\sum_{t_1=0}^{n-1} \boldsymbol{x}_{t_1} e^{-\frac{2\pi i}{n}tt_1} e^{\frac{2\pi i}{n}st}$$

$$= \frac{1}{n}\sum_{t=0}^{n-1}\sum_{t_1=0}^{n-1} \boldsymbol{x}_{t_1} e^{-\frac{2\pi i}{n}t(s-t_1)} = \frac{1}{n}\sum_{t_1=0}^{n-1} \boldsymbol{x}_{t_1} \sum_{t=0}^{n-1} e^{-\frac{2\pi i}{n}t(s-t_1)}$$

Since $\sum_{t=0}^{n-1} e^{-\frac{2\pi i}{n}t(s-t_1)}$ represents the sum of n-th roots of unity,

$\sum_{t=0}^{n-1} e^{-\frac{2\pi i}{n}t(s-t_1)} = \begin{cases} 0, \ s \neq t_1 \\ n, \ s = t_1 \end{cases}.$

Therefore, the equality above is continued as

$$= \frac{1}{n} n \boldsymbol{x}_s = \boldsymbol{x}_s$$

The statement $\boldsymbol{x} = IDFT^L\big(DFT^L(\boldsymbol{x})\big)$ is proved in a similar way. □

The left and the right discrete Fourier transforms of a sequence $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$ over the real quaternions are, in general, non-equal. Consider Example 9.1.

Example 9.1 The left and the right discrete Fourier transform coefficients of the sequence $\boldsymbol{x} = [\,1, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\,]$ are listed in Table 9.1:

Table 9.1 Left and right discrete Fourier transform coefficients of the sequence $\boldsymbol{x} = [\,1, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\,]$.

s	$\boldsymbol{X}_s^L$	$\lVert\boldsymbol{X}_s^L\rVert$	$\boldsymbol{X}_s^R$	$\lVert\boldsymbol{X}_s^R\rVert$
0	$1+\boldsymbol{i}+\boldsymbol{j}+\boldsymbol{k}$	4	$1+\boldsymbol{i}+\boldsymbol{j}+\boldsymbol{k}$	4
1	$2-2\boldsymbol{j}$	8	2	4
2	$1-\boldsymbol{i}+\boldsymbol{j}-\boldsymbol{k}$	4	$1-\boldsymbol{i}+\boldsymbol{j}-\boldsymbol{k}$	4
3	0	0	$-2\boldsymbol{j}$	4

It is easy to observe that $DFT^L(\boldsymbol{x}) \neq DFT^R(\boldsymbol{x})$.

Remark 9.1 For a sequence over the complex numbers, concepts of the left and the right Fourier transforms coincide, due to commutativity of the complex numbers. That is, $DFT^L(x) = DFT^R(x)$ for every sequence $x = [x_0, x_1, \dots, x_{n-1}]$ over the complex numbers.

However, as stated in Proposition 9.2 below, there exists a simple relationship between the left and the right discrete quaternionic Fourier transforms.

Proposition 9.2 Let $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-1}]$ be a sequence over the real quaternions, and $\boldsymbol{x}^* = [\boldsymbol{x}_0^*, \boldsymbol{x}_1^*, \dots, \boldsymbol{x}_{n-1}^*]$ be its conjugate sequence. Then, if we denote the s-th element of a sequence by $[\cdot]_s$,

$$[DFT^L(\boldsymbol{x})]_s = [DFT^R(\boldsymbol{x}^*)]_{n-s}^*$$

Proof.

$$[DFT^L(\boldsymbol{x})]_s = \sum_{t=0}^{n-1} e^{-\frac{2\pi i}{n}st}\boldsymbol{x}_t = \left(\sum_{t=0}^{n-1} \boldsymbol{x}_t^* e^{\frac{2\pi i}{n}st}\right)^* = \left(\sum_{t=0}^{n-1} \boldsymbol{x}_t^* e^{-\frac{2\pi i}{n}(n-s)t}\right)^* = [DFT^R(\boldsymbol{x}^*)]_{n-s}^*. \square$$

In contrast to sequences over the complex numbers, the left (right) discrete Fourier transform of a sequence over the real quaternions with all elements of equal norm is not always perfect. Consider two examples below, for non-perfect and perfect sequences over the real quaternions:

Example 9.2 Consider the non-perfect sequence $[\,1, 1, 1, \boldsymbol{k}\,]$ with all elements of norm 1.

$$DFT^L([\,1,1,1,\boldsymbol{k}\,]) = [\,3+\boldsymbol{k}, -\boldsymbol{i}-\boldsymbol{j}, 1-\boldsymbol{k}, \boldsymbol{i}+\boldsymbol{j}\,]$$

$$DFT^R([\,1,1,1,\boldsymbol{k}\,]) = [\,3+\boldsymbol{k}, -\boldsymbol{i}+\boldsymbol{j}, 1-\boldsymbol{k}, \boldsymbol{i}-\boldsymbol{j}\,]$$

Neither the left nor the right Fourier transforms are perfect. Indeed,

$$ACF^R_{DFT^L([\,1,1,1,\boldsymbol{k}\,])}(1)$$

$$= \frac{1}{4}\big((3+\boldsymbol{k})(-\boldsymbol{i}-\boldsymbol{j})^* + (-\boldsymbol{i}-\boldsymbol{j})(1-\boldsymbol{k})^* + (1-\boldsymbol{k})(\boldsymbol{i}+\boldsymbol{j})^* + (\boldsymbol{i}+\boldsymbol{j})(3+\boldsymbol{k})^*\big)$$

$$= \frac{1}{4}\big((2\boldsymbol{i}+4\boldsymbol{j}) + (-2\boldsymbol{i}) + (-2\boldsymbol{i}) + (2\boldsymbol{i}+4\boldsymbol{j})\big) = \frac{1}{4}\cdot 8\boldsymbol{j} \neq 0$$

$$ACF^R_{DFT^R([\,1,1,1,\boldsymbol{k}\,])}(1)$$

$$= \frac{1}{4}\big((3+\boldsymbol{k})(-\boldsymbol{i}+\boldsymbol{j})^* + (-\boldsymbol{i}+\boldsymbol{j})(1-\boldsymbol{k})^* + (1-\boldsymbol{k})(\boldsymbol{i}-\boldsymbol{j})^* + (\boldsymbol{i}-\boldsymbol{j})(3+\boldsymbol{k})^*\big)$$

$$= \frac{1}{4}\big((4\boldsymbol{i}-2\boldsymbol{j}) + 2\boldsymbol{j} + 2\boldsymbol{j} + (4\boldsymbol{i}-2\boldsymbol{j})\big) = \frac{1}{4}\cdot 8\boldsymbol{i} \neq 0$$

Example 9.3 Consider another sequence $[\,-1,-1,1,\boldsymbol{j},1,-1,-1,\boldsymbol{j}\,]$, which is perfect over the unit quaternions, of length 8. However,

$$DFT^L([\,-1,-1,1,\boldsymbol{j},1,-1,-1,\boldsymbol{j}\,]) \\ = [-2+2\boldsymbol{j},-2-2\boldsymbol{i},2\boldsymbol{i}+2\boldsymbol{k},-2+2\boldsymbol{i},2-2\boldsymbol{j},-2-2\boldsymbol{i},-2\boldsymbol{i}-2\boldsymbol{k},-2+2\boldsymbol{i}\,]$$

$$DFT^R([\,-1,-1,1,\boldsymbol{j},1,-1,-1,\boldsymbol{j}\,]) \\ = [-2+2\boldsymbol{j},-2+2\boldsymbol{i},-2\boldsymbol{i}+2\boldsymbol{k},-2-2\boldsymbol{i},2-2\boldsymbol{j},-2+2\boldsymbol{i},2\boldsymbol{i}-2\boldsymbol{k},-2-2\boldsymbol{i}\,]$$

are not perfect, since

$$ACF^R_{DFT^L([\,-1,-1,1,\boldsymbol{j},1,-1,-1,\boldsymbol{j}\,])}(2) \\ = \frac{1}{8}\big((-2+2\boldsymbol{j})(2\boldsymbol{i}+2\boldsymbol{k})^* + (-2-2\boldsymbol{i})(-2+2\boldsymbol{i})^* + (2\boldsymbol{i}+2\boldsymbol{k})(2-2\boldsymbol{j})^* \\ + (-2+2\boldsymbol{i})(-2-2\boldsymbol{i})^* + (2-2\boldsymbol{j})(-2\boldsymbol{i}-2\boldsymbol{k})^* + (-2-2\boldsymbol{i})(-2+2\boldsymbol{i})^* \\ + (-2\boldsymbol{i}-2\boldsymbol{k})(-2+2\boldsymbol{j})^* + (-2+2\boldsymbol{i})(-2-2\boldsymbol{i})^*\big)$$

$$= \frac{1}{8}\big((8\boldsymbol{k}) + (8\boldsymbol{i}) + (8\boldsymbol{k}) + (-8\boldsymbol{i}) + (8\boldsymbol{k}) + (8\boldsymbol{i}) + (8\boldsymbol{k}) + (8\boldsymbol{i})\big) = \frac{1}{8}\cdot 32\boldsymbol{k} \neq 0$$

$$ACF^L_{DFT^R([\,-1,-1,1,\boldsymbol{j},1,-1,-1,\boldsymbol{j}\,])}(2) \\ = \frac{1}{8}\big((-2+2\boldsymbol{j})(2\boldsymbol{i}-2\boldsymbol{k})^* + (-2+2\boldsymbol{i})(-2-2\boldsymbol{i})^* + (-2\boldsymbol{i}+2\boldsymbol{k})(-2+2\boldsymbol{j})^* \\ + (-2-2\boldsymbol{i})(-2+2\boldsymbol{i})^* + (2-2\boldsymbol{j})(-2\boldsymbol{i}+2\boldsymbol{k})^* + (-2+2\boldsymbol{i})(-2-2\boldsymbol{i})^* \\ + (2\boldsymbol{i}-2\boldsymbol{k})(2-2\boldsymbol{j})^* + (-2-2\boldsymbol{i})(-2+2\boldsymbol{i})^*\big)$$

$$= \frac{1}{8}\big((8\boldsymbol{i}) + (-8\boldsymbol{i}) + (8\boldsymbol{i}) + (8\boldsymbol{i}) + (8\boldsymbol{i}) + (-8\boldsymbol{i}) + (8\boldsymbol{i}) + (8\boldsymbol{i})\big) = \frac{1}{8}\cdot 32\boldsymbol{i} \neq 0$$

Example 9.3 demonstrates that perfection is not, in general, preserved by taking the left or the right discrete Fourier transform of a quaternionic perfect sequence.

9.2. Norm of the Discrete Fourier Transform Coefficients of a Perfect Sequence

In Section 4.1 of the present work, it has been shown that sequence $a = [a_0, a_1, \dots, a_{n-1}]$ over the complex numbers is perfect if and only if all its discrete Fourier transform coefficients have equal norm $\|a\|$. Would the condition of having all discrete Fourier transform coefficients of equal norm be necessary and sufficient for perfection over the quaternions? Consider the example below.

Example 9.4 The left and right Fourier transforms of the non-perfect sequence $\boldsymbol{x} = [\,1, 1, \boldsymbol{k}, -\boldsymbol{k}\,]$ are as follow:

$$DFT^L(\boldsymbol{x}) = [\,2, 1 - \boldsymbol{i} + \boldsymbol{j} - \boldsymbol{k}, 2\boldsymbol{k}, 1 + \boldsymbol{i} - \boldsymbol{j} - \boldsymbol{k}\,]$$

$$DFT^R(\boldsymbol{x}) = [\,2, 1 - \boldsymbol{i} - \boldsymbol{j} - \boldsymbol{k}, 2\boldsymbol{k}, 1 + \boldsymbol{i} + \boldsymbol{j} - \boldsymbol{k}\,]$$

It is easy to observe that $\|\boldsymbol{X}_0^L\| = \|\boldsymbol{X}_1^L\| = \|\boldsymbol{X}_2^L\| = \|\boldsymbol{X}_3^L\| = 4$ and $\|\boldsymbol{X}_0^R\| = \|\boldsymbol{X}_1^R\| = \|\boldsymbol{X}_2^R\| = \|\boldsymbol{X}_3^R\| = 4$.

So, the property of having the left and right discrete Fourier transform coefficients of equal norm is not sufficient for perfection over the quaternions.

However, as shown below, the condition of having all discrete Fourier transform coefficients of equal norm is necessary for perfection over the quaternions. The main result of this section is contained in the following statement:

Proposition 9.3 Let $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ be a perfect sequence over the real quaternions. Then, for $0 \le s \le n-1$,

$$\|\boldsymbol{A}_s^L\| = \|\boldsymbol{A}_s^R\| = \|\boldsymbol{a}\|$$

where $\boldsymbol{A}_s^L = \sum_{t=0}^{n-1} e^{-\frac{2\pi i}{n}st}\boldsymbol{a}_t$ and $\boldsymbol{A}_s^R = \sum_{t=0}^{n-1} \boldsymbol{a}_t e^{-\frac{2\pi i}{n}st}$ denote the s-th left and right discrete Fourier transform coefficients respectively.

Before we proceed with the proof, we need to make some remarks, illustrating that the statement of Proposition 9.3 is not trivial.

<u>Remark 9.2</u> For an arbitrary sequence $\boldsymbol{x}$ over the real quaternions, the norms of all the discrete Fourier transform coefficients are not necessarily equal. That is, there exist quaternionic sequences, whose discrete Fourier transform coefficients are of non-equal norm. Consider the simple Example 9.5.

<u>Example 9.5</u> The discrete Fourier transforms of the non-perfect sequence $\boldsymbol{x} = [\,1, 1, 1, \boldsymbol{k}\,]$ with all elements of norm 1 from Example 9.2 are as follow:

$$\boldsymbol{X}^L = DFT^L([\,1, 1, 1, \boldsymbol{k}\,]) = [\,3 + \boldsymbol{k}, -\boldsymbol{i} - \boldsymbol{j}, 1 - \boldsymbol{k}, \boldsymbol{i} + \boldsymbol{j}\,]$$

$$\boldsymbol{X}^R = DFT^R([\,1, 1, 1, \boldsymbol{k}\,]) = [\,3 + \boldsymbol{k}, -\boldsymbol{i} + \boldsymbol{j}, 1 - \boldsymbol{k}, \boldsymbol{i} - \boldsymbol{j}\,]$$

It is easy to observe that

$$10 = \|\boldsymbol{X}_0^L\| = \|\boldsymbol{X}_0^R\| \neq \|\boldsymbol{x}\| = 4$$

$$2 = \|\boldsymbol{X}_1^L\| = \|\boldsymbol{X}_1^R\| \neq \|\boldsymbol{x}\| = 4$$

$$2 = \|\boldsymbol{X}_2^L\| = \|\boldsymbol{X}_2^R\| \neq \|\boldsymbol{x}\| = 4$$

$$2 = \|\boldsymbol{X}_3^L\| = \|\boldsymbol{X}_3^R\| \neq \|\boldsymbol{x}\| = 4$$

<u>Remark 9.3</u> Since the sequence $\omega(\boldsymbol{a}) = [\omega^0\boldsymbol{a_0}, \omega^1\boldsymbol{a_1}, \dots, \omega^{n-1}\boldsymbol{a_{n-1}}]$, where $\omega = e^{\frac{2\pi s\boldsymbol{i}}{n}}$ is an n-th complex root of unity, $1 \le s \le n-1$, is not, in general, perfect for an arbitrary perfect sequence $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ over the real quaternions (refer to Example 6.1), Proposition 9.3 is not a simple consequence of the Balance Theorem (Proposition 8.1) for the sequence $\omega(\boldsymbol{a})$.

<u>Remark 9.4</u> The proof of Proposition 4.1, stating that the condition of having all discrete Fourier transform coefficients of equal norm is necessary and sufficient for perfection over the complex numbers, relies on the commutative law for the complex numbers. Due to the non-commutative nature of the quaternions, this proof cannot be adopted here. Use of commutative law is avoided in the proof of Proposition 9.3, to be presented in this section.

Before proceeding with a proof of Proposition 9.3, some important properties of the real quaternions and sequences over the real quaternions need to be discussed.

9.3. Alternative Definition of Perfection

In the next few paragraphs an alternative definition of a perfect sequence will be given.

Consider the $n \times n$ matrix with entries 0 and 1:

$$C = \begin{bmatrix} 0 & 1 & 0 & \dots & \dots & 0 \\ 0 & 0 & 1 & & & \vdots \\ \vdots & 0 & 0 & \ddots & & \vdots \\ \vdots & & 0 & \ddots & 1 & 0 \\ 0 & & & \ddots & 0 & 1 \\ 1 & 0 & \dots & \dots & 0 & 0 \end{bmatrix}$$

Matrix C has $(n-1)$ 1's in the positions just above the main diagonal and one 1 in the bottom left corner; all other entries are zero. It is a *permutation matrix*, meaning that its columns are a permutation of columns of the identity matrix I.

If we consider a sequence $\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-1}]$ as a column vector $\boldsymbol{x}^T = \begin{bmatrix} \boldsymbol{x}_0 \\ \boldsymbol{x}_1 \\ \vdots \\ \boldsymbol{x}_{n-1} \end{bmatrix}$, then the product of matrix C and column vector $\boldsymbol{x}^T$ will be another column vector corresponding to the shift of the original sequence $\boldsymbol{x}$ by 1: $C\boldsymbol{x}^T = \begin{bmatrix} \boldsymbol{x}_1 \\ \boldsymbol{x}_2 \\ \vdots \\ \boldsymbol{x}_0 \end{bmatrix}$.

It is obvious the multiplication of the sequence column vector $\boldsymbol{x}^T$ by the consecutive powers of C from the left give consecutive cyclic shifts of the sequence. Thus, all shifts of the original sequence $\boldsymbol{x}$ can be expressed by the multiplication of the vector $\boldsymbol{x}^T$ by the corresponding powers of the matrix C from the left: $C^m\boldsymbol{x}^T = \begin{bmatrix} \boldsymbol{x}_m \\ \boldsymbol{x}_{m+1} \\ \vdots \\ \boldsymbol{x}_{m-1} \end{bmatrix}$. Raising C to the n-th power will give the identity matrix I, $C^n = I$. Therefore, the product of matrix C^n and vector $\boldsymbol{x}^T$ is equal to the original vector $\boldsymbol{x}^T$, which represents the original sequence $\boldsymbol{x}$.

Consider the left autocorrelation function of a sequence $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{n-1}]$ over $\mathbb{H}$,

$ACF_{\boldsymbol{a}}^L(m) = \frac{1}{\|x\|}\sum_{t=0}^{n-1} \boldsymbol{a}_t^* \boldsymbol{a}_{t+m}$. By definition, $\boldsymbol{a}$ is a perfect sequence if and only if $ACF_{\boldsymbol{a}}^L(m) = 0$ for all non zero shifts m, $1 \le m \le n-1$. Recall (Section 3.10 of the present work) that the inner product of two vectors $\boldsymbol{x}^T = \begin{bmatrix} \boldsymbol{x}_0 \\ \boldsymbol{x}_1 \\ \vdots \\ \boldsymbol{x}_{n-1} \end{bmatrix}$ and $\boldsymbol{y}^T = \begin{bmatrix} \boldsymbol{y}_0 \\ \boldsymbol{y}_1 \\ \vdots \\ \boldsymbol{y}_{n-1} \end{bmatrix}$ from $\mathbb{H}^n$ is defined by $\langle \boldsymbol{x}^T, \boldsymbol{y}^T \rangle = \sum_{t=0}^{n-1} \boldsymbol{x}_t^* \boldsymbol{y}_t$.

Since any shift of a sequence can be represented as the product of the respective power of matrix C and the column vector corresponding to this sequence, it can be stated that sequence $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ over the real quaternions is (left) perfect if and only if $\langle \boldsymbol{a}^T, C^m \boldsymbol{a}^T \rangle = 0$ for every integer m, $1 \leq m \leq n-1$.

Therefore, the set of equations

$$\langle \boldsymbol{a}^T, C^m \boldsymbol{a}^T \rangle = 0, \qquad 1 \leq t \leq n-1 \tag{9.1}$$

can be regarded as an alternative set of defining equations for a (left) perfect sequence. Therefore, the problem of finding a (left) perfect sequence is equivalent to finding a solution of the equations (9.1).

Thus, we have come to an alternative definition for (left) perfection. A sequence $\boldsymbol{a}$ over the real quaternions is (left) perfect if and only if equations (9.1) hold.

9.4. Diagonalization of Matrix C

It is easy to see that matrix

$$C = \begin{bmatrix} 0 & 1 & 0 & \dots & \dots & 0 \\ 0 & 0 & 1 & & & \vdots \\ \vdots & 0 & 0 & \ddots & & \vdots \\ \vdots & & 0 & \ddots & 1 & 0 \\ 0 & & & \ddots & 0 & 1 \\ 1 & 0 & \dots & \dots & 0 & 0 \end{bmatrix}$$

is a unitary matrix, therefore normal (refer to Section 3.8, Definition 3.8, for definitions of normal and unitary matrices). Properties of matrices over the real quaternions have been briefly discussed in Section 3.9.1 of the present work. It is known (Lee [59]) that every normal matrix over the real quaternions can be transformed into the diagonal form by a similarity transformation. That is, if $\boldsymbol{Q}$ is a normal matrix over the real quaternions then there exists a unitary matrix $\boldsymbol{U}$ such that $\boldsymbol{D} = \boldsymbol{U}^{\dagger}\boldsymbol{Q}\boldsymbol{U}$, where $\boldsymbol{D}$ is a diagonal matrix. Moreover, each diagonal element of $\boldsymbol{D}$ is some right eigenvalue of $\boldsymbol{Q}$ (Farenick and Pidkowich [30]). Therefore, the problem of finding a diagonal form for a given matrix with real quaternion entries is equivalent to the problem of finding its right eigenvalues.

It is known that a quaternion matrix may have infinitely many right eigenvalues. In fact, if $\boldsymbol{q}$ is an eigenvalue of a matrix $\boldsymbol{Q}$ with quaternion entries then every $\boldsymbol{x} \in [\boldsymbol{q}]$, where $[\boldsymbol{q}]$ denotes the similarity class containing $\boldsymbol{q}$, is an eigenvalue too. However, the number of similarity classes is not unbounded for the given matrix $\boldsymbol{Q}$. It has been proved (Farenick and Pidkowich [30]) that the number of distinct similarity classes of right eigenvalues of an arbitrary $n \times n$ quaternion matrix $\boldsymbol{Q}$ does not exceed n.

We now transform matrix C into a diagonal form. Calculating eigenvalues of an arbitrary quaternion matrix is not a simple task. However, because matrix C contains only 0 and 1 as its entries, we can regard C as a matrix over the complex field $\mathbb{C}$. A complex matrix is diagonalizable over $\mathbb{H}$ if and only if it is diagonalizable over $\mathbb{C}$ (Zhang [98], Corollary 7.2). If matrix C is transformed into a diagonal form $\boldsymbol{D}$ by a similarity transformation over the complex field $\mathbb{C}$, then every quaternion similar to a diagonal entry of $\boldsymbol{D}$ is an eigenvalue of matrix C, if C is regarded as a matrix over the real quaternion algebra $\mathbb{H}$ (refer to Section 3.6 for brief explanation of quaternion similarity). Every diagonal matrix obtained from $\boldsymbol{D}$ by substitution of any main diagonal entry by a similar quaternion will be another diagonal form of matrix C over $\mathbb{H}$.

So, by considering C as a matrix with complex entries, we transfer the problem of finding its eigenvalues into the domain of complex algebra. A task of matrix diagonalization over the complex field $\mathbb{C}$ belongs to the well studied area of commutative linear algebra. In particular, it is known (Byron and Fuller [15], Theorem 4.23) that normal matrices over the complex field $\mathbb{C}$ are diagonalizable by unitary similarity transformations, and their diagonal forms contain complex valued eigenvalues on the main diagonal (Hungerford [48], Theorem 5.5). Moreover, columns of the unitary matrix U, which diagonalizes the normal matrix Q by the similarity transformation, are eigenvectors of Q (Mirsky [67], Theorem 10.2.1).

Throughout this work bold fonts are reserved for quaternions, sequences, vectors and matrices over quaternions. All matrices considered in the two lemmas that follow are regarded as matrices over the complex field $\mathbb{C}$, so we do not use bold fonts when writing their notations.

In linear algebra, the equation $\det(M - \lambda I) = 0$ in the single variable λ is called a *characteristic equation* of a square matrix M. Eigenvalues of M are roots of the characteristic equation. The task of finding a diagonal form of matrix M is therefore reduced to the task of finding roots of its characteristic equation.

Lemma 9.1 $\lambda^n - 1 = 0$ is the characteristic equation of the $n \times n$ matrix

$$C = \begin{bmatrix} 0 & 1 & 0 & \dots & \dots & 0 \\ 0 & 0 & 1 & & & \vdots \\ \vdots & 0 & 0 & \ddots & & \vdots \\ \vdots & & 0 & \ddots & 1 & 0 \\ 0 & & & \ddots & 0 & 1 \\ 1 & 0 & \dots & \dots & 0 & 0 \end{bmatrix}$$

Proof. Since $\det(M^T) = \det(M)$ (Barnett [8]), we have

$$0 = \det(C - \lambda I) = \begin{vmatrix} -\lambda & 1 & 0 & \dots & \dots & 0 \\ 0 & -\lambda & 1 & & & \vdots \\ \vdots & & -\lambda & \ddots & & \vdots \\ \vdots & & & \ddots & 1 & 0 \\ 0 & & & & -\lambda & 1 \\ 1 & 0 & \dots & \dots & 0 & -\lambda \end{vmatrix} = \left| \begin{bmatrix} -\lambda & 1 & 0 & \dots & \dots & 0 \\ 0 & -\lambda & 1 & & & \vdots \\ \vdots & & -\lambda & \ddots & & \vdots \\ \vdots & & & \ddots & 1 & 0 \\ 0 & & & & -\lambda & 1 \\ 1 & 0 & \dots & \dots & 0 & -\lambda \end{bmatrix}^T \right|$$

$$= \begin{vmatrix} -\lambda & 0 & 0 & \dots & 0 & 1 \\ 1 & -\lambda & 0 & & & 0 \\ 0 & 1 & -\lambda & \ddots & & \vdots \\ \vdots & & 1 & \ddots & 0 & 0 \\ \vdots & & & \ddots & -\lambda & 0 \\ 0 & \dots & \dots & 0 & 1 & -\lambda \end{vmatrix}$$

We now expand the last determinant by minors along the first row using the Laplace expansion formula $|A| = \sum_{s=0}^{n-1} (-1)^{s+t} \, a_{st} M_{st}$, where M_{st} is a minor obtained from matrix A by removal of row s and column t (refer to Horn and Johnson [44]).

$$= (-1)^{0+0}(-\lambda)\begin{vmatrix} -\lambda & 0 & \dots & 0 \\ 1 & -\lambda & & \vdots \\ & \ddots & \ddots & 0 \\ 0 & & 1 & -\lambda \end{vmatrix}_{(n-1)\times(n-1)} + (-1)^{0+n-1}\begin{vmatrix} 1 & -\lambda & & 0 \\ 0 & 1 & \ddots & \\ \vdots & & \ddots & -\lambda \\ 0 & \dots & 0 & 1 \end{vmatrix}_{(n-1)\times(n-1)}$$

$$= (-\lambda)\begin{vmatrix} -\lambda & 0 & \dots & 0 \\ 1 & -\lambda & & \vdots \\ & \ddots & \ddots & 0 \\ 0 & & 1 & -\lambda \end{vmatrix}_{(n-1)\times(n-1)} + (-1)^{n-1}\begin{vmatrix} 1 & -\lambda & & 0 \\ 0 & 1 & \ddots & \\ \vdots & & \ddots & -\lambda \\ 0 & \dots & 0 & 1 \end{vmatrix}_{(n-1)\times(n-1)}$$

The determinant of a triangular matrix is equal to the product of all diagonal elements (Barnett [8]), therefore

$$= (-\lambda)(-\lambda)^{n-1} + (-1)^{n-1} = (-\lambda)^n + (-1)^{n-1}$$

If n is an even number then $0 = (-\lambda)^n + (-1)^{n-1} = \lambda^n - 1$. If n is an odd number then $0 = (-\lambda)^n + (-1)^{n-1} = -\lambda^n + 1$. In both cases we can write the characteristic equation of the matrix C in the form $\lambda^n - 1 = 0$. □

Lemma 9.2 Let $\omega = e^{\frac{2\pi i}{n}}$ be the principal n-th root of unity. Then the unitary matrix

$$U = \frac{1}{\sqrt{n}}\begin{bmatrix} \omega^0 & \omega^0 & \omega^0 & \dots & \omega^0 & \omega^0 \\ \omega^0 & \omega^1 & \omega^2 & \dots & \omega^{n-2} & \omega^{n-1} \\ \omega^0 & \omega^2 & \omega^4 & \dots & \omega^{n-4} & \omega^{n-2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \omega^0 & \omega^{n-2} & \omega^{n-4} & \dots & \omega^4 & \omega^2 \\ \omega^0 & \omega^{n-1} & \omega^{n-2} & \dots & \omega^2 & \omega^1 \end{bmatrix}$$ transforms the $n \times n$ matrix

$$C = \begin{bmatrix} 0 & 1 & 0 & \dots & \dots & 0 \\ 0 & 0 & 1 & & & \vdots \\ \vdots & 0 & 0 & \ddots & & \vdots \\ \vdots & & 0 & \ddots & 1 & 0 \\ 0 & & & \ddots & 0 & 1 \\ 1 & 0 & \dots & \dots & 0 & 0 \end{bmatrix}$$ into diagonal form $$D = \begin{bmatrix} \omega^0 & 0 & \dots & 0 \\ 0 & \omega^1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & \omega^{n-1} \end{bmatrix}$$ by the similarity transformation $D = U^{\dagger}CU$.

Proof. In the light of Lemma 9.1, the *spectrum* (that is, the set of all eigenvalues) of matrix C coincides with the set of all n-th roots of unity $\{\omega^0, \omega^1, \omega^2, \dots, \omega^{n-1}\}$. Therefore, the main diagonal entries of a diagonal form of matrix C represent some permutation of the set of all n-th roots of unity. In fact, every permutation of the eigenvalues on the main diagonal gives a diagonal form of matrix C. We pick up one of the available diagonal forms of the matrix C, as follows

$$D = \mathrm{diag}(\omega^0, \omega^1, \dots, \omega^{n-1}) = \begin{bmatrix} \omega^0 & 0 & \dots & 0 \\ 0 & \omega^1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & \omega^{n-1} \end{bmatrix}$$

It is known (Mirsky [67], Theorem 10.2.1) that a unitary matrix U, which diagonalizes matrix C, contains eigenvectors of the matrix C as its columns. Therefore, in order to find U, we need to find eigenvectors of C.

Since we consider C as a matrix over the complex field $\mathbb{C}$, an eigenvector ξ of the matrix C corresponding to the eigenvalue λ satisfies the equation $C\xi = \lambda\xi$. We expand and solve this equation for ξ:

$$\begin{bmatrix} 0 & 1 & 0 & \dots & \dots & 0 \\ 0 & 0 & 1 & & & \vdots \\ \vdots & 0 & 0 & \ddots & & \vdots \\ \vdots & & 0 & \ddots & 1 & 0 \\ 0 & & & \ddots & 0 & 1 \\ 1 & 0 & \dots & \dots & 0 & 0 \end{bmatrix} \begin{bmatrix} \xi_0 \\ \xi_1 \\ \xi_2 \\ \vdots \\ \xi_{n-2} \\ \xi_{n-1} \end{bmatrix} = \lambda \begin{bmatrix} \xi_0 \\ \xi_1 \\ \xi_2 \\ \vdots \\ \xi_{n-2} \\ \xi_{n-1} \end{bmatrix} \Leftrightarrow$$

$$\begin{bmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \\ \vdots \\ \xi_{n-1} \\ \xi_0 \end{bmatrix} = \begin{bmatrix} \lambda\xi_0 \\ \lambda\xi_1 \\ \lambda\xi_2 \\ \vdots \\ \lambda\xi_{n-2} \\ \lambda\xi_{n-1} \end{bmatrix} \Leftrightarrow$$

$$\begin{cases} \xi_1 = \lambda\xi_0 \\ \xi_2 = \lambda\xi_1 \\ \xi_3 = \lambda\xi_2 \\ \quad \dots \\ \xi_{n-1} = \lambda\xi_{n-2} \\ \xi_0 = \lambda\xi_{n-1} \end{cases} \Leftrightarrow$$

$$\begin{cases} \xi_1 = \lambda\xi_0 \\ \xi_2 = \lambda^2\xi_0 \\ \xi_3 = \lambda^3\xi_0 \\ \quad\cdots \\ \xi_{n-1} = \lambda^{n-1}\xi_0 \\ \xi_0 = \lambda^n\xi_0 \end{cases}$$

The last set of equations is consistent if and only if $\lambda^n = 1$, that is, when λ is an n-th root of unity.

If we consider ξ_0 as an independent variable $\xi_0 = c$, then the solutions of the system above, the eigenvectors of the matrix C, can be written as $\xi_\lambda = \begin{bmatrix} c \\ \lambda c \\ \lambda^2 c \\ \vdots \\ \lambda^{n-2} c \\ \lambda^{n-1} c \end{bmatrix} = c\begin{bmatrix} \lambda^0 \\ \lambda^1 \\ \lambda^2 \\ \vdots \\ \lambda^{n-2} \\ \lambda^{n-1} \end{bmatrix}$.

We now construct the matrix U, consisting of eigenvectors ξ_λ:

$$U = [\xi_{\omega^0}, \xi_{\omega^1}, \dots, \xi_{\omega^{n-1}}] = c\begin{bmatrix} \omega^0 & \omega^0 & \omega^0 & \dots & \omega^0 & \omega^0 \\ \omega^0 & \omega^1 & \omega^2 & \dots & \omega^{n-2} & \omega^{n-1} \\ \omega^0 & \omega^2 & \omega^4 & \dots & \omega^{2(n-2)} & \omega^{2(n-1)} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \omega^0 & \omega^{n-2} & \omega^{(n-2)\cdot 2} & \dots & \omega^{(n-2)(n-2)} & \omega^{(n-2)(n-1)} \\ \omega^0 & \omega^{n-1} & \omega^{(n-1)\cdot 2} & \dots & \omega^{(n-1)(n-2)} & \omega^{(n-1)(n-1)} \end{bmatrix}$$

$$= c\begin{bmatrix} \omega^0 & \omega^0 & \omega^0 & \dots & \omega^0 & \omega^0 \\ \omega^0 & \omega^1 & \omega^2 & \dots & \omega^{n-2} & \omega^{n-1} \\ \omega^0 & \omega^2 & \omega^4 & \dots & \omega^{n-4} & \omega^{n-2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \omega^0 & \omega^{n-2} & \omega^{n-4} & \dots & \omega^4 & \omega^2 \\ \omega^0 & \omega^{n-1} & \omega^{n-2} & \dots & \omega^2 & \omega^1 \end{bmatrix}$$

Note that matrix U is *symmetric*, $U = U^T$, and therefore $U^\dagger = U^*$.

If ω^t is an n-th root of unity then its conjugate $\overline{\omega^t} = \omega^{n-t}$. Therefore,

$$U^{\dagger} = U^{*} = c\begin{bmatrix} \omega^0 & \omega^0 & \omega^0 & \dots & \omega^0 & \omega^0 \\ \omega^0 & \omega^1 & \omega^2 & \dots & \omega^{n-2} & \omega^{n-1} \\ \omega^0 & \omega^2 & \omega^4 & \dots & \omega^{n-4} & \omega^{n-2} \\ & \cdots & \cdots & \cdots\cdots & \cdots & \\ \omega^0 & \omega^{n-2} & \omega^{n-4} & \dots & \omega^4 & \omega^2 \\ \omega^0 & \omega^{n-1} & \omega^{n-2} & \dots & \omega^2 & \omega^1 \end{bmatrix}^{*}$$

$$= c\begin{bmatrix} \omega^0 & \omega^0 & \omega^0 & \dots & \omega^0 & \omega^0 \\ \omega^0 & \omega^{n-1} & \omega^{n-2} & \dots & \omega^2 & \omega^1 \\ \omega^0 & \omega^{n-2} & \omega^{n-4} & \dots & \omega^4 & \omega^2 \\ & \cdots & \cdots & \cdots\cdots & \cdots & \\ \omega^0 & \omega^2 & \omega^4 & \dots & \omega^{n-4} & \omega^{n-2} \\ \omega^0 & \omega^1 & \omega^2 & \dots & \omega^{n-2} & \omega^{n-1} \end{bmatrix}$$

By direct calculation, we have

$$U^{\dagger}U = U^{*}U =$$

$$= c\begin{bmatrix} \omega^0 & \omega^0 & \omega^0 & \dots & \omega^0 & \omega^0 \\ \omega^0 & \omega^{n-1} & \omega^{n-2} & \dots & \omega^2 & \omega^1 \\ \omega^0 & \omega^{n-2} & \omega^{n-4} & \dots & \omega^4 & \omega^2 \\ & \cdots & \cdots & \cdots\cdots & \cdots & \\ \omega^0 & \omega^2 & \omega^4 & \dots & \omega^{n-4} & \omega^{n-2} \\ \omega^0 & \omega^1 & \omega^2 & \dots & \omega^{n-2} & \omega^{n-1} \end{bmatrix} \cdot c\begin{bmatrix} \omega^0 & \omega^0 & \omega^0 & \dots & \omega^0 & \omega^0 \\ \omega^0 & \omega^1 & \omega^2 & \dots & \omega^{n-2} & \omega^{n-1} \\ \omega^0 & \omega^2 & \omega^4 & \dots & \omega^{n-4} & \omega^{n-2} \\ & \cdots & \cdots & \cdots\cdots & \cdots & \\ \omega^0 & \omega^{n-2} & \omega^{n-4} & \dots & \omega^4 & \omega^2 \\ \omega^0 & \omega^{n-1} & \omega^{n-2} & \dots & \omega^2 & \omega^1 \end{bmatrix}$$

The main diagonal elements of the product of two matrices above are, in fact, the sums of terms of the form $\omega^{n-t} \cdot \omega^{t} = 1$, each taken n times, and therefore equal to n. Elements off the main diagonal represent the sums of all m-th roots of unity $\omega^{m} = \omega^{n-t} \cdot \omega^{t+m}$, for m a divisor of n, and therefore equal to zero.

$$= c^2\begin{bmatrix} n & & & 0 \\ & n & & \\ & & \ddots & \\ 0 & & & n \end{bmatrix} = c^2 n$$

Choosing the normalizing factor $c = \frac{1}{\sqrt{n}}$ brings the above equation to the form $U^{\dagger}U = I$ and matrix U becomes unitary. This completes the proof of Lemma 9.2 □

The following lemmas involve matrices over the quaternions, so bold fonts are used.

Lemma 9.3 If a unitary matrix $\boldsymbol{U}$ over the real quaternions diagonalizes an $n \times n$ matrix $\boldsymbol{M}$ over the real quaternions by similarly transformation, i.e. $\boldsymbol{D} = \boldsymbol{U}^{\dagger}\boldsymbol{M}\boldsymbol{U}$, where $\boldsymbol{D}$ is a diagonal matrix, then $\boldsymbol{U}$ diagonalizes $\boldsymbol{M}^m$ for every positive integer m; moreover, $\boldsymbol{D}^m$ is a diagonal form of the matrix $\boldsymbol{M}^m$.

Proof.

$$\boldsymbol{D}^m = (\boldsymbol{U}^{\dagger}\boldsymbol{M}\boldsymbol{U})^m = \underbrace{(\boldsymbol{U}^{\dagger}\boldsymbol{M}\boldsymbol{U})(\boldsymbol{U}^{\dagger}\boldsymbol{M}\boldsymbol{U}) \dots (\boldsymbol{U}^{\dagger}\boldsymbol{M}\boldsymbol{U})}_{m\ times} = \boldsymbol{U}^{\dagger}\, \underbrace{\boldsymbol{M}(\boldsymbol{U}\boldsymbol{U}^{\dagger})\boldsymbol{M} \dots \boldsymbol{M}(\boldsymbol{U}\boldsymbol{U}^{\dagger})\boldsymbol{M}}_{m\ times}\, \boldsymbol{U} =$$

$$\boldsymbol{U}^{\dagger}\, \underbrace{\boldsymbol{M}\boldsymbol{I}\boldsymbol{M} \dots \boldsymbol{M}\boldsymbol{I}\boldsymbol{M}}_{m\ times}\, \boldsymbol{U} = \boldsymbol{U}^{\dagger}\boldsymbol{M}^m\boldsymbol{U}. \square$$

Lemma 9.4 Let $\boldsymbol{U}$ be an $n \times n$ matrix over the real quaternions and $\boldsymbol{x}^T$ be any column vector over the real quaternions. Then $\langle \boldsymbol{x}^T, \boldsymbol{U}\boldsymbol{x}^T \rangle = \langle \boldsymbol{U}^{\dagger}\boldsymbol{x}^T, \boldsymbol{x}^T \rangle$.

Proof. If we denote the s-row t-column entry of the matrix $\boldsymbol{U}$ by $[\boldsymbol{U}]_{st} = \boldsymbol{u}_{st},\ s, t = 0, \dots, n-1$ then we have

$$\langle \boldsymbol{U}^{\dagger}\boldsymbol{x}^T, \boldsymbol{x}^T \rangle = [\boldsymbol{U}^{\dagger}\boldsymbol{x}^T]_0^*\boldsymbol{x}_0 + [\boldsymbol{U}^{\dagger}\boldsymbol{x}^T]_1^*\boldsymbol{x}_1 + \cdots + [\boldsymbol{U}^{\dagger}\boldsymbol{x}^T]_{n-1}^*\boldsymbol{x}_{n-1}$$

$$= (\boldsymbol{u}_{00}^*\boldsymbol{x}_0 + \boldsymbol{u}_{10}^*\boldsymbol{x}_1 + \cdots + \boldsymbol{u}_{n-1,0}^*\boldsymbol{x}_{n-1})^*\boldsymbol{x}_0 + (\boldsymbol{u}_{01}^*\boldsymbol{x}_0 + \boldsymbol{u}_{11}^*\boldsymbol{x}_1 + \cdots + \boldsymbol{u}_{n-1,1}^*\boldsymbol{x}_{n-1})^*\boldsymbol{x}_1 + \cdots$$
$$+ (\boldsymbol{u}_{0,n-1}^*\boldsymbol{x}_0 + \boldsymbol{u}_{1,n-1}^*\boldsymbol{x}_1 + \cdots + \boldsymbol{u}_{n-1,n-1}^*\boldsymbol{x}_{n-1})^*\boldsymbol{x}_{n-1}$$

$$= (\boldsymbol{x}_0^*\boldsymbol{u}_{00} + \boldsymbol{x}_1^*\boldsymbol{u}_{10} + \cdots + \boldsymbol{x}_{n-1}^*\boldsymbol{u}_{n-1,0})\boldsymbol{x}_0 + (\boldsymbol{x}_0^*\boldsymbol{u}_{01} + \boldsymbol{x}_1^*\boldsymbol{u}_{11} + \cdots + \boldsymbol{x}_{n-1}^*\boldsymbol{u}_{n-1,1})\boldsymbol{x}_1 + \cdots$$
$$+ (\boldsymbol{x}_0^*\boldsymbol{u}_{0,n-1} + \boldsymbol{x}_1^*\boldsymbol{u}_{1,n-1} + \cdots + \boldsymbol{x}_{n-1}^*\boldsymbol{u}_{n-1,n-1})\boldsymbol{x}_{n-1}$$

$$= \boldsymbol{x}_0^*\boldsymbol{u}_{00}\boldsymbol{x}_0 + \boldsymbol{x}_1^*\boldsymbol{u}_{10}\boldsymbol{x}_0 + \cdots + \boldsymbol{x}_{n-1}^*\boldsymbol{u}_{n-1,0}\boldsymbol{x}_0 + \boldsymbol{x}_0^*\boldsymbol{u}_{01}\boldsymbol{x}_1 + \boldsymbol{x}_1^*\boldsymbol{u}_{11}\boldsymbol{x}_1 + \cdots + \boldsymbol{x}_{n-1}^*\boldsymbol{u}_{n-1,1}\boldsymbol{x}_1 + \cdots$$
$$+ \boldsymbol{x}_0^*\boldsymbol{u}_{0,n-1}\boldsymbol{x}_{n-1} + \boldsymbol{x}_1^*\boldsymbol{u}_{1,n-1}\boldsymbol{x}_{n-1} + \cdots + \boldsymbol{x}_{n-1}^*\boldsymbol{u}_{n-1,n-1}\boldsymbol{x}_{n-1}$$

$$= \boldsymbol{x}_0^*\left(\boldsymbol{u}_{00}\boldsymbol{x}_0 + \boldsymbol{u}_{01}\boldsymbol{x}_1 + \cdots + \boldsymbol{u}_{0,n-1}\boldsymbol{x}_{n-1}\right) + \boldsymbol{x}_1^*\left(\boldsymbol{u}_{10}\boldsymbol{x}_0 + \boldsymbol{u}_{11}\boldsymbol{x}_1 + \cdots + \boldsymbol{u}_{1,n-1}\boldsymbol{x}_{n-1}\right) + \cdots$$
$$+ \boldsymbol{x}_{n-1}^*\left(\boldsymbol{u}_{n-1,0}\boldsymbol{x}_0 + \boldsymbol{u}_{n-1,1}\boldsymbol{x}_1 + \cdots + \boldsymbol{u}_{n-1,n-1}\boldsymbol{x}_{n-1}\right)$$

$$= \boldsymbol{x}_0^*[\boldsymbol{U}\boldsymbol{x}^T]_0 + \boldsymbol{x}_1^*[\boldsymbol{U}\boldsymbol{x}^T]_1 + \cdots + \boldsymbol{x}_{n-1}^*[\boldsymbol{U}\boldsymbol{x}^T]_{n-1}$$

$$= \langle \boldsymbol{x}^T, \boldsymbol{U}\boldsymbol{x}^T \rangle. \square$$

9.5. Additional Results Required for Proof of the Main Result

A few lemmas, used in the proof of Proposition 9.3, are presented in this part.

Lemma 9.5 Let $t_1$and t_2 be two integers such that $0 \leq t_1, t_2 \leq n-1$, $t_1 \neq t_2$ and $t_1 + t_2 \neq n$. Then rows t_1 and t_2 of the $n \times n$ matrix

$$R_{cos} = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & \cos\frac{2\pi\cdot 1\cdot 1}{n} & \cos\frac{2\pi\cdot 1\cdot 2}{n} & \dots & \cos\frac{2\pi\cdot 1\cdot(n-2)}{n} & \cos\frac{2\pi\cdot 1\cdot(n-1)}{n} \\ 1 & \cos\frac{2\pi\cdot 2\cdot 1}{n} & \cos\frac{2\pi\cdot 2\cdot 2}{n} & \dots & \cos\frac{2\pi\cdot 2\cdot(n-2)}{n} & \cos\frac{2\pi\cdot 2\cdot(n-1)}{n} \\ & \dots & \dots & \dots & \dots & \dots \\ 1 & \cos\frac{2\pi\cdot(n-2)\cdot 1}{n} & \cos\frac{2\pi\cdot(n-2)\cdot 2}{n} & \dots & \cos\frac{2\pi\cdot(n-2)\cdot(n-2)}{n} & \cos\frac{2\pi\cdot(n-2)\cdot(n-1)}{n} \\ 1 & \cos\frac{2\pi\cdot(n-1)\cdot 1}{n} & \cos\frac{2\pi\cdot(n-1)\cdot 2}{n} & \dots & \cos\frac{2\pi\cdot(n-1)\cdot(n-2)}{n} & \cos\frac{2\pi\cdot(n-1)\cdot(n-1)}{n} \end{bmatrix}$$

over the real numbers are orthogonal in respect to the Euclidian inner product

$\langle x, y\rangle_{\mathbb{R}} = \sum_{t=0}^{n-1} x_t y_t$.

Proof. Express matrix R_{cos} as follows:

$$R_{cos} = \begin{bmatrix} \cos\frac{2\pi\cdot 0\cdot 0}{n} & \cos\frac{2\pi\cdot 0\cdot 1}{n} & \cos\frac{2\pi\cdot 0\cdot 2}{n} & \dots & \cos\frac{2\pi\cdot 0\cdot(n-2)}{n} & \cos\frac{2\pi\cdot 0\cdot(n-1)}{n} \\ \cos\frac{2\pi\cdot 1\cdot 0}{n} & \cos\frac{2\pi\cdot 1\cdot 1}{n} & \cos\frac{2\pi\cdot 1\cdot 2}{n} & \dots & \cos\frac{2\pi\cdot 1\cdot(n-2)}{n} & \cos\frac{2\pi\cdot 1\cdot(n-1)}{n} \\ \cos\frac{2\pi\cdot 2\cdot 0}{n} & \cos\frac{2\pi\cdot 2\cdot 1}{n} & \cos\frac{2\pi\cdot 2\cdot 2}{n} & \dots & \cos\frac{2\pi\cdot 2\cdot(n-2)}{n} & \cos\frac{2\pi\cdot 2\cdot(n-1)}{n} \\ & \dots & \dots & \dots & \dots & \dots \\ \cos\frac{2\pi\cdot(n-2)\cdot 0}{n} & \cos\frac{2\pi\cdot(n-2)\cdot 1}{n} & \cos\frac{2\pi\cdot(n-2)\cdot 2}{n} & \dots & \cos\frac{2\pi\cdot(n-2)\cdot(n-2)}{n} & \cos\frac{2\pi\cdot(n-2)\cdot(n-1)}{n} \\ \cos\frac{2\pi\cdot(n-1)\cdot 0}{n} & \cos\frac{2\pi\cdot(n-1)\cdot 1}{n} & \cos\frac{2\pi\cdot(n-1)\cdot 2}{n} & \dots & \cos\frac{2\pi\cdot(n-1)\cdot(n-2)}{n} & \cos\frac{2\pi\cdot(n-1)\cdot(n-1)}{n} \end{bmatrix}$$

Let t_1 and t_2 be two integers satisfying the conditions of Lemma 9.5. We will show that the inner product of rows t_1 and t_2 is equal to zero.

$$\left\langle\left[\cos\frac{2\pi\cdot t_1\cdot 0}{n},\cos\frac{2\pi\cdot t_1\cdot 1}{n},\dots,\cos\frac{2\pi\cdot t_1\cdot(n-1)}{n}\right],\left[\cos\frac{2\pi\cdot t_2\cdot 0}{n},\cos\frac{2\pi\cdot t_2\cdot 1}{n},\dots,\cos\frac{2\pi\cdot t_2\cdot(n-1)}{n}\right]\right\rangle_{\mathbb{R}} =$$

$$\cos\frac{2\pi\cdot t_1\cdot 0}{n}\cos\frac{2\pi\cdot t_2\cdot 0}{n}+\cos\frac{2\pi\cdot t_1\cdot 1}{n}\cos\frac{2\pi\cdot t_2\cdot 1}{n}+\cdots+\cos\frac{2\pi\cdot t_1\cdot(n-1)}{n}\cos\frac{2\pi\cdot t_2\cdot(n-1)}{n}$$

From the product-to-sum trigonometric identity (Abramowitz and Stegun [1], p. 72) $\cos\alpha\cos\beta=\frac{1}{2}(\cos(\alpha+\beta)+\cos(\alpha-\beta))$, the equality continues as

$$=$$

$$\frac{1}{2}\cos\frac{2\pi\cdot(t_1+t_2)\cdot 0}{n}+\frac{1}{2}\cos\frac{2\pi\cdot(t_1-t_2)\cdot 0}{n}+\frac{1}{2}\cos\frac{2\pi\cdot(t_1+t_2)\cdot 1}{n}+\frac{1}{2}\cos\frac{2\pi\cdot(t_1-t_2)\cdot 1}{n}+\cdots+$$

$$\frac{1}{2}\cos\frac{2\pi\cdot(t_1+t_2)\cdot(n-1)}{n}+\frac{1}{2}\cos\frac{2\pi\cdot(t_1-t_2)\cdot(n-1)}{n}$$

$$=\frac{1}{2}\left(\cos\frac{2\pi\cdot(t_1+t_2)\cdot 0}{n}+\cos\frac{2\pi\cdot(t_1+t_2)\cdot 1}{n}+\cdots+\cos\frac{2\pi\cdot(t_1+t_2)\cdot(n-1)}{n}\right)+\frac{1}{2}\left(\cos\frac{2\pi\cdot(t_1-t_2)\cdot 0}{n}+\right.$$

$$\left.\cos\frac{2\pi\cdot(t_1-t_2)\cdot 1}{n}+\cdots+\cos\frac{2\pi\cdot(t_1-t_2)\cdot(n-1)}{n}\right)$$

Applying the sum of cosines with arguments in arithmetic progression formula (Knapp [54]) $\cos\varphi+\cos(\varphi+\alpha)+\cos(\varphi+2\alpha)+\cdots+\cos(\varphi+(n-1)\alpha)=\frac{\sin\frac{n\alpha}{2}\cos\left(\varphi+\frac{(n-1)\alpha}{2}\right)}{\sin\frac{\alpha}{2}}$ with $\varphi=0$ and $\alpha=\frac{2\pi(t_1\pm t_2)}{n}$ to each of the brackets above, we have

$$=\frac{1}{2}\,\frac{\sin\frac{n\frac{2\pi(t_1+t_2)}{n}}{2}\cos\frac{(n-1)\frac{2\pi(t_1+t_2)}{n}}{2}}{\sin\frac{\frac{2\pi(t_1+t_2)}{n}}{2}}+\frac{1}{2}\,\frac{\sin\frac{n\frac{2\pi(t_1-t_2)}{n}}{2}\cos\frac{(n-1)\frac{2\pi(t_1-t_2)}{n}}{2}}{\sin\frac{\frac{2\pi(t_1-t_2)}{n}}{2}}$$

$$=\frac{1}{2}\,\frac{\sin\pi(t_1+t_2)\cos\left(\pi(t_1+t_2)-\frac{\pi(t_1+t_2)}{n}\right)}{\sin\frac{\pi(t_1+t_2)}{n}}+\frac{1}{2}\,\frac{\sin\pi(t_1-t_2)\cos\left(\pi(t_1-t_2)-\frac{\pi(t_1-t_2)}{n}\right)}{\sin\frac{\pi(t_1-t_2)}{n}}=0$$

The last equality holds, since both $\sin\pi(t_1+t_2)$ and $\sin\pi(t_1-t_2)$ are equal to zero for all integers t_1,t_2, and both summands in the last expression are equal to zero too, and thus so is their sum. □

Corollary 9.1 The first $\left\lfloor \frac{n}{2} \right\rfloor + 1$ rows of the $n \times n$ matrix R_{cos} are linearly independent.

Proof. Integers $t_1 \neq t_2$ in the range $0 \leq t_1, t_2 \leq \left\lfloor \frac{n}{2} \right\rfloor + 1$ satisfy the conditions of Lemma 9.5, and therefore are mutually orthogonal. Non-zero non-zero mutually orthogonal vectors are linearly independent. □

Corollary 9.2 Rank$(R_{cos}) = \left\lfloor \frac{n}{2} \right\rfloor + 1$.

Proof. Cosine is an even function of period 2π, $\cos\frac{2\pi \cdot s \cdot t}{n} = \cos\frac{2\pi \cdot (n-s) \cdot t}{n}$, for all $1 \leq s \leq \left\lfloor \frac{n}{2} \right\rfloor$ and all $0 \leq t \leq n-1$. Then, rows s and $n-s$ are equal to each other. Because the first $\left\lfloor \frac{n}{2} \right\rfloor + 1$ rows are linearly independent, by Corollary 9.1, Rank$(R_{cos}) = \left\lfloor \frac{n}{2} \right\rfloor + 1$. □

Lemma 9.6 Let $t_1$and t_2 be two integers such that $0 \leq t_1, t_2 \leq n-1$, $t_1 \neq t_2$ and $t_1 + t_2 \neq n$. Then rows t_1 and t_2 of the $n \times n$ matrix

$$R_{sin} = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & 0 \\ 0 & \sin\frac{2\pi \cdot 1 \cdot 1}{n} & \sin\frac{2\pi \cdot 1 \cdot 2}{n} & \ldots & \sin\frac{2\pi \cdot 1 \cdot (n-2)}{n} & \sin\frac{2\pi \cdot 1 \cdot (n-1)}{n} \\ 0 & \sin\frac{2\pi \cdot 2 \cdot 1}{n} & \sin\frac{2\pi \cdot 2 \cdot 2}{n} & \ldots & \sin\frac{2\pi \cdot 2 \cdot (n-2)}{n} & \sin\frac{2\pi \cdot 2 \cdot (n-1)}{n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \sin\frac{2\pi \cdot (n-2) \cdot 1}{n} & \sin\frac{2\pi \cdot (n-2) \cdot 2}{n} & \ldots & \sin\frac{2\pi \cdot (n-2) \cdot (n-2)}{n} & \sin\frac{2\pi \cdot (n-2) \cdot (n-1)}{n} \\ 0 & \sin\frac{2\pi \cdot (n-1) \cdot 1}{n} & \sin\frac{2\pi \cdot (n-1) \cdot 2}{n} & \cdots & \sin\frac{2\pi \cdot (n-1) \cdot (n-2)}{n} & \sin\frac{2\pi \cdot (n-1) \cdot (n-1)}{n} \end{bmatrix}$$

over the real numbers are orthogonal in respect to the Euclidian inner product

$\langle x, y \rangle_{\mathbb{R}} = \sum_{t=0}^{n-1} x_t y_t$.

Proof. The proof is quite similar to Lemma 9.5. Express matrix R_{sin} as follows:

$$R_{sin} = \begin{bmatrix} \sin\frac{2\pi\cdot 0\cdot 0}{n} & \sin\frac{2\pi\cdot 0\cdot 1}{n} & \sin\frac{2\pi\cdot 0\cdot 2}{n} & \dots & \sin\frac{2\pi\cdot 0\cdot (n-2)}{n} & \sin\frac{2\pi\cdot 0\cdot (n-1)}{n} \\ \sin\frac{2\pi\cdot 1\cdot 0}{n} & \sin\frac{2\pi\cdot 1\cdot 1}{n} & \sin\frac{2\pi\cdot 1\cdot 2}{n} & \dots & \sin\frac{2\pi\cdot 1\cdot (n-2)}{n} & \sin\frac{2\pi\cdot 1\cdot (n-1)}{n} \\ \sin\frac{2\pi\cdot 0\cdot 2}{n} & \sin\frac{2\pi\cdot 2\cdot 1}{n} & \sin\frac{2\pi\cdot 2\cdot 2}{n} & \dots & \sin\frac{2\pi\cdot 2\cdot (n-2)}{n} & \sin\frac{2\pi\cdot 2\cdot (n-1)}{n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \sin\frac{2\pi\cdot (n-2)\cdot 0}{n} & \sin\frac{2\pi\cdot (n-2)\cdot 1}{n} & \sin\frac{2\pi\cdot (n-2)\cdot 2}{n} & \dots & \sin\frac{2\pi\cdot (n-2)\cdot (n-2)}{n} & \sin\frac{2\pi\cdot (n-2)\cdot (n-1)}{n} \\ \sin\frac{2\pi\cdot (n-1)\cdot 0}{n} & \sin\frac{2\pi\cdot (n-1)\cdot 1}{n} & \sin\frac{2\pi\cdot (n-1)\cdot 2}{n} & \cdots & \sin\frac{2\pi\cdot (n-1)\cdot (n-2)}{n} & \sin\frac{2\pi\cdot (n-1)\cdot (n-1)}{n} \end{bmatrix}$$

Let $t_1 \neq t_2$ be two integers satisfying the conditions of Lemma 9.6. Consider the inner product of rows t_1 and t_2. We will show it is equal to zero. We have

$$\left\langle \left[\sin\frac{2\pi\cdot t_1\cdot 0}{n}, \sin\frac{2\pi\cdot t_1\cdot 1}{n}, \dots, \sin\frac{2\pi\cdot t_1\cdot (n-1)}{n}\right], \left[\sin\frac{2\pi\cdot t_2\cdot 0}{n}, \sin\frac{2\pi\cdot t_2\cdot 1}{n}, \dots, \sin\frac{2\pi\cdot t_2\cdot (n-1)}{n}\right]\right\rangle_{\mathbb{R}} =$$

$$\sin\frac{2\pi\cdot t_1\cdot 0}{n}\sin\frac{2\pi\cdot t_2\cdot 0}{n} + \sin\frac{2\pi\cdot t_1\cdot 1}{n}\sin\frac{2\pi\cdot t_2\cdot 1}{n} + \cdots + \sin\frac{2\pi\cdot t_1\cdot (n-1)}{n}\sin\frac{2\pi\cdot t_2\cdot (n-1)}{n}$$

From the product-to-sum trigonometric identity (Abramowitz and Stegun [1], p. 72) $\sin\alpha\sin\beta = \frac{1}{2}(\cos(\alpha-\beta) - \cos(\alpha+\beta))$, the last equality can be continued as

$$= \frac{1}{2}\cos\frac{2\pi\cdot(t_1-t_2)\cdot 0}{n} - \frac{1}{2}\cos\frac{2\pi\cdot(t_1+t_2)\cdot 0}{n} + \frac{1}{2}\cos\frac{2\pi\cdot(t_1-t_2)\cdot 1}{n} - \frac{1}{2}\cos\frac{2\pi\cdot(t_1+t_2)\cdot 1}{n} + \cdots + \frac{1}{2}\cos\frac{2\pi\cdot(t_1-t_2)\cdot(n-1)}{n} - \frac{1}{2}\cos\frac{2\pi\cdot(t_1+t_2)\cdot(n-1)}{n}$$

$$= \frac{1}{2}\left(\cos\frac{2\pi\cdot(t_1-t_2)\cdot 0}{n} + \cos\frac{2\pi\cdot(t_1-t_2)\cdot 1}{n} + \cdots + \cos\frac{2\pi\cdot(t_1-t_2)\cdot(n-1)}{n}\right) - \frac{1}{2}\left(\cos\frac{2\pi\cdot(t_1+t_2)\cdot 0}{n} + \cos\frac{2\pi\cdot(t_1+t_2)\cdot 1}{n} + \cdots + \cos\frac{2\pi\cdot(t_1+t_2)\cdot(n-1)}{n}\right)$$

Applying the sum of cosines with arguments in arithmetic progression formula (Knapp [54]) $\cos\varphi + \cos(\varphi+\alpha) + \cos(\varphi+2\alpha) + \cdots + \cos(\varphi+(n-1)\alpha) = \frac{\sin\frac{n\alpha}{2}\cos(\varphi+\frac{(n-1)\alpha}{2})}{\sin\frac{\alpha}{2}}$ with $\varphi = 0$ and $\alpha = \frac{2\pi(t_1 \pm t_2)}{n}$ to each of the above brackets, we have

$$= \frac{1}{2}\frac{\sin\frac{n\frac{2\pi(t_1-t_2)}{n}}{2}\cos\frac{(n-1)\frac{2\pi(t_1-t_2)}{n}}{2}}{\sin\frac{\frac{2\pi(t_1-t_2)}{n}}{2}} - \frac{1}{2}\frac{\sin\frac{n\frac{2\pi(t_1+t_2)}{n}}{2}\cos\frac{(n-1)\frac{2\pi(t_1+t_2)}{n}}{2}}{\sin\frac{\frac{2\pi(t_1+t_2)}{n}}{2}}$$

$$= \frac{1}{2}\frac{\sin\pi(t_1-t_2)\cos(\pi(t_1-t_2)-\frac{\pi(t_1-t_2)}{n})}{\sin\frac{\pi(t_1-t_2)}{n}} - \frac{1}{2}\frac{\sin\pi(t_1+t_2)\cos(\pi(t_1+t_2)-\frac{\pi(t_1+t_2)}{n})}{\sin\frac{\pi(t_1+t_2)}{n}} = 0$$

Indeed, since both $\sin\pi(t_1+t_2)$ and $\sin\pi(t_1-t_2)$ are equal to zero for all integers t_1, t_2, both summands in the last expression above are zeros too, and so is their sum. □

Observation 9.1 The first row of the matrix R_{sin} is the all-zero row; if n is an even number, then row $\frac{n}{2}$ is the all-zero row too.

Corollary 9.3 The first $\left\lceil\frac{n}{2}\right\rceil - 1$ non-zero rows of $n \times n$ matrix R_{sin} (numbered from 1 to $\left\lceil\frac{n}{2}\right\rceil - 1$) are linearly independent.

Proof. Integers $t_1 \neq t_2$ in the range $1 \leq t_1, t_2 \leq \left\lceil\frac{n}{2}\right\rceil - 1$ satisfy the conditions of Lemma 9.6. The first $\left\lfloor\frac{n}{2}\right\rfloor + 1$ rows of matrix R_{sin} (including all-zero rows) are mutually orthogonal, therefore, $\left\lceil\frac{n}{2}\right\rceil - 1$ non-zero rows are linearly independent. □

Corollary 9.4 Rank$(R_{sin}) = \left\lceil\frac{n}{2}\right\rceil - 1$.

Proof. Sine is an odd function of period 2π, $\sin\frac{2\pi\cdot s\cdot t}{n} = -\sin\frac{2\pi\cdot(n-s)\cdot t}{n}$, for all $1 \leq s \leq \left\lfloor\frac{n}{2}\right\rfloor$ and all $0 \leq t \leq n-1$. Then, rows s and $n-s$ are negatives of each other. Because the first $\left\lceil\frac{n}{2}\right\rceil - 1$ non-zero rows are linearly independent, by Corollary 9.3, Rank$(R_{sin}) = \left\lceil\frac{n}{2}\right\rceil - 1$. □

Lemma 9.7 For $a \in \mathbb{R}$, the general solution in $\mathbb{R}^n$ of the system of simultaneous linear equations

$$\begin{cases} z_0 + z_1 + \cdots + z_{n-1} = a \\ z_0 + z_1 \cos\frac{2\pi\cdot 1\cdot 1}{n} + z_2 \cos\frac{2\pi\cdot 1\cdot 2}{n} + \cdots + z_{n-1}\cos\frac{2\pi\cdot 1\cdot (n-1)}{n} = 0 \\ z_0 + z_1 \cos\frac{2\pi\cdot 2\cdot 1}{n} + z_2 \cos\frac{2\pi\cdot 2\cdot 2}{n} + \cdots + z_{n-1}\cos\frac{2\pi\cdot 2\cdot (n-1)}{n} = 0 \\ \cdots \\ z_0 + z_1 \cos\frac{2\pi\cdot (n-2)\cdot 1}{n} + z_2 \cos\frac{2\pi\cdot (n-2)\cdot 2}{n} + \cdots + z_{n-1}\cos\frac{2\pi\cdot (n-2)\cdot (n-1)}{n} = 0 \\ z_0 + z_1 \cos\frac{2\pi\cdot (n-1)\cdot 1}{n} + z_2 \cos\frac{2\pi\cdot (n-1)\cdot 2}{n} + \cdots + z_{n-1}\cos\frac{2\pi\cdot (n-1)\cdot (n-1)}{n} = 0 \end{cases}$$

(9.2)

is either $z_0 = \frac{a}{n},\ z_1 = \frac{2a}{n} - z_{n-1}, \dots,\ z_{\frac{n}{2}-1} = \frac{2a}{n} - z_{\frac{n}{2}+1}, z_{\frac{n}{2}} = \frac{a}{n}$, when n is even;

or $z_0 = \frac{a}{n},\ z_1 = \frac{2a}{n} - z_{n-1}, \dots,\ z_{\left\lfloor \frac{n}{2} \right\rfloor} = \frac{2a}{n} - z_{\left\lceil \frac{n}{2} \right\rceil}$, when n is odd.

Proof. Note that the matrix of system (9.2) is exactly R_{cos}, defined in Lemma 9.5. By Corollary 9.2, the rank of system (9.2) is $\mathrm{Rank}(R_{cos}) = \left\lfloor \frac{n}{2} \right\rfloor + 1$ and, therefore, the general solution will have $n - \left\lfloor \frac{n}{2} \right\rfloor - 1 = \left\lceil \frac{n}{2} \right\rceil - 1$ independent and $\left\lfloor \frac{n}{2} \right\rfloor + 1$ dependent variables.

Because, by Corollary 9.1, the first $\left\lfloor \frac{n}{2} \right\rfloor + 1$ rows of the matrix R_{cos} are linearly independent, (9.2) is equivalent to (9.3), which consists of only the $\left\lfloor \frac{n}{2} \right\rfloor + 1$ first equations from (9.2):

$$\begin{cases} z_0 + z_1 + \cdots + z_{n-1} = a \\ z_0 + z_1 \cos\frac{2\pi\cdot 1\cdot 1}{n} + z_2 \cos\frac{2\pi\cdot 1\cdot 2}{n} + \cdots + z_{n-1}\cos\frac{2\pi\cdot 1\cdot (n-1)}{n} = 0 \\ z_0 + z_1 \cos\frac{2\pi\cdot 2\cdot 1}{n} + z_2 \cos\frac{2\pi\cdot 2\cdot 2}{n} + \cdots + z_{n-1}\cos\frac{2\pi\cdot 2\cdot (n-1)}{n} = 0 \\ \cdots \\ z_0 + z_1 \cos\frac{2\pi\cdot \left\lfloor \frac{n}{2} \right\rfloor\cdot 1}{n} + z_2 \cos\frac{2\pi\cdot \left\lfloor \frac{n}{2} \right\rfloor\cdot 2}{n} + \cdots + z_{n-1}\cos\frac{2\pi\cdot \left\lfloor \frac{n}{2} \right\rfloor\cdot (n-1)}{n} = 0 \\ z_0 + z_1 \cos\frac{2\pi\cdot (\left\lfloor \frac{n}{2} \right\rfloor+1)\cdot 1}{n} + z_2 \cos\frac{2\pi\cdot (\left\lfloor \frac{n}{2} \right\rfloor+1)\cdot 2}{n} + \cdots + z_{n-1}\cos\frac{2\pi\cdot (\left\lfloor \frac{n}{2} \right\rfloor+1)\cdot (n-1)}{n} = 0 \end{cases}$$

(9.3)

Note that $\cos\frac{2\pi k\cdot t}{n} = \cos\frac{2\pi k\cdot (n-t)}{n}$ for every integer $0 \le k \le \left\lfloor \frac{n}{2} \right\rfloor$, and therefore the matrix of system (9.3) possesses a special symmetry: the second column is equal to the last column, the third column is equal to the one just before last, and so on. Thus, each equation in (9.3) contains pairs of equal coefficients.

Consider two cases, n even or n odd, separately.

If n is an even number, then (9.3) consists of $\frac{n}{2}+1$ equations. Every term in each equation, except for the first and the last ones, has an equal counterpart in the same equation. Therefore, after re-arranging the equal terms together, (9.3) can be written as

$$\begin{cases} z_0 + (z_1 + z_{n-1}) + \cdots + \left(z_{\frac{n}{2}-1} + z_{\frac{n}{2}+1}\right) + z_{\frac{n}{2}} = a \\ z_0 + (z_1 + z_{n-1}) \cos\frac{2\pi\cdot 1\cdot 1}{n} + \cdots + \left(z_{\frac{n}{2}-1} + z_{\frac{n}{2}+1}\right) \cos\frac{2\pi\cdot 1\cdot(\frac{n}{2}-1)}{n} + z_{\frac{n}{2}} \cos\frac{2\pi\cdot 1\cdot\frac{n}{2}}{n} = 0 \\ z_0 + (z_1 + z_{n-1}) \cos\frac{2\pi\cdot 2\cdot 1}{n} + \cdots + \left(z_{\frac{n}{2}-1} + z_{\frac{n}{2}+1}\right) \cos\frac{2\pi\cdot 2\cdot(\frac{n}{2}-1)}{n} + z_{\frac{n}{2}} \cos\frac{2\pi\cdot 2\cdot\frac{n}{2}}{n} = 0 \\ \cdots \\ z_0 + (z_1 + z_{n-1}) \cos\frac{2\pi\cdot(\frac{n}{2}-1)\cdot 1}{n} + \cdots + \left(z_{\frac{n}{2}-1} + z_{\frac{n}{2}+1}\right) \cos\frac{2\pi\cdot(\frac{n}{2}-1)\cdot(\frac{n}{2}-1)}{n} + z_{\frac{n}{2}} \cos\frac{2\pi\cdot(\frac{n}{2}-1)\cdot\frac{n}{2}}{n} = 0 \\ z_0 + (z_1 + z_{n-1}) \cos\frac{2\pi\cdot\frac{n}{2}\cdot 1}{n} + \cdots + \left(z_{\frac{n}{2}-1} + z_{\frac{n}{2}+1}\right) \cos\frac{2\pi\cdot\frac{n}{2}\cdot(\frac{n}{2}-1)}{n} + z_{\frac{n}{2}} \cos\frac{2\pi\cdot\frac{n}{2}\cdot\frac{n}{2}}{n} = 0 \end{cases}$$

After the substitution of variables

$$x_0 = z_0,\ x_1 = z_1 + z_{n-1}, \ldots, x_{\frac{n}{2}-1} = z_{\frac{n}{2}-1} + z_{\frac{n}{2}+1},\ x_{\frac{n}{2}} = z_{\frac{n}{2}}$$

(9.3) can be written as

$$\begin{cases} x_0 + x_1 + \cdots + x_{\frac{n}{2}-1} + x_{\frac{n}{2}} = a \\ x_0 + x_1 \cos\frac{2\pi\cdot 1\cdot 1}{n} + \cdots + x_{\frac{n}{2}-1} \cos\frac{2\pi\cdot 1\cdot(\frac{n}{2}-1)}{n} + x_{\frac{n}{2}} \cos\frac{2\pi\cdot 1\cdot\frac{n}{2}}{n} = 0 \\ x_0 + x_1 \cos\frac{2\pi\cdot 2\cdot 1}{n} + \cdots + x_{\frac{n}{2}-1} \cos\frac{2\pi\cdot 2\cdot(\frac{n}{2}-1)}{n} + x_{\frac{n}{2}} \cos\frac{2\pi\cdot 2\cdot\frac{n}{2}}{n} = 0 \\ \cdots \\ x_0 + x_1 \cos\frac{2\pi\cdot(\frac{n}{2}-1)\cdot 1}{n} + \cdots + x_{\frac{n}{2}-1} \cos\frac{2\pi\cdot(\frac{n}{2}-1)\cdot(\frac{n}{2}-1)}{n} + x_{\frac{n}{2}} \cos\frac{2\pi\cdot(\frac{n}{2}-1)\cdot\frac{n}{2}}{n} = 0 \\ x_0 + x_1 \cos\frac{2\pi\cdot\frac{n}{2}\cdot 1}{n} + \cdots + x_{\frac{n}{2}-1} \cos\frac{2\pi\cdot\frac{n}{2}\cdot(\frac{n}{2}-1)}{n} + x_{\frac{n}{2}} \cos\frac{2\pi\cdot\frac{n}{2}\cdot\frac{n}{2}}{n} = 0 \end{cases} \tag{9.4}$$

Because the $\left(\frac{n}{2}+1\right)\times\left(\frac{n}{2}+1\right)$ matrix of system (9.4) has been obtained by elimination of $\frac{n}{2}-1$ 'twin' columns in the $\left(\frac{n}{2}+1\right)\times n$ matrix of system (9.3), which has rank $\frac{n}{2}+1$, the matrix of system (9.4) has the same rank $\frac{n}{2}+1$. Therefore, the matrix of system (9.4) is non-singular and (9.4) has exactly one solution in $\mathbb{R}^{\frac{n}{2}+1}$.

It is not difficult to see, without actually solving the system, that

$$x_0=\frac{a}{n}, x_1=\frac{2a}{n}, \dots, x_{\frac{n}{2}-1}=\frac{2a}{n}, x_{\frac{n}{2}}=\frac{a}{n}$$

is the solution of (9.4).

Indeed, the first equation is obviously true for $x_0=\frac{a}{n}, x_1=\frac{2a}{n}, \dots, x_{\frac{n}{2}-1}=\frac{2a}{n}, x_{\frac{n}{2}}=\frac{a}{n}$,

because $\frac{a}{n}+\underbrace{\frac{2a}{n}+\cdots+\frac{2a}{n}}_{\left(\frac{n-2}{2}\right)\,times}+\frac{a}{n}=n\cdot\frac{a}{n}=a.$

The k-th equation, for $1\le k\le\frac{n}{2}$, after substitution $x_0=\frac{a}{n}, x_1=\frac{2a}{n}, \dots, x_{\frac{n}{2}-1}=\frac{2a}{n}, x_{\frac{n}{2}}=\frac{a}{n}$, becomes

$$\frac{a}{n}+\frac{2a}{n}\cos\frac{2\pi k\cdot 1}{n}+\cdots+\frac{2a}{n}\cos\frac{2\pi k\cdot\left(\frac{n}{2}-1\right)}{n}+\frac{a}{n}\cos\frac{2\pi k\cdot\frac{n}{2}}{n}$$

$$=\frac{a}{n}\left(1+2\cos\frac{2\pi k\cdot 1}{n}+\cdots+2\cos\frac{2\pi k\cdot\left(\frac{n}{2}-1\right)}{n}+\cos\frac{2\pi k\cdot\frac{n}{2}}{n}\right)$$

$$=\frac{a}{n}\left(-1+2\cos\frac{2\pi k\cdot 0}{n}+2\cos\frac{2\pi k\cdot 1}{n}+\cdots+2\cos\frac{2\pi k\cdot\left(\frac{n}{2}-1\right)}{n}+\cos\pi k\right)$$

$$=\frac{a}{n}\left(-1+2\left(\cos\frac{2\pi k\cdot 0}{n}+\cdots+\cos\frac{2\pi k\cdot(\frac{n}{2}-1)}{n}\right)+\cos\pi k\right)$$

Applying the formula (Knapp [54])

$$\cos\varphi+\cos(\varphi+\alpha)+\cos(\varphi+2\alpha)+\cdots+\cos(\varphi+n\alpha)=\frac{\sin\frac{(n+1)\alpha}{2}\cos(\varphi+\frac{n\alpha}{2})}{\sin\frac{\alpha}{2}},$$

with $\varphi = 0$ and $\alpha = \frac{2\pi k}{n}$, we can continue the equality as

$$= \frac{a}{n}\left(-1 + 2\frac{\sin\frac{\frac{n}{2}\cdot\frac{2\pi k}{n}}{2}\cos\frac{(\frac{n}{2}-1)\cdot\frac{2\pi k}{n}}{2}}{\sin\frac{\frac{2\pi k}{n}}{2}} + \cos\pi k\right) = \frac{a}{n}\left(-1 + 2\frac{\sin\frac{\pi k}{2}\cos(\frac{\pi k}{2}-\frac{\pi k}{n})}{\sin\frac{\pi k}{n}} + \cos\pi k\right)$$

If k is an even number then $\sin\frac{\pi k}{2} = 0$, $\cos\pi k = 1$, and the equality continues as

$$= \frac{a}{n}(-1 + 0 + 1) = 0.$$

If k is an odd number then $\frac{\sin\frac{\pi k}{2}\cos(\frac{\pi k}{2}-\frac{\pi k}{n})}{\sin\frac{\pi k}{n}} = \frac{(\pm 1)\cdot(\pm\sin\frac{\pi k}{n})}{\sin\frac{\pi k}{n}} = 1$, $\cos\pi k = -1$ and the equality continues as

$$= \frac{a}{n}(-1 + 2\cdot 1 - 1) = 0.$$

So, the k-th equation in (9.4) holds, for $0 \le k \le \frac{n}{2}$, and the solution of (9.4) for an even n is

$$x_0 = \frac{a}{n}, x_1 = \frac{2a}{n}, \dots, x_{\frac{n}{2}-1} = \frac{2a}{n}, x_{\frac{n}{2}} = \frac{a}{n}$$

Thus, the solution of (9.2) in $\mathbb{R}^n$ is $z_0 = \frac{a}{n}, z_1 + z_{n-1} = \frac{2a}{n}, \dots, z_{\frac{n}{2}-1} + z_{\frac{n}{2}+1} = \frac{2a}{n}, z_{\frac{n}{2}} = \frac{a}{n}$, or

$$z_0 = \frac{a}{n}, \qquad z_1 = \frac{2a}{n} - z_{n-1}, \quad \dots, \qquad z_{\frac{n}{2}-1} = \frac{2a}{n} - z_{\frac{n}{2}+1}, \qquad z_{\frac{n}{2}} = \frac{a}{n}$$

If n is an odd number, then (9.3) consists of $\left\lfloor\frac{n}{2}\right\rfloor + 1 = \left\lceil\frac{n}{2}\right\rceil$ equations. Every term in each equation has an equal counterpart in the same equation. System (9.3) can be written as

$$\begin{cases} z_0 + (z_1 + z_{n-1}) + \cdots + \left(z_{\left\lfloor \frac{n}{2} \right\rfloor} + z_{\left\lceil \frac{n}{2} \right\rceil}\right) = a \\ z_0 + (z_1 + z_{n-1}) \cos\frac{2\pi\cdot 1\cdot 1}{n} + \cdots + \left(z_{\left\lfloor \frac{n}{2} \right\rfloor} + z_{\left\lceil \frac{n}{2} \right\rceil}\right) \cos\frac{2\pi\cdot 1\cdot \left\lfloor \frac{n}{2} \right\rfloor}{n} = 0 \\ z_0 + (z_1 + z_{n-1}) \cos\frac{2\pi\cdot 2\cdot 1}{n} + \cdots + \left(z_{\left\lfloor \frac{n}{2} \right\rfloor} + z_{\left\lceil \frac{n}{2} \right\rceil}\right) \cos\frac{2\pi\cdot 2\cdot \left\lfloor \frac{n}{2} \right\rfloor}{n} = 0 \\ \cdots \\ z_0 + (z_1 + z_{n-1}) \cos\frac{2\pi\cdot(\left\lfloor \frac{n}{2} \right\rfloor - 1)\cdot 1}{n} + \cdots + \left(z_{\left\lfloor \frac{n}{2} \right\rfloor} + z_{\left\lceil \frac{n}{2} \right\rceil}\right) \cos\frac{2\pi\cdot(\left\lfloor \frac{n}{2} \right\rfloor - 1)\cdot \left\lfloor \frac{n}{2} \right\rfloor}{n} = 0 \\ z_0 + (z_1 + z_{n-1}) \cos\frac{2\pi\cdot \left\lfloor \frac{n}{2} \right\rfloor \cdot 1}{n} + \cdots + \left(z_{\left\lfloor \frac{n}{2} \right\rfloor} + z_{\left\lceil \frac{n}{2} \right\rceil}\right) \cos\frac{2\pi\cdot \left\lfloor \frac{n}{2} \right\rfloor \cdot \left\lfloor \frac{n}{2} \right\rfloor}{n} = 0 \end{cases}$$

After the substitution of variables

$$x_0 = z_0, x_1 = z_1 + z_{n-1}, \dots,\ x_{\left\lfloor \frac{n}{2} \right\rfloor} = z_{\frac{n}{2}-1} + z_{\frac{n}{2}+1}$$

(9.3) can be written as

$$\begin{cases} x_0 + x_1 + \cdots + x_{\left\lfloor \frac{n}{2} \right\rfloor} = a \\ x_0 + x_1 \cos\frac{2\pi\cdot 1\cdot 1}{n} + \cdots + x_{\left\lfloor \frac{n}{2} \right\rfloor} \cos\frac{2\pi\cdot 1\cdot \left\lfloor \frac{n}{2} \right\rfloor}{n} = 0 \\ x_0 + x_1 \cos\frac{2\pi\cdot 2\cdot 1}{n} + \cdots + x_{\left\lfloor \frac{n}{2} \right\rfloor} \cos\frac{2\pi\cdot 2\cdot \left\lfloor \frac{n}{2} \right\rfloor}{n} = 0 \\ \cdots \\ x_0 + x_1 \cos\frac{2\pi\cdot(\left\lfloor \frac{n}{2} \right\rfloor - 1)\cdot 1}{n} + \cdots + x_{\left\lfloor \frac{n}{2} \right\rfloor} \cos\frac{2\pi\cdot(\left\lfloor \frac{n}{2} \right\rfloor - 1)\cdot \left\lfloor \frac{n}{2} \right\rfloor}{n} = 0 \\ x_0 + x_1 \cos\frac{2\pi\cdot \left\lfloor \frac{n}{2} \right\rfloor \cdot 1}{n} + \cdots + x_{\left\lfloor \frac{n}{2} \right\rfloor} \cos\frac{2\pi\cdot \left\lfloor \frac{n}{2} \right\rfloor \cdot \left\lfloor \frac{n}{2} \right\rfloor}{n} = 0 \end{cases} \tag{9.5}$$

Because the $\left\lceil \frac{n}{2} \right\rceil \times \left\lceil \frac{n}{2} \right\rceil$ matrix of system (9.5) has been obtained by elimination of $\left\lfloor \frac{n}{2} \right\rfloor$ 'twin' columns in the $\left\lceil \frac{n}{2} \right\rceil \times n$ matrix of system (9.3), which has rank $\left\lfloor \frac{n}{2} \right\rfloor + 1 = \left\lceil \frac{n}{2} \right\rceil$, the matrix of system (9.5) has rank $\left\lceil \frac{n}{2} \right\rceil$. Therefore, the matrix of system (9.5) is non-singular and (9.5) has exactly one solution in $\mathbb{R}^{\left\lceil \frac{n}{2} \right\rceil}$.

Similar to the case of an even n, it is not difficult to see, without actually solving the system, that

$$x_0 = \frac{a}{n}, x_1 = \frac{2a}{n}, \dots,\ x_{\left\lfloor\frac{n}{2}\right\rfloor} = \frac{2a}{n}$$

is the solution for (9.5).

Again, the first equation is obviously true for $x_0 = \frac{a}{n}, x_1 = \frac{2a}{n}, \dots,\ x_{\left\lfloor\frac{n}{2}\right\rfloor} = \frac{2a}{n}$,

since $\frac{a}{n} + \underbrace{\frac{2a}{n} + \cdots + \frac{2a}{n}}_{\left(\frac{n-1}{2}\right)\ times} = n \cdot \frac{a}{n} = a.$

The k-th equation, for $1 \le k \le \left\lfloor\frac{n}{2}\right\rfloor$, after substitution $x_0 = \frac{a}{n}, x_1 = \frac{2a}{n}, \dots, x_{\left\lfloor\frac{n}{2}\right\rfloor} = \frac{2a}{n}$, becomes

$$\frac{a}{n} + \frac{2a}{n}\cos\frac{2\pi k\cdot 1}{n} + \cdots + \frac{2a}{n}\cos\frac{2\pi k\cdot\left\lfloor\frac{n}{2}\right\rfloor}{n} = \frac{a}{n}\left(1 + 2\cos\frac{2\pi k\cdot 1}{n} + \cdots + 2\cos\frac{2\pi k\cdot\left\lfloor\frac{n}{2}\right\rfloor}{n}\right)$$

$$= \frac{a}{n}\left(-1 + 2\cos\frac{2\pi k\cdot 0}{n} + 2\cos\frac{2\pi k\cdot 1}{n} + \cdots + 2\cos\frac{2\pi k\cdot\left\lfloor\frac{n}{2}\right\rfloor}{n}\right)$$

$$= \frac{a}{n}\left(-1 + 2\left(\cos\frac{2\pi k\cdot 0}{n} + \cdots + \cos\frac{2\pi k\cdot\left\lfloor\frac{n}{2}\right\rfloor}{n}\right)\right) = \frac{a}{n}\left(-1 + 2\,\frac{\sin\frac{\left(\left\lfloor\frac{n}{2}\right\rfloor+1\right)\cdot\frac{2\pi k}{n}}{2}\cos\frac{\left\lfloor\frac{n}{2}\right\rfloor\cdot\frac{2\pi k}{n}}{2}}{\sin\frac{\frac{2\pi k}{n}}{2}}\right)$$

$$= \frac{a}{n}\left(-1 + 2\,\frac{\sin\frac{\left(\frac{n-1}{2}+1\right)\cdot\frac{2\pi k}{n}}{2}\cos\frac{\frac{n-1}{2}\cdot\frac{2\pi k}{n}}{2}}{\sin\frac{\frac{2\pi k}{n}}{2}}\right) = \frac{a}{n}\left(-1 + 2\,\frac{\sin\frac{\frac{n+1}{2}\cdot\frac{2\pi k}{n}}{2}\cos\frac{\frac{n-1}{2}\cdot\frac{2\pi k}{n}}{2}}{\sin\frac{\frac{2\pi k}{n}}{2}}\right)$$

$$= \frac{a}{n}\left(-1 + 2\,\frac{\sin\left(\frac{\pi k}{2}+\frac{\pi k}{2n}\right)\cos\left(\frac{\pi k}{2}-\frac{\pi k}{2n}\right)}{\sin\frac{\pi k}{n}}\right)$$

From the formula (Abramowitz and Stegun [1], p. 72) $\sin\alpha + \sin\beta = 2\sin\frac{\alpha+\beta}{2}\cos\frac{\alpha-\beta}{2}$, the equality continues

$$= -1 + \frac{\sin\pi k + \sin\frac{\pi k}{n}}{\sin\frac{\pi k}{n}} = -1 + \frac{\sin\pi k}{\sin\frac{\pi k}{n}} + 1 = 0.$$

Therefore, the k-th equation in (9.5) holds, for $0 \le k \le \left\lfloor\frac{n}{2}\right\rfloor$, and the solution of (9.5) for an odd n is

$$x_0 = \frac{a}{n}, x_1 = \frac{2a}{n}, \dots, x_{\left\lfloor \frac{n}{2} \right\rfloor} = \frac{2a}{n}$$

Thus, the solution of (9.2) in $\mathbb{R}^n$ is $z_0 = \frac{a}{n}, z_1 + z_{n-1} = \frac{2a}{n}, \dots, z_{\left\lfloor \frac{n}{2} \right\rfloor} + z_{\left\lceil \frac{n}{2} \right\rceil} = \frac{2a}{n}$, or

$$z_0 = \frac{a}{n}, \qquad z_1 = \frac{2a}{n} - z_{n-1}, \quad \dots , \qquad z_{\left\lfloor \frac{n}{2} \right\rfloor} = \frac{2a}{n} - z_{\left\lceil \frac{n}{2} \right\rceil}$$

This completes the proof of Lemma 9.7. □

<u>Lemma 9.8</u> The general solution in $\mathbb{H}^n$ of the system of simultaneous linear equations

$$\begin{cases} \boldsymbol{z}_0 \sin\frac{2\pi\cdot 0\cdot 0}{n} + \boldsymbol{z}_1 \sin\frac{2\pi\cdot 1\cdot 0}{n} + \cdots + \boldsymbol{z}_{n-1} \sin\frac{2\pi\cdot(n-1)\cdot 0}{n} = 0 \\ \boldsymbol{z}_0 \sin\frac{2\pi\cdot 1\cdot 0}{n} + \boldsymbol{z}_1 \sin\frac{2\pi\cdot 1\cdot 1}{n} + \cdots + \boldsymbol{z}_{n-1} \sin\frac{2\pi\cdot(n-1)\cdot 1}{n} = 0 \\ \boldsymbol{z}_0 \sin\frac{2\pi\cdot 2\cdot 0}{n} + \boldsymbol{z}_1 \sin\frac{2\pi\cdot 2\cdot 1}{n} + \cdots + \boldsymbol{z}_{n-1} \sin\frac{2\pi\cdot 2\cdot(n-1)}{n} = 0 \\ \cdots \\ \boldsymbol{z}_0 \sin\frac{2\pi\cdot(n-2)\cdot 0}{n} + \boldsymbol{z}_1 \sin\frac{2\pi\cdot(n-2)\cdot 1}{n} + \cdots + \boldsymbol{z}_{n-1} \sin\frac{2\pi\cdot(n-2)\cdot(n-1)}{n} = 0 \\ \boldsymbol{z}_0 \sin\frac{2\pi\cdot(n-1)\cdot 0}{n} + \boldsymbol{z}_1 \sin\frac{2\pi\cdot(n-1)\cdot 1}{n} + \cdots + \boldsymbol{z}_{n-1} \sin\frac{2\pi\cdot(n-1)\cdot(n-1)}{n} = 0 \end{cases} \tag{9.6}$$

is $\boldsymbol{z}_1 = \boldsymbol{z}_{n-1}$, $\boldsymbol{z}_2 = \boldsymbol{z}_{n-2}$, … , $\boldsymbol{z}_{\left\lceil \frac{n}{2} \right\rceil - 1} = \boldsymbol{z}_{\left\lfloor \frac{n}{2} \right\rfloor + 1}$; $\boldsymbol{z}_0$ and, in the case of even n, $\boldsymbol{z}_{\frac{n}{2}}$ are arbitrary quaternions.

<u>Proof.</u> Unlike in Lemma 9.7, where we were interested in finding solutions of simultaneous linear equations in $\mathbb{R}^n$, we now seek for the general solution in $\mathbb{H}^n$. Although a problem of finding solutions of a linear equation $\boldsymbol{Ax} = \boldsymbol{b}$ over the real quaternions may look somewhat complicated, we will be able to reduce the system in question to the special case $\boldsymbol{Ax} = 0$, for which it is known (Zhang [98], Theorem 4.3) that, in the case of an invertible matrix $\boldsymbol{A}$, it has a unique solution $\boldsymbol{x} = 0$.

The concepts of rank, linear independence, characteristic matrix etc are applicable to matrices over $\mathbb{H}$ (Zhang [98]). However, because of the non-commutative nature of the quaternions, the left and right linear independence over $\mathbb{H}$ is to be treated separately. There are examples of left linear dependent vectors which are right linearly independent, and vice versa. Note that two linear dependent vectors over $\mathbb{H}^n$ may be linearly independent over $\mathbb{C}^n$. However, since the real numbers commute with all quaternions, it is easy to understand that for vectors from $\mathbb{R}^n$, which is a subspace of $\mathbb{H}^n$, concepts of left and right linear independence are equivalent, and their linear independence over $\mathbb{C}^n$ implies linear independence over $\mathbb{H}^n$.

The rank of a quaternion matrix $\boldsymbol{Q}$ is defined as the maximum number of rows which are left linearly independent. If a matrix $\boldsymbol{Q}$ is of rank r, then r is also the maximum number of columns that are right linearly independent. An $n \times n$ matrix $\boldsymbol{Q}$ is invertible, meaning there exists $\boldsymbol{B}$ such that $\boldsymbol{QB} = \boldsymbol{BQ} = I$, if and only if $\mathrm{Rank}(\boldsymbol{Q}) = n$. If $\boldsymbol{A}$ is an $m \times n$ matrix over $\mathbb{H}$ of rank r, then the solutions of $\boldsymbol{Ax} = 0$ form a subspace in $\mathbb{H}^n$ of dimension $n - r$.

Because for vectors from $\mathbb{R}^n$ linear independence over $\mathbb{C}^n$ is equivalent to linear independence over $\mathbb{H}^n$, the rank of a matrix with real entries over $\mathbb{C}$ coincides with its rank over $\mathbb{H}$. That is, if R is a matrix over the real field $\mathbb{R}$, then $\mathrm{Rank}_{\mathbb{C}}(R) = \mathrm{Rank}_{\mathbb{H}}(R)$. Therefore, the dimension of the subspace of solutions of $R\boldsymbol{x} = 0$ in $\mathbb{H}^n$ is $n - \mathrm{Rank}_{\mathbb{C}}(R)$.

Note that the matrix of system (9.6) is exactly the matrix R_{sin}, defined in Lemma 9.6, which is a matrix over $\mathbb{R}$. By Corollary 9.4, the rank of system (9.6) is $\mathrm{Rank}_{\mathbb{C}}(R_{sin}) = \left\lceil \frac{n}{2} \right\rceil - 1$, and therefore the subspace of its solutions is of dimension $n - \left\lceil \frac{n}{2} \right\rceil + 1 = \left\lfloor \frac{n}{2} \right\rfloor + 1$ and the general solution of (9.6) has $\left\lfloor \frac{n}{2} \right\rfloor + 1$ independent and $\left\lceil \frac{n}{2} \right\rceil - 1$ dependent variables. The first and, in the case of even n, the $\frac{n}{2}$-th columns of matrix R_{sin} are columns of zeros. That implies that $\boldsymbol{z}_0$ and, for even n, $\boldsymbol{z}_{\frac{n}{2}}$ can be taken as any arbitrary quaternions in the solution of (9.6).

Because, by Corollary 9.3, the first $\left\lceil \frac{n}{2} \right\rceil - 1$ non-zero rows of the matrix R_{sin} are linearly independent, system (9.6) is equivalent to system (9.7), which contains only the $\left\lceil \frac{n}{2} \right\rceil - 1$ first non-trivial equations from (9.6):

$$\begin{cases} \boldsymbol{z}_0 \sin\frac{2\pi\cdot 1\cdot 0}{n} + \boldsymbol{z}_1 \sin\frac{2\pi\cdot 1\cdot 1}{n} + \cdots + \boldsymbol{z}_{n-1} \sin\frac{2\pi\cdot 1\cdot (n-1)}{n} = 0 \\ \boldsymbol{z}_0 \sin\frac{2\pi\cdot 2\cdot 0}{n} + \boldsymbol{z}_1 \sin\frac{2\pi\cdot 2\cdot 1}{n} + \cdots + \boldsymbol{z}_{n-1} \sin\frac{2\pi\cdot 2\cdot (n-1)}{n} = 0 \\ \cdots \\ \boldsymbol{z}_0 \sin\frac{2\pi\cdot(\left\lceil\frac{n}{2}\right\rceil-1)\cdot 0}{n} + \boldsymbol{z}_1 \sin\frac{2\pi\cdot(\left\lceil\frac{n}{2}\right\rceil-1)\cdot 1}{n} + \cdots + \boldsymbol{z}_{n-1} \sin\frac{2\pi\cdot\left(\left\lceil\frac{n}{2}\right\rceil-1\right)\cdot(n-1)}{n} = 0 \end{cases}$$

(9.7)

Elimination of the all-zero column $\#0$ and, if n is even, $\#\frac{n}{2}$ does not change the solution, and therefore the system becomes:

$$\begin{cases} \boldsymbol{z}_1 \sin\frac{2\pi\cdot 1\cdot 1}{n} + \cdots + \boldsymbol{z}_{\left\lceil\frac{n}{2}\right\rceil-1} \sin\frac{2\pi\cdot 1\cdot(\left\lceil\frac{n}{2}\right\rceil-1)}{n} + \boldsymbol{z}_{\left\lfloor\frac{n}{2}\right\rfloor+1} \sin\frac{2\pi\cdot 1\cdot(\left\lfloor\frac{n}{2}\right\rfloor+1)}{n} \ldots + \boldsymbol{z}_{n-1} \sin\frac{2\pi\cdot 1\cdot(n-1)}{n} = 0 \\ \boldsymbol{z}_1 \sin\frac{2\pi\cdot 2\cdot 1}{n} + \cdots + \boldsymbol{z}_{\left\lceil\frac{n}{2}\right\rceil-1} \sin\frac{2\pi\cdot 2\cdot(\left\lceil\frac{n}{2}\right\rceil-1)}{n} + \boldsymbol{z}_{\left\lfloor\frac{n}{2}\right\rfloor+1} \sin\frac{2\pi\cdot 2\cdot(\left\lfloor\frac{n}{2}\right\rfloor+1)}{n} \ldots + \boldsymbol{z}_{n-1} \sin\frac{2\pi\cdot 2\cdot(n-1)}{n} = 0 \\ \cdots \\ \boldsymbol{z}_1 \sin\frac{2\pi\cdot(\left\lceil\frac{n}{2}\right\rceil-1)\cdot 1}{n} + \cdots + \boldsymbol{z}_{\left\lceil\frac{n}{2}\right\rceil-1} \sin\frac{2\pi\cdot(\left\lceil\frac{n}{2}\right\rceil-1)\cdot(\left\lceil\frac{n}{2}\right\rceil-1)}{n} + \boldsymbol{z}_{\left\lfloor\frac{n}{2}\right\rfloor+1} \sin\frac{2\pi\cdot(\left\lceil\frac{n}{2}\right\rceil-1)\cdot(\left\lfloor\frac{n}{2}\right\rfloor+1)}{n} \ldots + \boldsymbol{z}_{n-1} \sin\frac{2\pi\cdot\left(\left\lceil\frac{n}{2}\right\rceil-1\right)\cdot(n-1)}{n} = 0 \end{cases}$$

(9.8)

Note that $\sin\frac{2\pi k\cdot t}{n} = -\sin\frac{2\pi k\cdot(n-t)}{n}$ for every $0 \le k \le \left\lfloor\frac{n}{2}\right\rfloor$, and therefore the matrix of system (9.8) possesses a special kind of anti-symmetry: the first column is equal to the negative of the last column, the second column is equal to the negative of the one just before last, and so on. Because every equation in (9.8) has an even number of summands, after re-arranging the mutually negative sines together, (9.8) can be written as

$$\begin{cases} (\boldsymbol{z}_1 - \boldsymbol{z}_{n-1}) \sin\frac{2\pi\cdot 1\cdot 1}{n} + \cdots + (\boldsymbol{z}_{\left\lceil\frac{n}{2}\right\rceil-1} - \boldsymbol{z}_{\left\lfloor\frac{n}{2}\right\rfloor+1}) \sin\frac{2\pi\cdot 1\cdot(\left\lceil\frac{n}{2}\right\rceil-1)}{n} = 0 \\ (\boldsymbol{z}_1 - \boldsymbol{z}_{n-1}) \sin\frac{2\pi\cdot 2\cdot 1}{n} + \cdots + (\boldsymbol{z}_{\left\lceil\frac{n}{2}\right\rceil-1} - \boldsymbol{z}_{\left\lfloor\frac{n}{2}\right\rfloor+1}) \sin\frac{2\pi\cdot 2\cdot(\left\lceil\frac{n}{2}\right\rceil-1)}{n} = 0 \\ \cdots \\ (\boldsymbol{z}_1 - \boldsymbol{z}_{n-1}) \sin\frac{2\pi\cdot(\left\lceil\frac{n}{2}\right\rceil-1)\cdot 1}{n} + \cdots + (\boldsymbol{z}_{\left\lceil\frac{n}{2}\right\rceil-1} - \boldsymbol{z}_{\left\lfloor\frac{n}{2}\right\rfloor+1}) \sin\frac{2\pi\cdot(\left\lceil\frac{n}{2}\right\rceil-1)\cdot(\left\lceil\frac{n}{2}\right\rceil-1)}{n} = 0 \end{cases}$$

and, after substitution of variables $\boldsymbol{x}_1 = \boldsymbol{z}_1 - \boldsymbol{z}_{n-1}, \ldots, \boldsymbol{x}_{\left\lceil\frac{n}{2}\right\rceil-1} = \boldsymbol{z}_{\left\lceil\frac{n}{2}\right\rceil-1} + \boldsymbol{z}_{\left\lfloor\frac{n}{2}\right\rfloor+1}$, we have

$$\begin{cases} \boldsymbol{x}_1 \sin\frac{2\pi\cdot 1\cdot 1}{n} + \cdots + \boldsymbol{x}_{\lceil\frac{n}{2}\rceil-1} \sin\frac{2\pi\cdot 1\cdot(\lceil\frac{n}{2}\rceil-1)}{n} = 0 \\ \boldsymbol{x}_1 \sin\frac{2\pi\cdot 2\cdot 1}{n} + \cdots + \boldsymbol{x}_{\lceil\frac{n}{2}\rceil-1} \sin\frac{2\pi\cdot 2\cdot(\lceil\frac{n}{2}\rceil-1)}{n} = 0 \\ \cdots \\ \boldsymbol{x}_1 \sin\frac{2\pi\cdot(\lceil\frac{n}{2}\rceil-1)\cdot 1}{n} + \cdots + \boldsymbol{x}_{\lceil\frac{n}{2}\rceil-1} \sin\frac{2\pi\cdot(\lceil\frac{n}{2}\rceil-1)\cdot(\lceil\frac{n}{2}\rceil-1)}{n} = 0 \end{cases} \tag{9.9}$$

Since the $\left(\left\lceil\frac{n}{2}\right\rceil - 1\right) \times \left(\left\lceil\frac{n}{2}\right\rceil - 1\right)$ matrix of system (9.9) has been obtained by elimination of $\left\lfloor\frac{n}{2}\right\rfloor + 1$ 'negative-twin' and zero columns in the $\left(\left\lceil\frac{n}{2}\right\rceil - 1\right) \times n$ matrix of system (9.8), which has rank $\left\lceil\frac{n}{2}\right\rceil - 1$, the matrix of system (9.9) is also of rank $\left\lceil\frac{n}{2}\right\rceil - 1$. Then, the matrix of system (9.9) is non-singular, and therefore invertible. It is known (Zhang [98], Theorem 4.3) that if a quaternion matrix $\boldsymbol{A}$ is invertible then the equation $\boldsymbol{A}\boldsymbol{x} = 0$ has a unique solution over $\mathbb{H}^n$. Therefore, system (9.9) has exactly one solution in $\mathbb{H}^n$, namely $\boldsymbol{x} = 0$.

Thus, $\boldsymbol{x}_1 = \boldsymbol{x}_2 = \cdots = \boldsymbol{x}_{\lceil\frac{n}{2}\rceil-1} = 0$ is the unique solution of the system (9.9).

Therefore, 0$= \boldsymbol{z}_1 - \boldsymbol{z}_{n-1}, \dots, 0 = \boldsymbol{z}_{\lceil\frac{n}{2}\rceil-1} + \boldsymbol{z}_{\lfloor\frac{n}{2}\rfloor+1}$, and

$$\boldsymbol{z}_1 = \boldsymbol{z}_{n-1},\ \boldsymbol{z}_2 = \boldsymbol{z}_{n-2}, \dots, \boldsymbol{z}_{\lceil\frac{n}{2}\rceil-1} = \boldsymbol{z}_{\lfloor\frac{n}{2}\rfloor+1}$$

is the unique solution of system (9.6). As it has been shown above, $\boldsymbol{z}_0$ and, if n is even, $\boldsymbol{z}_{\frac{n}{2}}$ can be chosen as arbitrary quaternions.

This completes the proof of Lemma 9.8. □

<u>Lemma 9.9</u> Let $\boldsymbol{x} = x_0 + x_1\boldsymbol{i} + x_2\boldsymbol{j} + x_3\boldsymbol{k}$ be an arbitrary real quaternion. Then

$$\boldsymbol{x}^*\boldsymbol{i}\boldsymbol{x} = (x_0^2 + x_1^2 - x_2^2 - x_3^2)\boldsymbol{i} + 2(-x_0x_3 + x_1x_2)\boldsymbol{j} + 2(x_0x_2 + x_1x_3)\boldsymbol{k}$$

<u>Proof.</u> $\boldsymbol{x}^*\boldsymbol{i}\boldsymbol{x} = (x_0 - x_1\boldsymbol{i} - x_2\boldsymbol{j} - x_3\boldsymbol{k})\boldsymbol{i}(x_0 + x_1\boldsymbol{i} + x_2\boldsymbol{j} + x_3\boldsymbol{k})$

$$= (x_0\boldsymbol{i} + x_1 + x_2\boldsymbol{k} - x_3\boldsymbol{j})(x_0 + x_1\boldsymbol{i} + x_2\boldsymbol{j} + x_3\boldsymbol{k})$$

$$= x_0^2\boldsymbol{i} + x_0x_1 + x_0x_2\boldsymbol{k} - x_0x_3\boldsymbol{j} - x_0x_1 + x_1^2\boldsymbol{i} + x_1x_2\boldsymbol{j} + x_1x_3\boldsymbol{k} + x_0x_2\boldsymbol{k} + x_1x_2\boldsymbol{j} - x_2^2\boldsymbol{i} - x_2x_3 - x_0x_3\boldsymbol{j} + x_1x_3\boldsymbol{k} + x_2x_3 - x_3^2\boldsymbol{i}$$

$$= (x_0x_1 - x_0x_1 - x_2x_3 + x_2x_3) + (x_0^2 + x_1^2 - x_2^2 - x_3^2)\boldsymbol{i} + (-x_0x_3 + x_1x_2 + x_1x_2 - x_0x_3)\boldsymbol{j} + (x_0x_2 + x_1x_3 + x_0x_2 + x_1x_3)\boldsymbol{k}$$

$$= (x_0^2 + x_1^2 - x_2^2 - x_3^2)\boldsymbol{i} + 2(-x_0x_3 + x_1x_2)\boldsymbol{j} + 2(x_0x_2 + x_1x_3)\boldsymbol{k} \, \square$$

<u>Lemma 9.10</u> Let $\boldsymbol{x}$ and $\boldsymbol{y}$ be arbitrary quaternions. If $\boldsymbol{x}^*\boldsymbol{i}\boldsymbol{x} = \boldsymbol{y}^*\boldsymbol{i}\boldsymbol{y}$, then $\|\boldsymbol{x}\| = \|\boldsymbol{y}\|$.

<u>Proof.</u>

$$\boldsymbol{x}^*\boldsymbol{i}\boldsymbol{x} = \boldsymbol{y}^*\boldsymbol{i}\boldsymbol{y} \;\Rightarrow\; (\boldsymbol{x}^*\boldsymbol{i}\boldsymbol{x})^2 = (\boldsymbol{y}^*\boldsymbol{i}\boldsymbol{y})^2$$

$$\Rightarrow\; \boldsymbol{x}^*\boldsymbol{i}\boldsymbol{x}\boldsymbol{x}^*\boldsymbol{i}\boldsymbol{x} = \boldsymbol{y}^*\boldsymbol{i}\boldsymbol{y}\boldsymbol{y}^*\boldsymbol{i}\boldsymbol{y}$$

$$\Rightarrow\; \boldsymbol{x}^*\boldsymbol{i}\|\boldsymbol{x}\|\boldsymbol{i}\boldsymbol{x} = \boldsymbol{y}^*\boldsymbol{i}\|\boldsymbol{y}\|\boldsymbol{i}\boldsymbol{y}$$

$$\Rightarrow \|\boldsymbol{x}\|\boldsymbol{x}^*\boldsymbol{i}^2\boldsymbol{x} = \|\boldsymbol{y}\|\boldsymbol{y}^*\boldsymbol{i}^2\boldsymbol{y}$$

$$\Rightarrow -\|\boldsymbol{x}\|\boldsymbol{x}^*\boldsymbol{x} = -\|\boldsymbol{y}\|\boldsymbol{y}^*\boldsymbol{y}$$

$$\Rightarrow -\|\boldsymbol{x}\|^2 = -\|\boldsymbol{y}\|^2$$

$$\Rightarrow\; \|\boldsymbol{x}\| = \|\boldsymbol{y}\|. \;\square$$

9.6. Proof of the Main Result

We are now in the position to prove the main result of Part 9, Proposition 9.3.

<u>Proof of Proposition 9.3</u> We append the set of equations (9.1), defining perfection of a sequence $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$, by one more equation, namely

$$\langle \boldsymbol{a}^T, \boldsymbol{a}^T \rangle = \sum_{t=0}^{n-1} \boldsymbol{a}_t^* \boldsymbol{a}_t = \sum_{t=0}^{n-1} \|\boldsymbol{a}_t\| = \|\boldsymbol{a}\|$$

As $C^n = I$, we can rewrite the above equation as $\langle \boldsymbol{a}^T, \boldsymbol{a}^T \rangle = \langle \boldsymbol{a}^T, I\boldsymbol{a}^T \rangle = \langle \boldsymbol{a}^T, C^n\boldsymbol{a}^T \rangle = \|\boldsymbol{a}\|$.

Therefore, a sequence $\boldsymbol{a}$ over the real quaternions is perfect if and only if

$$\langle \boldsymbol{a}^T, C^m\boldsymbol{a}^T \rangle = 0$$

for every $m, 1 \le m \le n-1$ and

$$\langle \boldsymbol{a}^T, C^n\boldsymbol{a}^T \rangle = \|\boldsymbol{a}\| \tag{9.1a}$$

Consider the equation $\langle \boldsymbol{a}^T, C^m\boldsymbol{a}^T \rangle = 0$. By Lemma 9.3, matrix C^m is diagonalizable by the unitary matrix U, where U is defined in Lemma 9.2. That is, $D^m = U^\dagger C^m U$, where D is a diagonal form of the matrix C. Then,

$$D^m = U^\dagger C^m U \iff C^m = UD^mU^\dagger$$

Using the results of Lemma 9.4 and making the substitution $\boldsymbol{y} = U^\dagger \boldsymbol{a}^T$, we transform the equation $\langle \boldsymbol{a}^T, C^m\boldsymbol{a}^T \rangle = 0$ as follows:

$$0 = \langle \boldsymbol{a}^T, C^m\boldsymbol{a}^T \rangle = \langle \boldsymbol{a}^T, UD^mU^\dagger\boldsymbol{a}^T \rangle = \langle U^\dagger\boldsymbol{a}^T, D^mU^\dagger\boldsymbol{a}^T \rangle = \langle U^\dagger\boldsymbol{a}^T, D^m(U^\dagger\boldsymbol{a}^T) \rangle = \langle \boldsymbol{y}, D^m\boldsymbol{y} \rangle$$

Note that, by definition, $\boldsymbol{y}$ is a column vector rather than a sequence. All its components $\boldsymbol{y}_0, \boldsymbol{y}_1, \dots, \boldsymbol{y}_{n-1}$ are quaternions. With such defined $\boldsymbol{y}$, our primary goal is to prove that $\|\boldsymbol{y}_0\| = \|\boldsymbol{y}_1\| = \cdots = \|\boldsymbol{y}_{n-1}\| = \frac{\|\boldsymbol{a}\|}{n}$.

Continue the equality above:

$$0=\langle \boldsymbol{y},D^m\boldsymbol{y}\rangle=\langle\begin{bmatrix}\boldsymbol{y}_0\\ \boldsymbol{y}_1\\ \vdots\\ \boldsymbol{y}_{n-1}\end{bmatrix},\begin{bmatrix}\omega^0 & 0 & \dots & 0\\ 0 & \omega^1 & & \vdots\\ \vdots & & \ddots & 0\\ 0 & \dots & 0 & \omega^{n-1}\end{bmatrix}^m\begin{bmatrix}\boldsymbol{y}_0\\ \boldsymbol{y}_1\\ \vdots\\ \boldsymbol{y}_{n-1}\end{bmatrix}\rangle$$

$$=\langle\begin{bmatrix}\boldsymbol{y}_0\\ \boldsymbol{y}_1\\ \vdots\\ \boldsymbol{y}_{n-1}\end{bmatrix},\begin{bmatrix}(\omega^0)^m & 0 & \dots & 0\\ 0 & (\omega^1)^m & & \vdots\\ \vdots & & \ddots & 0\\ 0 & \dots & 0 & (\omega^{n-1})^m\end{bmatrix}\begin{bmatrix}\boldsymbol{y}_0\\ \boldsymbol{y}_1\\ \vdots\\ \boldsymbol{y}_{n-1}\end{bmatrix}\rangle$$

$$=\langle\begin{bmatrix}\boldsymbol{y}_0\\ \boldsymbol{y}_1\\ \vdots\\ \boldsymbol{y}_{n-1}\end{bmatrix},\begin{bmatrix}(\omega^0)^m\boldsymbol{y}_0\\ (\omega^1)^m\boldsymbol{y}_1\\ \vdots\\ (\omega^{n-1})^m\boldsymbol{y}_{n-1}\end{bmatrix}\rangle=\sum_{t=0}^{n-1}\boldsymbol{y}_t^*\omega^{tm}\boldsymbol{y}_t$$

Each ω^{tm} denotes an n-th root of unity, a complex number, and we write

$\omega^{tm}=\mathrm{Re}(\omega^{tm})+\boldsymbol{i}\mathrm{Im}(\omega^{tm})$, where $\mathrm{Re}(\omega^{tm})$ and $\mathrm{Im}(\omega^{tm})$, the real and imaginary parts, are real numbers.

Therefore, the equality continues

$$=\sum_{t=0}^{n-1}\boldsymbol{y}_t^*\big(\mathrm{Re}(\omega^{tm})+\boldsymbol{i}\mathrm{Im}(\omega^{tm})\big)\boldsymbol{y}_t=\sum_{t=0}^{n-1}\boldsymbol{y}_t^*\mathrm{Re}(\omega^{tm})\boldsymbol{y}_t+\sum_{t=0}^{n-1}\boldsymbol{y}_t^*\boldsymbol{i}\mathrm{Im}(\omega^{tm})\boldsymbol{y}_t$$

Real numbers commute with all quaternions (Zhang [98], Theorem 2.1), and so the equality continues

$$=\sum_{t=0}^{n-1}\mathrm{Re}(\omega^{tm})\boldsymbol{y}_t^*\boldsymbol{y}_t+\sum_{t=0}^{n-1}\mathrm{Im}(\omega^{tm})\boldsymbol{y}_t^*\boldsymbol{i}\boldsymbol{y}_t=\sum_{t=0}^{n-1}\mathrm{Re}(\omega^{tm})\|\boldsymbol{y}_t\|+\sum_{t=0}^{n-1}\mathrm{Im}(\omega^{tm})\boldsymbol{y}_t^*\boldsymbol{i}\boldsymbol{y}_t$$

Thus,

$$\sum_{t=0}^{n-1}\mathrm{Re}(\omega^{tm})\|\boldsymbol{y}_t\|+\sum_{t=0}^{n-1}\mathrm{Im}(\omega^{tm})\boldsymbol{y}_t^*\boldsymbol{i}\boldsymbol{y}_t=0 \tag{9.10}$$

The left hand side of equation (9.10), being a real quaternion, represents the sum of two terms. The first term, $\sum_{t=0}^{n-1}\mathrm{Re}(\omega^{tm})\|\boldsymbol{y}_t\|$, is a real number. The second term is the summation of n

products of the form $r\boldsymbol{x}^*\boldsymbol{ix}$, where r is a real number, $\boldsymbol{x}$ is a real quaternion and $\boldsymbol{i}$ is the imaginary unit in $\mathbb{C}$. By Lemma 9.10, a product of the form $\boldsymbol{x}^*\boldsymbol{ix}$ is always a pure quaternion (that is, a quaternion with zero real part). Then, $r\boldsymbol{x}^*\boldsymbol{ix}$ is a pure quaternion too. Thus, the first and the second terms in the left hand side of equation (9.10) represent the real and imaginary parts of the sum respectively.

Because a quaternion is equal to zero if and only if its real and imaginary parts are both equal to zero, equation (9.10) implies that

$$\sum_{t=0}^{n-1} \mathrm{Re}(\omega^{tm})\|\boldsymbol{y}_t\| = 0$$

(9.11)

If we chose $m = n$ and apply the same chain of transformations as above to the equation $\langle \boldsymbol{a}^T, C^n\boldsymbol{a}^T\rangle = \|\boldsymbol{a}\|$, we have

$$\sum_{t=0}^{n-1} \mathrm{Re}(\omega^{tn})\|\boldsymbol{y}_t\| = \langle \boldsymbol{a}^T, C^n\boldsymbol{a}^T\rangle = \|\boldsymbol{a}\|$$

(9.12)

Combining equations (9.11) and (9.12) together, we have the following system of linear equations in variables $\|\boldsymbol{y}_0\|,\ldots,\|\boldsymbol{y}_{n-1}\|$:

$$\begin{cases} \mathrm{Re}(\omega^0)\|\boldsymbol{y}_0\| + \mathrm{Re}(\omega^1)\|\boldsymbol{y}_1\| + \mathrm{Re}(\omega^2)\|\boldsymbol{y}_2\| + \cdots + \mathrm{Re}(\omega^{n-1})\|\boldsymbol{y}_{n-1}\| = 0 \\ \mathrm{Re}(\omega^{0\cdot 2})\|\boldsymbol{y}_0\| + \mathrm{Re}(\omega^{1\cdot 2})\|\boldsymbol{y}_1\| + \mathrm{Re}(\omega^{2\cdot 2})\|\boldsymbol{y}_2\| + \cdots + \mathrm{Re}\left(\omega^{(n-1)\cdot 2}\right)\|\boldsymbol{y}_{n-1}\| = 0 \\ \mathrm{Re}(\omega^{0\cdot 3})\|\boldsymbol{y}_0\| + \mathrm{Re}(\omega^{1\cdot 3})\|\boldsymbol{y}_1\| + \mathrm{Re}(\omega^{2\cdot 3})\|\boldsymbol{y}_2\| + \cdots + \mathrm{Re}\left(\omega^{(n-1)\cdot 3}\right)\|\boldsymbol{y}_{n-1}\| = 0 \\ \cdots \\ \mathrm{Re}\left(\omega^{0\cdot(n-1)}\right)\|\boldsymbol{y}_0\| + \mathrm{Re}\left(\omega^{1\cdot(n-1)}\right)\|\boldsymbol{y}_1\| + \mathrm{Re}\left(\omega^{2\cdot(n-1)}\right)\|\boldsymbol{y}_2\| + \cdots + \mathrm{Re}\left(\omega^{(n-1)\cdot(n-1)}\right)\|\boldsymbol{y}_{n-1}\| = 0 \\ \mathrm{Re}(\omega^{0\cdot n})\|\boldsymbol{y}_0\| + \mathrm{Re}(\omega^{1\cdot n})\|\boldsymbol{y}_1\| + \mathrm{Re}(\omega^{2\cdot n})\|\boldsymbol{y}_2\| + \cdots + \mathrm{Re}\left(\omega^{(n-1)\cdot n}\right)\|\boldsymbol{y}_{n-1}\| = \|\boldsymbol{a}\| \end{cases}$$

(9.13)

The principal n-th root of unity is expressed by the Euler's formula (Abramowitz and Stegun [1], p. 74) as $\omega = e^{\boldsymbol{i}\frac{2\pi}{n}} = \cos\frac{2\pi}{n} + \boldsymbol{i}\sin\frac{2\pi}{n}$.

The powers of the principal root are, by the De Moivre’s Theorem (Abramowitz and Stegun [1], p. 74), $\omega^t = \left(e^{\boldsymbol{i}\frac{2\pi}{n}}\right)^t = e^{\boldsymbol{i}\frac{2\pi t}{n}} = \cos\frac{2\pi t}{n} + \boldsymbol{i}\sin\frac{2\pi t}{n}$.

It is clear that $\mathrm{Re}(\omega^t) = \cos\frac{2\pi t}{n}$, therefore (9.13) can be written as

$$\begin{cases} \cos\frac{2\pi\cdot 1\cdot 0}{n}\|\boldsymbol{y}_0\| + \cos\frac{2\pi\cdot 1\cdot 1}{n}\|\boldsymbol{y}_1\| + \cos\frac{2\pi\cdot 1\cdot 2}{n}\|\boldsymbol{y}_2\| + \cdots + \cos\frac{2\pi\cdot 1\cdot(n-1)}{n}\|\boldsymbol{y}_{n-1}\| = 0 \\ \cos\frac{2\pi\cdot 2\cdot 0}{n}\|\boldsymbol{y}_0\| + \cos\frac{2\pi\cdot 2\cdot 1}{n}\|\boldsymbol{y}_1\| + \cos\frac{2\pi\cdot 2\cdot 2}{n}\|\boldsymbol{y}_2\| + \cdots + \cos\frac{2\pi\cdot 2\cdot(n-1)}{n}\|\boldsymbol{y}_{n-1}\| = 0 \\ \cos\frac{2\pi\cdot 3\cdot 0}{n}\|\boldsymbol{y}_0\| + \cos\frac{2\pi\cdot 3\cdot 1}{n}\|\boldsymbol{y}_1\| + \cos\frac{2\pi\cdot 3\cdot 2}{n}\|\boldsymbol{y}_2\| + \cdots + \cos\frac{2\pi\cdot 3\cdot(n-1)}{n}\|\boldsymbol{y}_{n-1}\| = 0 \\ \cdots \\ \cos\frac{2\pi\cdot(n-1)\cdot 0}{n}\|\boldsymbol{y}_0\| + \cos\frac{2\pi\cdot(n-1)\cdot 1}{n}\|\boldsymbol{y}_1\| + \cos\frac{2\pi\cdot(n-1)\cdot 2}{n}\|\boldsymbol{y}_2\| + \cdots + \cos\frac{2\pi\cdot(n-1)\cdot(n-1)}{n}\|\boldsymbol{y}_{n-1}\| = 0 \\ \cos\frac{2\pi\cdot n\cdot 0}{n}\|\boldsymbol{y}_0\| + \cos\frac{2\pi\cdot n\cdot 1}{n}\|\boldsymbol{y}_1\| + \cos\frac{2\pi\cdot n\cdot 2}{n}\|\boldsymbol{y}_2\| + \cdots + \cos\frac{2\pi\cdot n\cdot(n-1)}{n}\|\boldsymbol{y}_{n-1}\| = \|\boldsymbol{a}\| \end{cases}$$

(9.14)

Since every cosine in the first term of each equation of system (9.14), as well as every cosine in the last equation, are equal to 1, system (9.14) is equivalent to

$$\begin{cases} \|\boldsymbol{y}_0\| + \|\boldsymbol{y}_1\| + \|\boldsymbol{y}_2\| + \cdots + \|\boldsymbol{y}_{n-1}\| = \|\boldsymbol{a}\| \\ \|\boldsymbol{y}_0\| + \cos\frac{2\pi\cdot 1\cdot 1}{n}\|\boldsymbol{y}_1\| + \cos\frac{2\pi\cdot 1\cdot 2}{n}\|\boldsymbol{y}_2\| + \cdots + \cos\frac{2\pi\cdot 1\cdot(n-1)}{n}\|\boldsymbol{y}_{n-1}\| = 0 \\ \|\boldsymbol{y}_0\| + \cos\frac{2\pi\cdot 2\cdot 1}{n}\|\boldsymbol{y}_1\| + \cos\frac{2\pi\cdot 2\cdot 2}{n}\|\boldsymbol{y}_2\| + \cdots + \cos\frac{2\pi\cdot 2\cdot(n-1)}{n}\|\boldsymbol{y}_{n-1}\| = 0 \\ \cdots \\ \|\boldsymbol{y}_0\| + \cos\frac{2\pi\cdot(n-2)\cdot 1}{n}\|\boldsymbol{y}_1\| + \cos\frac{2\pi\cdot(n-2)\cdot 2}{n}\|\boldsymbol{y}_2\| + \cdots + \cos\frac{2\pi\cdot(n-2)\cdot(n-1)}{n}\|\boldsymbol{y}_{n-1}\| = 0 \\ \|\boldsymbol{y}_0\| + \cos\frac{2\pi\cdot(n-1)\cdot 1}{n}\|\boldsymbol{y}_1\| + \cos\frac{2\pi\cdot(n-1)\cdot 2}{n}\|\boldsymbol{y}_2\| + \cdots + \cos\frac{2\pi\cdot(n-1)\cdot(n-1)}{n}\|\boldsymbol{y}_{n-1}\| = 0 \end{cases}$$

(9.15)

If we regard (9.15) as simultaneous linear equations in $\|\boldsymbol{y}_0\|, \|\boldsymbol{y}_1\|, \dots, \|\boldsymbol{y}_{n-1}\|$, the matrix of this system will be

$$R_{cos} = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & \cos\frac{2\pi\cdot 1}{n} & \cos\frac{2\pi\cdot 2}{n} & \dots & \cos\frac{2\pi\cdot(n-2)}{n} & \cos\frac{2\pi\cdot(n-1)}{n} \\ 1 & \cos\frac{2\pi\cdot 2\cdot 1}{n} & \cos\frac{2\pi\cdot 2\cdot 2}{n} & \dots & \cos\frac{2\pi\cdot 2\cdot(n-2)}{n} & \cos\frac{2\pi\cdot 2\cdot(n-1)}{n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \cos\frac{2\pi\cdot(n-2)\cdot 1}{n} & \cos\frac{2\pi\cdot(n-2)\cdot 2}{n} & \dots & \cos\frac{2\pi\cdot(n-2)\cdot(n-2)}{n} & \cos\frac{2\pi\cdot(n-2)\cdot(n-1)}{n} \\ 1 & \cos\frac{2\pi\cdot(n-1)\cdot 1}{n} & \cos\frac{2\pi\cdot(n-1)\cdot 2}{n} & \cdots & \cos\frac{2\pi\cdot(n-1)\cdot(n-2)}{n} & \cos\frac{2\pi\cdot(n-1)\cdot(n-1)}{n} \end{bmatrix}.$$

By Lemma 9.7, the general solution for (9.15) is

$\|\boldsymbol{y}_0\| = \frac{\|\boldsymbol{a}\|}{n},\ \|\boldsymbol{y}_1\| + \|\boldsymbol{y}_{n-1}\| = \frac{2\|\boldsymbol{a}\|}{n}, \dots ,\ \left\|\boldsymbol{y}_{\frac{n}{2}-1}\right\| + \left\|\boldsymbol{y}_{\frac{n}{2}+1}\right\| = \frac{2\|\boldsymbol{a}\|}{n}, \left\|\boldsymbol{y}_{\frac{n}{2}}\right\| = \frac{\|\boldsymbol{a}\|}{n}$, if n even;

$\|\boldsymbol{y}_0\| = \frac{\|\boldsymbol{a}\|}{n},\ \|\boldsymbol{y}_1\| + \|\boldsymbol{y}_{n-1}\| = \frac{2\|\boldsymbol{a}\|}{n}, \dots ,\ \left\|\boldsymbol{y}_{\left\lfloor\frac{n}{2}\right\rfloor}\right\| + \left\|\boldsymbol{y}_{\left\lceil\frac{n}{2}\right\rceil}\right\| = \frac{2\|\boldsymbol{a}\|}{n}$, if n odd.

(9.16)

We will show that $\|\boldsymbol{y}_t\| = \|\boldsymbol{y}_{n-t}\|$, for all $1 \le t \le \left\lceil\frac{n}{2}\right\rceil - 1$.

Consider equation (9.10) again. As it was already mentioned, the second term in the left hand side of this equation, $\sum_{t=0}^{n-1} \mathrm{Im}(\omega^{tm})\boldsymbol{y}_t^*\boldsymbol{i}\boldsymbol{y}_t$, is the imaginary part of a quaternion, which is equal to zero.

This implies that

$$\sum_{t=0}^{n-1} \mathrm{Im}(\omega^{tm})\boldsymbol{y}_t^*\boldsymbol{i}\boldsymbol{y}_t = 0$$

(9.17)

Equation (9.17) holds for all $m, 1 \le m \le n$. So, we can construct a system:

$$\begin{cases} \mathrm{Im}(\omega^{0})\boldsymbol{y}_0^*\boldsymbol{i}\boldsymbol{y}_0 + \mathrm{Im}(\omega^{1})\boldsymbol{y}_1^*\boldsymbol{i}\boldsymbol{y}_1 + \cdots + \mathrm{Im}(\omega^{n-1})\boldsymbol{y}_{n-1}^*\boldsymbol{i}\boldsymbol{y}_{n-1} = 0 \\ \mathrm{Im}(\omega^{0\cdot 2})\boldsymbol{y}_0^*\boldsymbol{i}\boldsymbol{y}_0 + \mathrm{Im}(\omega^{1\cdot 2})\boldsymbol{y}_1^*\boldsymbol{i}\boldsymbol{y}_1 + \cdots + \mathrm{Im}\left(\omega^{(n-1)\cdot 2}\right)\boldsymbol{y}_{n-1}^*\boldsymbol{i}\boldsymbol{y}_{n-1} = 0 \\ \mathrm{Im}(\omega^{0\cdot 3})\boldsymbol{y}_0^*\boldsymbol{i}\boldsymbol{y}_0 + \mathrm{Im}(\omega^{1\cdot 3})\boldsymbol{y}_1^*\boldsymbol{i}\boldsymbol{y}_1 + \cdots + \mathrm{Im}\left(\omega^{(n-1)\cdot 3}\right)\boldsymbol{y}_{n-1}^*\boldsymbol{i}\boldsymbol{y}_{n-1} = 0 \\ \cdots \\ \mathrm{Im}\left(\omega^{0\cdot(n-1)}\right)\boldsymbol{y}_0^*\boldsymbol{i}\boldsymbol{y}_0 + \mathrm{Im}\left(\omega^{1\cdot(n-1)}\right)\boldsymbol{y}_1^*\boldsymbol{i}\boldsymbol{y}_1 + \cdots + \mathrm{Im}\left(\omega^{(n-1)\cdot(n-1)}\right)\boldsymbol{y}_{n-1}^*\boldsymbol{i}\boldsymbol{y}_{n-1} = 0 \\ \mathrm{Im}(\omega^{0\cdot n})\boldsymbol{y}_0^*\boldsymbol{i}\boldsymbol{y}_0 + \mathrm{Im}(\omega^{1\cdot n})\boldsymbol{y}_1^*\boldsymbol{i}\boldsymbol{y}_1 + \cdots + \mathrm{Im}\left(\omega^{(n-1)\cdot n}\right)\boldsymbol{y}_{n-1}^*\boldsymbol{i}\boldsymbol{y}_{n-1} = 0 \end{cases}$$

(9.18)

Using the Euler formula $\omega^t = \cos\frac{2\pi t}{n} + \boldsymbol{i}\sin\frac{2\pi t}{n}$, and moving the last equation on the top, we transform system (9.18) into

$$\begin{cases} \sin\frac{2\pi\cdot 0\cdot 0}{n}\boldsymbol{y}_0^*\boldsymbol{i}\boldsymbol{y}_0 + \sin\frac{2\pi\cdot 0\cdot 1}{n}\boldsymbol{y}_1^*\boldsymbol{i}\boldsymbol{y}_1 + \cdots + \sin\frac{2\pi\cdot 0\cdot (n-1)}{n}\boldsymbol{y}_{n-1}^*\boldsymbol{i}\boldsymbol{y}_{n-1} = 0 \\ \sin\frac{2\pi\cdot 1\cdot 0}{n}\boldsymbol{y}_0^*\boldsymbol{i}\boldsymbol{y}_0 + \sin\frac{2\pi\cdot 1\cdot 1}{n}\boldsymbol{y}_1^*\boldsymbol{i}\boldsymbol{y}_1 + \cdots + \sin\frac{2\pi\cdot 1\cdot (n-1)}{n}\boldsymbol{y}_{n-1}^*\boldsymbol{i}\boldsymbol{y}_{n-1} = 0 \\ \sin\frac{2\pi\cdot 2\cdot 0}{n}\boldsymbol{y}_0^*\boldsymbol{i}\boldsymbol{y}_0 + \sin\frac{2\pi\cdot 2\cdot 1}{n}\boldsymbol{y}_1^*\boldsymbol{i}\boldsymbol{y}_1 + \cdots + \sin\frac{2\pi\cdot 2\cdot (n-1)}{n}\boldsymbol{y}_{n-1}^*\boldsymbol{i}\boldsymbol{y}_{n-1} = 0 \\ \cdots \\ \sin\frac{2\pi\cdot (n-2)\cdot 0}{n}\boldsymbol{y}_0^*\boldsymbol{i}\boldsymbol{y}_0 + \sin\frac{2\pi\cdot (n-2)\cdot 1}{n}\boldsymbol{y}_1^*\boldsymbol{i}\boldsymbol{y}_1 + \cdots + \sin\frac{2\pi\cdot (n-2)\cdot (n-1)}{n}\boldsymbol{y}_{n-1}^*\boldsymbol{i}\boldsymbol{y}_{n-1} = 0 \\ \sin\frac{2\pi\cdot (n-1)\cdot 0}{n}\boldsymbol{y}_0^*\boldsymbol{i}\boldsymbol{y}_0 + \sin\frac{2\pi\cdot (n-1)\cdot 1}{n}\boldsymbol{y}_1^*\boldsymbol{i}\boldsymbol{y}_1 + \cdots + \sin\frac{2\pi\cdot (n-1)\cdot (n-1)}{n}\boldsymbol{y}_{n-1}^*\boldsymbol{i}\boldsymbol{y}_{n-1} = 0 \end{cases} \tag{9.19}$$

By Lemma 9.8, if we assume $\boldsymbol{z}_0 = \boldsymbol{y}_0^*\boldsymbol{i}\boldsymbol{y}_0, \boldsymbol{z}_1 = \boldsymbol{y}_1^*\boldsymbol{i}\boldsymbol{y}_1, \dots, \boldsymbol{z}_{n-1} = \boldsymbol{y}_{n-1}^*\boldsymbol{i}\boldsymbol{y}_{n-1}$, the general solution for the system (9.19) is

$$\boldsymbol{y}_1^*\boldsymbol{i}\boldsymbol{y}_1 = \boldsymbol{y}_{n-1}^*\boldsymbol{i}\boldsymbol{y}_{n-1},\ \boldsymbol{y}_2^*\boldsymbol{i}\boldsymbol{y}_2 = \boldsymbol{y}_{n-2}^*\boldsymbol{i}\boldsymbol{y}_{n-2}, \dots, \boldsymbol{y}_{\lceil\frac{n}{2}\rceil-1}^*\boldsymbol{i}\boldsymbol{y}_{\lceil\frac{n}{2}\rceil-1} = \boldsymbol{y}_{\lfloor\frac{n}{2}\rfloor+1}^*\boldsymbol{i}\boldsymbol{y}_{\lfloor\frac{n}{2}\rfloor+1}.$$

Then, by Lemma 9.10,

$$\|\boldsymbol{y}_1\| = \|\boldsymbol{y}_{n-1}\|, \|\boldsymbol{y}_2\| = \|\boldsymbol{y}_{n-2}\|, \dots, \left\|\boldsymbol{y}_{\lceil\frac{n}{2}\rceil-1}\right\| = \left\|\boldsymbol{y}_{\lfloor\frac{n}{2}\rfloor+1}\right\| \tag{9.20}$$

Combination of (9.16) and (9.20) gives the desired identities

$$\|\boldsymbol{y}_0\| = \frac{\|\boldsymbol{a}\|}{n}, \|\boldsymbol{y}_1\| = \frac{\|\boldsymbol{a}\|}{n}, \dots, \|\boldsymbol{y}_{n-1}\| = \frac{\|\boldsymbol{a}\|}{n}$$

Thus, what we have proved so far is that if the sequence $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ is perfect, then the norm of each element $\boldsymbol{y}_t$ of the sequence $\boldsymbol{y} = U^\dagger\boldsymbol{a}^T$ is equal to $\frac{\|\boldsymbol{a}\|}{n}$.

Because $\boldsymbol{y} = U^\dagger\boldsymbol{a}^T$, expanding each $\boldsymbol{y}_t$, we have

$$\|\boldsymbol{y}_0\| = \left\|\frac{1}{\sqrt{n}}\sum_{t=0}^{n-1}(\omega^0)^{n-t}\boldsymbol{a}_t\right\| = \left\|\frac{1}{\sqrt{n}}\sum_{t=0}^{n-1}e^{\frac{2\pi i}{n}(n-t)\cdot 0}\boldsymbol{a}_t\right\| = \frac{1}{n}\left\|\sum_{t=0}^{n-1}\boldsymbol{a}_t\right\| = \frac{\|\boldsymbol{a}\|}{n}$$

$$\|\boldsymbol{y}_1\| = \left\|\frac{1}{\sqrt{n}}\sum_{t=0}^{n-1}(\omega^1)^{n-t}\boldsymbol{a}_t\right\| = \left\|\frac{1}{\sqrt{n}}\sum_{t=0}^{n-1}e^{\frac{2\pi i}{n}(n-t)\cdot 1}\boldsymbol{a}_t\right\| = \frac{1}{n}\left\|\sum_{t=0}^{n-1}e^{-\frac{2\pi i}{n}t}\boldsymbol{a}_t\right\| = \frac{\|\boldsymbol{a}\|}{n}$$

$$\|\boldsymbol{y}_2\| = \left\|\frac{1}{\sqrt{n}}\sum_{t=0}^{n-1}(\omega^2)^{n-t}\boldsymbol{a}_t\right\| = \left\|\frac{1}{\sqrt{n}}\sum_{t=0}^{n-1}e^{\frac{2\pi i}{n}(n-t)\cdot 2}\boldsymbol{a}_t\right\| = \frac{1}{n}\left\|\sum_{t=0}^{n-1}e^{-\frac{2\pi i}{n}2t}\boldsymbol{a}_t\right\| = \frac{\|\boldsymbol{a}\|}{n}$$

$$\dots$$

$$\|\boldsymbol{y}_{n-1}\| = \left\|\frac{1}{\sqrt{n}}\sum_{t=0}^{n-1}(\omega^{n-1})^{n-t}\boldsymbol{a}_t\right\| = \left\|\frac{1}{\sqrt{n}}\sum_{t=0}^{n-1}e^{\frac{2\pi i}{n}(n-t)\cdot(n-1)}\boldsymbol{a}_t\right\| = \frac{1}{n}\left\|\sum_{t=0}^{n-1}e^{-\frac{2\pi i}{n}(n-1)t}\boldsymbol{a}_t\right\| = \frac{\|\boldsymbol{a}\|}{n}$$

or

$$\left\{\begin{array}{c}\|\boldsymbol{A}_0^L\| = \|\boldsymbol{a}\| \\ \|\boldsymbol{A}_1^L\| = \|\boldsymbol{a}\| \\ \|\boldsymbol{A}_2^L\| = \|\boldsymbol{a}\| \\ \dots \\ \|\boldsymbol{A}_{n-1}^L\| = \|\boldsymbol{a}\|\end{array}\right. \tag{9.21}$$

So, we have proved Proposition 9.3 for the left discrete Fourier transform.

Now, since $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ is assumed perfect, its conjugate sequence $\boldsymbol{a}^* = [\boldsymbol{a}_0^*, \boldsymbol{a}_1^*, \dots, \boldsymbol{a}_{n-1}^*]$ is also perfect, by Corollary 5.1. It is clear that $\|\boldsymbol{a}^*\| = \|\boldsymbol{a}\|$. Applying the left discrete Fourier transform to the conjugate sequence $\boldsymbol{a}^*$, we have $\|[DFT^L(\boldsymbol{a}^*)]_s\| = \|\boldsymbol{a}^*\| = \|\boldsymbol{a}\|$. By Proposition 9.2, $[DFT^L(\boldsymbol{a}^*)]_s = [DFT^R(\boldsymbol{a})]_{n-s}^*$, for $0 \le s \le n-1$. Therefore, $\|\boldsymbol{a}\| = \|[DFT^L(\boldsymbol{a}^*)]_s\| = \|[DFT^R(\boldsymbol{a})]_{n-s}^*\| = \|[DFT^R(\boldsymbol{a})]_{n-s}\|$. Thus, for all t, $0 \le t \le n-1$,

$$\|[DFT^R(\boldsymbol{a})]_t\| = \|\boldsymbol{A}_t^R\| = \|\boldsymbol{a}\| \tag{9.22}$$

Combination of (9.21) and (9.22) gives the desired identities

$$\|\boldsymbol{A}_s^L\| = \|\boldsymbol{A}_s^R\| = \|\boldsymbol{a}\|$$

for $0 \le s \le n-1$. □

Corollary 9.5 Let $\boldsymbol{a} = [\boldsymbol{a}_0, \boldsymbol{a}_1, \dots, \boldsymbol{a}_{n-1}]$ be a perfect sequence over unit quaternions. Then, for $0 \leq s \leq n-1$,

$$\|\boldsymbol{A}_s^L\| = \|\boldsymbol{A}_s^R\| = n$$

where $\boldsymbol{A}_s^L = \sum_{t=0}^{n-1} e^{-\frac{2\pi i}{n}st}\boldsymbol{a}_t$ and $\boldsymbol{A}_s^R = \sum_{t=0}^{n-1} \boldsymbol{a}_t e^{-\frac{2\pi i}{n}st}$ denote the s-th left and right discrete Fourier transform coefficients respectively.

Proof. For sequences over unit quaternions, $\|\boldsymbol{a}\| = n$. □

Example 9.6 For the perfect sequence $\boldsymbol{a} = [\,1 + \boldsymbol{j}, 1, 0, -\boldsymbol{j}]$, as in Example 6.1, we have

$\|\boldsymbol{a}\| = \|1 + \boldsymbol{j}\| + \|1\| + \|0\| + \|-\boldsymbol{j}\| = 2 + 1 + 0 + 1 = 4$

$$\boldsymbol{A}^L = DFT^L([\,1 + \boldsymbol{j}, 1, 0, -\boldsymbol{j}]) = [\,2, 1 - \boldsymbol{i} + \boldsymbol{j} - \boldsymbol{k}, 2\boldsymbol{j}, 1 + \boldsymbol{i} + \boldsymbol{j} + \boldsymbol{k}]$$

$$\boldsymbol{A}^R = DFT^R([\,1 + \boldsymbol{j}, 1, 0, -\boldsymbol{j}]) = [\,2, 1 - \boldsymbol{i} + \boldsymbol{j} + \boldsymbol{k}, 2\boldsymbol{j}, 1 + \boldsymbol{i} + \boldsymbol{j} - \boldsymbol{k}]$$

It is easy to see that

$\|\boldsymbol{A}_0^L\| = \|2\| = 4 = \|\boldsymbol{a}\|$ $\quad$ $\|\boldsymbol{A}_0^R\| = \|2\| = 4 = \|\boldsymbol{a}\|$

$\|\boldsymbol{A}_1^L\| = \|1 - \boldsymbol{i} + \boldsymbol{j} - \boldsymbol{k}\| = 4 = \|\boldsymbol{a}\|$ $\quad$ $\|\boldsymbol{A}_1^R\| = \|1 - \boldsymbol{i} + \boldsymbol{j} + \boldsymbol{k}\| = 4 = \|\boldsymbol{a}\|$

$\|\boldsymbol{A}_2^L\| = \|2\boldsymbol{j}\| = 4 = \|\boldsymbol{a}\|$ $\quad$ $\|\boldsymbol{A}_2^R\| = \|2\boldsymbol{j}\| = 4 = \|\boldsymbol{a}\|$

$\|\boldsymbol{A}_3^L\| = \|1 + \boldsymbol{i} + \boldsymbol{j} + \boldsymbol{k}\| = 4 = \|\boldsymbol{a}\|$ $\quad$ $\|\boldsymbol{A}_3^R\| = \|1 + \boldsymbol{i} + \boldsymbol{j} - \boldsymbol{k}\| = 4 = \|\boldsymbol{a}\|$

10. Conclusion

In the present work, perfect sequences over the real quaternions have been introduced and their properties have been studied. Many examples of quaternionic perfect sequences, found by a computer search, are given in the text. Perfect sequences over the quaternions have never been considered in the literature in the past.

Due to non-commutativity of the quaternions, we define left and right autocorrelation functions, and give corresponding definitions of the left and right perfect sequences. A very important result, proved in Section 5, is that left and right perfection over the quaternions are equivalent.

Perfection over the quaternions can be regarded as a generalization of the concept of perfection over the complex numbers. In this text, it has been shown that quaternionic perfect sequences share many common properties with perfect sequences over the complex numbers. However, due to the non-commutative nature of the quaternions, some properties of perfect sequences over the complex numbers do not hold for perfect sequences over the quaternions. Table 10.1 below provides a brief summary in comparison of quaternionic and complex perfect sequences.

Table 10.1 Comparison chart for properties of perfect sequences over the complex numbers and over the real quaternions.

Property of a Sequence	Sequences over the Complex Numbers	Sequences over the Real Quaternions
Left and right perfections are equivalent	Yes	Yes
Multiplication of perfect sequence by a scalar preserves perfection	Yes	Yes, for left and right multiplications
Conjugate sequence of a perfect sequence is perfect	Yes	Yes
Any shift of a perfect sequence is perfect	Yes	Yes
A proper decimation of a perfect sequence is perfect	Yes	Yes
The Product Theorem for autocorrelation functions hold	Yes	No
The composition of perfect sequences of co-prime lengths is perfect	Yes	Yes
Perfection preserved by unitary transformations of the space to which elements of the perfect sequence belong	Yes	Yes
The Balance Theorem holds	Yes	Yes
The discrete Fourier transform of an arbitrary sequence with all elements of the same norm is perfect	Yes	No
A sequence obtained by multiplication of the elements of a perfect sequence of the length n by consecutive powers of an n-th root of unity is perfect	Yes	No
The norms of the discrete Fourier transform coefficients of a perfect sequence a are all equal to the norm of the sequence $\|a\|$	Yes, necessary and sufficient condition for perfection	Yes, necessary condition for perfection only
It is conjectured that the maximum possible length of a perfect sequence is limited by the size of an alphabet	Yes, for sequences over roots of unity	No

Although practical applications of quaternionic perfect sequences are not yet known, study of an algebraic structure and properties of quaternionic perfect sequences can provide for better understanding and advances in studying complex perfect sequences, which have an abundance of practical applications in many aspects of communication systems. Besides, perfect sequences over the real quaternions may have applications in the modern coherent fiber optics communication systems and free space microwave links.

11. Bibliography

[1] Abramowitz, M., Stegun, I.A., Handbook of Mathematical Functions: with Formulas, Graphs, and Mathematical Tables, Dover Publications, New York, N.Y. (1965)

[2] Alltop, W., Complex Sequences with Low Periodic Correlations, IEEE Transactions on Information Theory, Vol. 26, No. 3, pp. 350-354 (1980)

[3] Arasu, K.T., DeLauney, W., Ma, S.L., On Circulant Complex Hadamard Matrices, Designs, Codes and Cryptography, Vol. 25, pp. 123-142 (2002)

[4] Artmann, B., The Concept of Number: from Quaternions to Monads and Topological Fields, Halsted Press: a Division of John Willey and Sons, Chichester (1988)

[5] Aslaksen, H., Quaternionic Determinants, Mathematical Intelligencer, Vol. 18, No. 3, pp. 57-65 (1996)

[6] Baez, J.C., On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry by John H. Conway and Derek A. Smith, Bulletin of the American Mathematical Society (New Series), Vol. 42, pp. 229-243 (2005)

[7] Barbe, A., Skordev, G., Decimation-Invariant Sequences and Their Automaticity, Theoretical Computer Science, Vol. 259, pp. 379-403 (2001)

[8] Barnett, S., Matrices: Methods and Applications, Oxford Applied Mathematics and Computing Science Series, Oxford University Press (1990)

[9] Baumert, L.D., Cyclic Difference Sets, Lecture Notes in Mathematics, Vol. 182, Springer-Verag Press (1971)

[10] Bomer, L., Antweiler, M., New Perfect Threelevel and Threephase Sequences, IEEE Proceedings of International Symposium on Information Theory, p. 280 (1991)

[11] Bomer, L., Antweiler, M., Perfect N-Phase Sequences and Arrays, IEEE Journal on Selected Areas in Communications, Vol. 10, No. 4, pp. 782-789 (1992)

[12] Bosma, W., Cannon, J., Playoust, C., The Magma Algebra System I: The user Language, Journal of Symbolic Computation, Vol. 24, No. 3-4, pp. 235-265 (1997)

[13] Boztas, S.¸ Parampalli, U., Nonbinary Sequences with Perfect and Nearly Perfect Autocorrelations, IEEE Proceedings of International Symposium on Information Theory, pp. 1300-1304 (2010)

[14] Brenner, J.L., Matrices of Quaternions, Pacific Journal of Mathematics, Vol. 1, No. 3, pp. 329-335 (1951)

[15] Byron, F.W., Fuller, R.W., Mathematics of Classical and Quantum Physics, Dover Publications,Inc., New York (1992)

[16] Cayley, A., On Certain Results Relating to Quaternions, Philosophical Magazine, Ser 3, Vol. 26, p. 142 (1845)

[17] Chang, J.A., Ternary Sequence with Zero Correlation, Proceedings of the IEEE, Vol. 55, No. 7, pp. 1211-1213 (1967)

[18] Chee, Y.M., Tan, Y., Zhou, Y., Almost p-ary Perfect Sequences, Lecture Notes in Computer Science, Vol. 6338, Sequences and Their Applications – SETA 2010, pp. 399-415 (2010)

[19] Chen, L.X., Definition of Determinant and Cramer Solutions over the Quaternion Field, Acta Mathematica Sinica, New Series, Vol. 7, No. 2, pp. 171-180 (1991)

[20] Cho, E., DeMoivre’s Formula for Quaternions, Applied Mathematics Letters, Vol. 11, No. 6, pp. 33-35 (1998)

[21] Chu, D.C., Polyphase Codes with Good Periodic Correlation Properties, IEEE Transactions on Information Theory, Vol. 18, No. 4, pp. 531-532 (1972)

[22] Chung, H., Kumar, P.V., A new General Construction for Generalized Bent Functions, IEEE Transactions on Information Theory, Vol. 35, No. 1, pp. 206-209 (1989)

[23] Cohen, N., DeLeo, S., The Quaternionic Determinant, The Electronic Journal of Linear Algebra, Vol. 7, pp. 100-111 (2000)

[24] Coxeter, H.S.M., Quaternions and Reflections, The American Mathematical Monthly, Vol. 53, No. 3, pp. 136-146 (1946)

[25] Darnell, M., Fan, P.Z., Perfect Sequences Derived from M-sequences, IEEE Proceedings of International Symposium on Information Theory, p. 461 (1995)

[26] DeLeo, S., Rotelly, P., Quaternionic Electroweak Theory, Journal of Physics, G: Nuclear Particle Physics, Vol. 22, pp. 1137-1150 (1996)

[27] Eilenberg, S., Niven, I., The Fundamental Theorem of Algebra for Quaternions, Bulletins of American Mathematical Society, Vol. 50, pp. 246-248 (1944)

[28] Fan, J., Determinants and Multiplicative Functionals on Quaternion Matrices, Linear Algebra and its Applications, Vol. 369, pp. 193-201 (2003)

[29] Fan, P.Z., Darnell, M., The Synthesis of Perfect Sequences, Lecture Notes in Computer Science, Vol. 1025, Proceedings of the 5th IMA Conference on Cryptography and Coding, pp. 63-73 (1995)

[30] Farenick, D.R., Pidkowich, B.A.F., The Spectral Theorem in Quaternions, Linear Algebra and its Applications, Vol. 71, pp. 75-102 (2003)

[31] Flaunt, C., Eigenvalues and Eigenvectors for the Quaternion Matrices of Degree Two, Annals of Ovidius University of Constanta, Vol. 10, No. 2, pp. 39-44 (2002)

[32] Frank, R.L., Comments on ‘Polyphase Codes with Good Correlation Properties’ by Chu, IEEE Transactions on Information Theory, Vol. 19, No. 2, p. 244 (1973)

[33] Frank, R.L., Phase Shift Pulse Codes with Good Periodic Correlation Properties (Correspondence), IRE Transactions on Information Theory, Vol. 8, No. 6, pp. 381-382 (1962)

[34] Gabidulin, E.M., Non-Binary Sequences with the Perfect Periodic Auto-correlation and with Optimal Periodic Cross-correlation, IEEE Proceedings of International Symposium on Information Theory, p. 412 (1993)

[35] Gabidulin, E.M., Partial Classification of Sequences with Perfect Auto-correlation and Bent Functions, IEEE Proceedings of International Symposium on Information Theory, p. 467 (1995)

[36] Gabidulin, E.M., Shorin, V.V., New Sequences with Zero Autocorrelation, Problems of Information Transmission, Vol. 38, No. 4, pp. 255-267 (2002)

[37] Hathaway, A.S., Quaternions as Numbers of Four-Dimensional Space, Bulletin of the American Mathematical Society, Vol. 4, pp. 54-57 (1897)

[38] Heimiller, R.C., Author’s Comment, IRE Transactions on Information Theory, Vol. 8, No. 6, p. 382 (1962)

[39] Heimiller, R.C., Phase Shift Pulse Codes with Good Periodic Correlation Properties, IRE Transactions on Information Theory, Vol. IT-7, pp. 254-257 (1961)

[40] Helleseth, T., Some Results About the Cross-correlation Function Between Two Maximal Linear Sequences, Discrete Mathematics, Vol. 16, pp. 209-232 (1976)

[41] Hoholdt, T., Justesen, J., Ternary Sequences with Perfect Periodic Auto-correlation, IEEE Transactions on Information Theory, Vol. 29, No. 4, pp. 597-600 (1983)

[42] Hoholdt, T., The Merit Factor of Binary Sequences, NATO Science Series, Vol. 542, Series C: Mathematical and Physical Studies, Difference Sets, Sequences and their Correlation Properties, Kluwer Academic Publishers, pp. 227-237 (1999)

[43] Horadam, K.J., Hadamard Matrices and Their Applications, Princeton University Press, Princeton, N.J. (2007)

[44] Horn, R.A., Johnson, C.R., Matrix Analysis, Cambridge University Press (1985)

[45] Horwitz, L.P., Biedenharn, L.C., Quaternion Quantum Mechanics: Second Quantization and Gauge Fields, Annals of Physics, Vol. 157, pp. 432-488 (1984)

[46] Huang, L., On Two Questions About Quaternion Matrices, Linear Algebra and its Applications, Vol. 318, pp. 79-86 (2000)

[47] Huang, L., So, W., On Left Eigenvalues of a Quaternionic Matrix, Linear Algebra and its Applications, Vol. 323, pp. 105-116 (2001)

[48] Hungerford, T.W., Algebra, Springer Science + Business Media, New York, N.Y., USA (1974)

[49] Ipatov, V.P., Periodic Discrete Signals with Optimal Correlation Properties, Radio I Svyaz, Moscow (1992)

[50] Ipatov, V.P., Ternary Sequences with Ideal Autocorrelation Properties, Radio Engineering and Electronic Physics, Vol. 24, pp. 75-79 (1979)

[51] Jacobson, N., An Application of E.H.Moore’s Determinant of a Hermitian Matrix, Bulletins of American Mathematical Society, Vol. 45, No. 10, pp. 745-748 (1939)

[52] Jungnickel, D., Pott, A., Difference Sets: An Introduction, NATO Science Series, Vol. 542, Series C: Mathematical and Physical Studies, Difference Sets, Sequences and their Correlation Properties, Kluwer Academic Publishers, pp. 259-295 (1999)

[53] Jungnickel, D., Pott, A., Perfect and Almost Perfect Sequences, Discrete Applied Mathematics, Vol. 95, pp. 331-359 (1999)

[54] Knapp, M.P., Sines and Cosines of Angles in Arithmetic Progression, Mathematics Magazine, Vol. 82, No. 5, pp. 371-372 (2009)

[55] Kuznetsov, O., Perfect Sequences Over the Real Quaternions, IEEE Proceedings of the Fourth International Workshop on Signal Design and its Applications in Communications, pp. 8-11 (2009)

[56] Kuznetsov, O., Hall, T.E., Perfect Sequences Over the Real Quaternions of Longer Lengths, The Online Journal on Mathematics and Statistics, Vol. 1, No. 1, pp. 17-20 (2010)

[57] Kyrala, A., Theoretical Physics: Applications of Vector, Matrices, Tensors and Quaternions, W.B.Saunders Company, Philadelphia (1967)

[58] Lee, C.M., On a New Class of 5-ary Sequences Exhibiting Ideal Periodic Autocorrelation Properties with Applications to Spread Spectrum Systems, PhD Thesis, Department of Electrical Engineeriring, Mississipi State University (1998)

[59] Lee, H.C., Eigenvalues and Canonical Forms of Matrices with Quaternion Coefficients, Proceedings of the Royal Irish Academy, Vol. 52, Sect A (1949)

[60] Lewis, B.L., Kretschmer, F.F., Linear Frequency Modulation Derived Polyphase Pulse Compression Codes, IEEE Transactions on Aerospace and Electronic Systems, Vol. AES-18, No. 5, pp. 637-641 (1982)

[61] Liebendorfer, C., Heights and Determinants over Quaternion Algebras, Communications in Algebra, Vol. 33, pp. 3699-3717 (2005)

[62] Luke, H.D., Sequences and Arrays with Perfect Periodic Correlation, IEEE Transactions on Aerospace and Electronic Systems, Vol. 24, No. 3 (1988)

[63] Luke, H.D., Binary and Quadriphase Sequences with Optimal Autocorrelation Properties: A Survey, IEEE Transactions on Information Technology, Vol. 49, No. 12, pp. 3271-3282 (2003)

[64] Ma, S.L., Ng, W.S., On Non-existence of Perfect and Nearly Perfect Sequences, International Journal of Information and Coding Theory, Vol. 1, No. 1, pp. 15-38 (2009)

[65] Macias-Virgos, E., Pereira-Saez, M.J., Left Eigenvalues of 2×2 Symplectic Matrices, Electronic Journal of Linear Algebra, Vol. 18, pp. 274-280 (2009)

[66] Milewski, A., Periodic Sequences with Optimal Properties for Channel Estimation and Fast Start-Up Equalization, IBM Journal of Research and Development, Vol. 27, No. 5, pp. 426-431 (1983)

[67] Mirsky, L., An Introduction to Linear Algebra, Dover Publications, Mineola, N.Y., p. 293 (1990)

[68] Mitchell, C., Comment on Existence of One-Dimensional Perfect Binary Arrays, Electronic Letters, Vol. 24, No. 11, p. 714 (1988)

[69] Moharir, P.S., Generalized PN Sequences, IEEE Transactions on Information Theory, Vol. IT-23, No. 6, pp. 782-784 (1977)

[70] Moore, E.H., On the Determinant of a Hermitian Matrix of Quaternionic Elements, Bulletins of American Mathematical Society, Vol. 28, pp. 161-162 (1922)

[71] Mow, W.H., A Unified Construction of Perfect Polyphase Sequences, IEEE Proceedings of International Symposium on Information Theory, p. 459 (1995)

[72] Mow, W.H., Sequence Design for Spread Spectrum, The Chinese University of Hong Kong Press, Sha Tin, N.T., Hong Kong (1995)

[73] Niven, I., Equations in Quaternions, American Mathematical Society Monthly, Vol. 48, pp. 654-661 (1995)

[74] Parraud, P., On the Non-existence of (Almost) Perfect Quaternary Sequences, Lecture Notes in Computer Science, Vol. 2227, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, pp. 210-218 (2001)

[75] Popovic, B.M., Efficient Matched Filter for the Generalized Chirp-Like Polyphase Sequences, IEEE Transactions on Aerospace and Electronic Systems, Vol. 30, No. 3, pp. 769-777 (1994)

[76] Popovic, B.M., GCL Polyphase Sequences with Minimum Alphabets, Electronic Letters, Vol. 30, No. 2, pp. 106-107 (1994)

[77] Popovic, B.M., Generalized Chirp-like Polyphase Sequences with Optimum Correlation Properties, IEEE Transactions on Information Theory, Vol. 38, No. 4, pp. 1406-1409 (1992)

[78] Renmin, H., Xuqiang, Z., Liangtao, W., The Double Determinant of Vandermonde's Type over Quaternion Field, Applied Mathematics and Mechanics, English Edition, Vol. 20, No. 9, pp. 1046-1053 (1999)

[79] Sangwine, S.J., Le Bihan, N., Quaternion Singular Value Decomposition Based on Bidiagonalization to a Real or Complex Matrix Using Quaternion Householder Transformations, Applied Mathematics and Computation, Vol. 182, pp. 727-738 (2006)

[80] Sarwate, D.V., Pursley, M.B., Crosscorrelation Properties of Pseudorandom and Related Sequences, Proceedings of the IEEE, Vol. 68. No. 5, pp. 593-619 (1980)

[81] Schmidt, B., Cyclotomic Integers and Finite Geometry, Journal of the American Mathematical Society, Vol. 12, No. 4, pp. 929-952 (1999)

[82] Schroeder, M., Number Theory in Science and Communication, 5th Edition, Springer-Verlag Berlin Heidelberg, p. 141 (2009)

[83] Shedd, D.A., Sarwate, D.V., Construction of Sequences with Good Correlation Properties, IEEE Transactions on Information Theory, Vol. IT-25, No. 1 (1979)

[84] Simon, M.K., Omura, J.K., Scholtz, R.A., Levitt, B.K., Spread Spectrum Communications Handbook, McGraw-Hill, New York, N.Y., USA (1994)

[85] Skaug, R., Hjelmstad, J.F., Spread Spectrum in Communication, Published by IET (1985)

[86] Stringham, W.I., Determination of the Finite Quaternion Groups, American Journal of Mathematics, Vol. 4, No. 1, pp. 345-357 (1881)

[87] Study, E., Zur Theorie der Linearen Gleichungen, Acta Mathematica, Vol. 42, pp. 1-61 (1920)

[88] Suehiro, N., Hatori, M., Modulatable Orthogonal Sequences and Their Application to SSMA Systems, IEEE Transactions on Information Theory, Vol. 34, No. 1, pp. 93-100 (1988)

[89] Tomlinson, G.H., Amplitude Distributions of Smoothed Inverse-Repeat Binary Sequences, International Journal of Electronics, Vol. 64, No. 2, pp. 289-297 (1988)

[90] Tompkins, D.N., Codes with Zero Correlation, Hughes Aircraft Company, Culver City, California, Technical Memo 651 (1960)

[91] Turyn, R.J., Character Sums and Difference Sets, Pacific Journal of Mathematics, Vol. 15, No. 1, pp. 319-346 (1965)

[92] VanDerWaerden, B.L., Hamilton’s Discovery of Quaternions, Mathematics Magazine, Vol. 49, No. 5, pp. 227-234 (1976)

[93] Vicci, L., Quaternions and Rotations in 3-Space: The Algebra and its Geometric Interpretation, Technical Report TR01-014, University of North Carolina at Chapel Hill, NC (2001)

[94] Viswanath, K., Normal Operators on Quaternionic Hilbert Spaces, Transactions of the American Mathematical Society, Vol. 162, pp. 337-350 (1971)

[95] Wood, R.M.W., Quaternionic Eigenvalues, Bulletins of London Mathematical Society, Vol. 17, pp. 137-138 (1985)

[96] Xian, Y.Y., Existence of One-Dimensional Perfect Binary Arrays, Electronic Letters, Vol. 23, No. 24, pp. 1277-1278 (1987)

[97] Young, R.M., When is $\mathbb{R}^n$ a Field?, The Mathematical Gazette, Vol. 72, No. 460, pp. 128-129 (1988)

[98] Zhang, F., Quaternions and Matrices of Quaternions, Linear Algebra and its Applications, Vol. 251, pp. 21-57 (1997)

[99] Zhang, N., Golomb, S.W., Polyphase Sequence with Low Autocorrelations, IEEE Transactions on Information Theory, Vol. 39, No. 3, pp. 1085-1089 (1993)