Universitatea *Transilvania* din Braşov

HABILITATION THESIS

Contributions to the study of algebras obtained by the Cayley Dickson process and some of their applications

Domain: Mathematics

Author: Cristina FLAUT

University:"Ovidius" of Constanta

BRASOV, 2016

CONTENT

Acknowledgement **5**

List of notations **7**

(A) Rezumat **9**

(B) Scientific and professional achievements and the evolution and development plans for career development

(B-i) Scientific and professional achievements **11**

Chapter 1: Introduction **11**

Chapter 2: Levels and sublevels of algebras obtained by the Cayley-Dickson process **22**

Chapter 3: Properties of algebras obtained by the Cayley-Dickson process and some of their applications **50**

Chapter 4: Some applications in Coding Theory **109**

(B-ii) The evolution and development plans for career development **153**

Annex 1 ..... **171**

Annex 2 ..... **173**

Annex 3 ..... **176**

(B-iii) Bibliography **178**

Acknowledgement. I would like tkank Professor Ravi P. Agarwal for his support, all my co-authors and my family: Dan and Theodora.

Notations

$A_t = \left(\frac{\alpha_1,\ldots,\alpha_t}{K}\right)$	the algebra obtained by the Cayley-Dickson process of dimension 2^t
$\mathbb{H}$	real quaternion division algebra
$\mathbb{O}$	real octonion division algebra
$\mathbb{H}(\alpha,\beta)$	generalized quaternion algebra
$\mathbb{O}(\alpha,\beta,\gamma)$	generalized octonion algebra
(V,b)	a symmetric bilinear space
$\mathbb{N}$	the set of natural numbers
$\mathbb{Z}$	the ring of integers
$\mathbb{Q}$	the field of rational numbers
$\mathbb{R}$	the field of real numbers
$\mathbb{C}$	the field of complex numbers
$V_1 \perp V_2$	the orthogonal sum of the vector spaces V_1 and V_2
$< \alpha_1, \ldots \alpha_n >$	a symmetric bilinear space with diagonal matrix $(\alpha_1, \ldots \alpha_n)$
$A \otimes B$	the tensor product of the matrix A and B
$< 1, -1 >$	the hyperbolic plane
φ	a $n-$dimensional quadratic irreducible form
$K(\varphi)$	the function field of φ
$\ll a_1, a_2, \ldots, a_n \gg$	a Pfister form
$i_W(V)$	the Witt index of (V,b)
$s(K)$	the level of the field K
$s(A)$	the level of the algebra A
$\underline{s}(A)$	the sublevel of the algebra A
$[x,y]$	the commutator of the elements x, y from the algebra A
$w_H(x)$	the Hamming weight
$d_H(x,y)$	the Hamming distance between two codewords
$\mathbb{F}_{p^n}$	a finite field

Rezumat

Aceasta teza prezinta, intr-o maniera succinta, rezultatele originale ale autorului in studiul algebrelor obtinute prin procedeul Cayley-Dickson.

Lucrarea este organizata in 4 capitole, are trei anexe si o bibliografie care cuprinde 135 de titluri. Ultima parte este dedicata prezentarii unor directii de dezvoltare personala si stiintifica.

Capitolul 1 prezinta pe scurt rezultate si proprietati cunoscute ale algebrelor obtinute prin procedeul Cayley-Dickson.

Capitolul 2 este dedicat prezentarii unor noi rezultate in cee ce priveste nivelul si subnivelul algebrelor de cuaternioni si octonioni generalizand aceste doua notiuni si pentru orice algebra obtinuta prin procedeul Cayley-Dickson. Un rezultat foarte important in acest studiu, demonstrat de catre autor, este faptul ca pentru orice numar natural n putem gasi o astfel de algebra care sa aiba nivelul n. Acest rezultat generalizeaza doua rezultate foarte tari datorate lui Pfister si T.Y. Lam si anume:

Orice corp este fie de nivel infinit, fie de nivel finit de forma 2^m *si pentru orice numar de forma* 2^m *putem gasi un corp* K *de nivel* 2^m, respectiv

Pentru orice numar natural n*, exista un domeniu de integritate* R *astfel incat nivelul sau sa fie* n.

Capitolul 3 prezinta noi rezultate importante ale algebrelor obtinute prin procedeul Cayley-Dickson. Este cunoscut faptul ca aceste algebre sunt sarace in proprietati. Cuaternnionii nu sunt algebre comutative iar Octonionii au pierdut si comutativitatea si asociativitatea. In schimb, sunt algebre alternative, asociative in puteri si flexibile. Incepand cu Sedenionii, raman valabile doar ultimele doua proprietati, pierzandu-se si alternativitatea. Identitatea lui Hall pentru cuaternioni si octonioni a fost generalizata pentru orice algebra obtinuta prin procedeul Cayley-Dickson. Folosindu-se o idee data de Bales in [Ba; 09], au fost gasite anumite proprietati ale elementelor unei baze intr-o astfel de algebra, permitandu-ne sa dam astfel un exemplu de functie olomorfa definita pe o algebra obtinuta prin procedeul Cayley-Dickson. In plus, s-au rezolvat anumite ecuatii si, folosindu-se cuaternionii de tip Fibonacci-Lucas peste $\mathbb{Q}$, s-a definit o structura de algebra peste aceste elemente.

Capitolul 4 este dedicat recentelor aplicatii ale algebrelor obtinute prin procedeul Cayley-Dickson in teoria codurilor. Pentru orice numar prim p, s-a identificat o submultime $\mathbb{V}$ in A_t cu ajutorul caruia am gasit un izomorfism intre corpul claselor de resturi modulo un prim π din $\mathbb{V}$ si $\mathbb{Z}_p$, cu p numar prim astfel incat $\mathbf{n}(\pi) = p$. In acest fel, s-a putut obtine un algoritm mult mai flexibil (pastrand proportiile, ca algoritmul lui Lenstra pe curbe eliptice comparat cu algoritmul $p-1$ al lui Pollard) care ne permite sa construim coduri corectoare de erori peste $\mathbb{Z}_p$ pentru aproape orice numar prim p.

Ultima parte este dedicata abordarii unor noi directii de cercetare care au ca punct de plecare rezultatele prezentate in aceasta lucrare: cum poate fi abordat studiul nivelului si subnivelului unei algebre obtinute prin procedeul Cayley-Dickson pentru a putea obtine noi rezultate, gasirea de noi identitati si proprietati ale acestor algebre si dezvoltarea aplicatiilor lor in teoria codurilor. In plus, au fost prezentate si alte noi directii care au ca baza noile conexiuni ale altor algebre in teoria codurilor, cum ar fi unele tipuri de algebre logice (BCK-algebras, BCI-algebras, etc). De asemenea, sunt prezentate si unele directii de dezvoltare ale activitatii didactice.

(B) Scientific and professional achievements and the evolution and development plans for career development
(B-i) Scientific and professional achievements

Chapter 1

Introduction

1. **Preliminaries**

Let K be a field, and let A be a vector space over the field K with a binary operation

$$" \cdot "A \times A \to A, \tag{1.1.}$$

called *the product* of the element x and y. We call A an *algebra* over the field K if we have the following identities, for all elements $x, y, z \in A$ and for all scalars $a, b \in K$:

$$(x + y) \cdot z = x \cdot z + yz;$$

$$x \cdot (y + z) = x \cdot y + x \cdot z;$$

$$(ax) \cdot (by) = (ab)(x \cdot y).$$

We remark that the binary operation (1.1) is bilinear and is called the multiplication in A. In general, the multiplication of elements of an algebra is not necessarily associative and, due to this situation, we will consider two distinct cases: *associative algebras* and *nonassociative algebras*. Sometime,

some authors use the notion of an *algebra* when they refer to an associative algebra.

An algebra A is called *unital* or *unitary* if this algebra contains an identity element with respect to the multiplication (1.1).

In the following, in all this study, we suppose that K is a commutative field with $charK \neq 2$ and A is an algebra over the field K. The *center* C of an algebra A is the set of all elements $c \in A$ which commute and associate with all elements $x \in A$.An algebra A is central if its center is equal with the ground field, $C = K$.

An algebra A is a *simple* algebra if A is not a zero algebra and $\{0\}$ and A are the only ideals of A. The algebra A is called *central simple* if the algebra $A_F = F \otimes_K A$ is simple for every extension F of K. A central simple algebra is a simple algebra. An algebra A is called *alternative* if $x^2y = x\,(xy)$ and $xy^2 = (xy)\,y$, for all $x, y \in A$, *flexible* if $x\,(yx) = (xy)\,x = xyx$, for all $x, y \in A$ and *power associative* if the subalgebra $< x >$ of A generated by any element $x \in A$ is associative. Each alternative algebra is a flexible algebra and a power associative algebra.

An element x in a ring R is called *nilpotent* if we can find a positive integer n such that $x^n = 0$.A power-associative algebra A is called a *nil algebra* if and only if each element of the algebra is nilpotent.

Artin's Theorem. [Sc; 66] *The subalgebra generated by two arbitrary elements x, y of an alternative algebra A is associative.*

In each alternative algebra A, the following identities

$$a(x(ay)) = (axa)y,$$

$$((xa)y)a = x(aya),$$

$$(ax)(ya) = a(xy)a$$

hold, for all $a, x, y \in A$. These identities are called the *Moufang identities.*

A unitary algebra $A \neq K$ such that we have $x^2 + \alpha_x x + \beta_x = 0$ for each $x \in A$, with $\alpha_x, \beta_x \in K$, is called a *quadratic algebra.*

It is known that a finite-dimensional algebra A is *a division* algebra if and only if A does not contain zero divisors. (See [Sc;66])

An algebra A is *semisimple* if it is a direct sum of simple algebras. An associative K-algebra A is said to be *separable* if for every field extension $K \subset L$ the algebra $A \otimes_K L$ is semisimple.

Wedderburn's Theorem. [Sch; 85] *Let A be a simple algebra over K. Then $A \simeq \mathcal{M}_n(D)$, where D is a division algebra over K.*

In the following, we will briefly present two important and very known algebras: the quaternion algebras,which are associative algebras, and octonions algebras, which are nonassociative algebras.

In October 1843, William Rowan Hamilton discovered the quaternions, which is a 4-dimensional algebra over $\mathbb{R}$. This algebra is an associative and a noncommutative algebra. In December 1843, John Graves discovered the octonions, an 8-dimensional algebra over $\mathbb{R}$ which is a nonassociative and a noncommutative algebra. In 1845, these algebras were rediscovered by Arthur Cayley. They are also known as the Cayley numbers. This process, of passing from $\mathbb{R}$ to $\mathbb{C}$, from $\mathbb{C}$ to $\mathbb{H}$ and from $\mathbb{H}$ to $\mathbb{O}$ was generalized to algebras over arbitrary fields and rings. It is called the *Cayley-Dickson doubling process* or the *Cayley–Dickson process.* Clifford algebras were discovered, in 1878, by W. K. Clifford. These algebras were defined to have generators e_1, $e_2, ..., e_n$ which anti-commute and satisfy $e_i^2 = a_i \in \mathbb{R}$, for all $i \in \{1, 2, ..., n\}$. These algebras generalize the real numbers, complex numbers and quaternions(see [Lew; 06])

1.1. **Quaternion algebras**

Let $\mathbb{H}$ be the real quaternion algebra with basis $\{1, i, j, k\}$, where

$$i^2 = j^2 = k^2 = -1, ij = -ji, ik = -ki, jk = -kj \qquad (1.2.)$$

and each element from $\mathbb{H}$ has the form $q = a + bi + cj + dk, a, b, c, d \in \mathbb{R}$.

We remark that $\mathbb{H}$ is a vector space of dimension 4 over $\mathbb{R}$ with the addition and scalar multiplication.

Also $\mathbb{H}$ has a ring structure with multiplication given by (1.2) and the usual distributivity law.

In the following, we will consider the quaternion algebra over an arbitrary field K with $charK \neq 2$.We consider two elements $\alpha, \beta \in K$ and we define a generalized quaternion algebra, denoted by $\mathbb{H}(\alpha, \beta) = \left(\frac{\alpha,\beta}{K}\right)$, with basis $\{1, f_1, f_2, f_3\}$ and multiplication given in the following table:

$\cdot$	1	f_1	f_2	f_3
1	1	f_1	f_2	f_3
f_1	f_1	α	f_3	αf_2
f_2	f_2	$-f_3$	β	$-\beta f_1$
f_3	f_3	$-\alpha f_2$	βf_1	$-\alpha\beta$

If $a \in \mathbb{H}(\alpha, \beta)$, $a = a_0 + a_1 f_1 + a_2 f_2 + a_3 f_3$, then

$$\bar{a} = a_0 - a_1 f_1 - a_2 f_2 - a_3 f_3$$

is called the *conjugate* of the element a. For $a \in \mathbb{H}(\alpha, \beta)$, we consider the following elements:

$$\mathbf{t}(a) = a + \overline{a} \in K$$

and

$$\mathbf{n}(a) = a\overline{a} = a_0^2 - \alpha a_1^2 - \beta a_2^2 + \alpha\beta a_3^2 \in K,$$

called the *trace*, respectively, the *norm* of the element $a \in \mathbb{H}(\alpha, \beta)$. It follows that

$$(a + \overline{a})\, a = a^2 + \overline{a}a = a^2 + \mathbf{n}(a) \cdot 1$$

and

$$a^2 - \mathbf{t}(a)\, a + \mathbf{n}(a) = 0, \forall a \in \mathbb{H}(\alpha, \beta),$$

therefore the generalized quaternion algebra is a *quadratic algebra*.

The subset

$$\mathbb{H}(\alpha, \beta)_0 = \{x \in \mathbb{H}(\alpha, \beta) \mid \mathbf{t}(x) = 0\}$$

of $\mathbb{H}(\alpha, \beta)$ is a subspace of the algebra $\mathbb{H}(\alpha, \beta)$. It is obvious that

$$\mathbb{H}(\alpha, \beta) = K \cdot 1 \oplus \mathbb{H}(\alpha, \beta)_0,$$

therefore each element $x \in \mathbb{H}(\alpha,\beta)$ has the form $x = x_0 \cdot 1 + \overrightarrow{x}$, with $x_0 \in K$ and $\overrightarrow{x} \in \mathbb{H}(\alpha,\beta)_0$. For $K = \mathbb{R}$, we call x_0 *the scalar part* and $\overrightarrow{x}$ *the vector part* for the quaternion x.

If, for $x \in \mathbb{H}(\alpha,\beta)$, the relation $\mathbf{n}(x) = 0$ implies $x = 0$, then the algebra $\mathbb{H}(\alpha,\beta)$ is a *division* algebra. A quaternion non-division algebra is called a *split* algebra.

Using the above notations, we remark that $\mathbb{H}(-1,-1) = \left(\frac{-1,-1}{\mathbb{R}}\right)$ is a division algebra.

Proposition 1. ([La; 04],Proposition 1.1)

1) *The quaternion algebra* $\mathbb{H}(\beta_1,\beta_2)$ *is isomorphic with the quaternion algebra* $\mathbb{H}\left(x^2\beta_1, y^2\beta_2\right)$, *where* $x, y \in K^*$.

2) $\mathbb{H}(-1,1) \simeq \mathcal{M}_2(K)$.□

From the above proposition, we have that a Quaternion algebra is a division or a split algebra.

1.2. Octonion algebras

The real octonion division algebra is a non-associative and non-commutative extension of the algebra of quaternions, $\mathbb{H}(-1,-1) = \left(\frac{-1,-1}{\mathbb{R}}\right)$. Among all real division algebras, octonion algebra forms the largest normed division algebra.([Sc; 54])

A generalized octonion algebra over an arbitrary field K, with $charK \neq 2$, is an algebra of dimension 8, denoted $\mathbb{O}(\alpha,\beta,\gamma)$, with basis $\{1, f_1, ..., f_7\}$ and multiplication given in the following table:

·	1	f_1	f_2	f_3	f_4	f_5	f_6	f_7
1	1	f_1	f_2	f_3	f_4	f_5	f_6	f_7
f_1	f_1	α	f_3	αf_2	f_5	αf_4	$-f_7$	$-\alpha f_6$
f_2	f_2	$-f_3$	β	$-\beta f_1$	f_6	f_7	βf_4	βf_5
f_3	f_3	$-\alpha f_2$	βf_1	$-\alpha\beta$	f_7	αf_6	$-\beta f_5$	$-\alpha\beta f_4$
f_4	f_4	$-f_5$	$-f_6$	$-f_7$	γ	$-\gamma f_1$	$-\gamma f_2$	$-\gamma f_3$
f_5	f_5	$-\alpha f_4$	$-f_7$	$-\alpha f_6$	γf_1	$-\alpha\gamma$	γf_3	$\alpha\gamma f_2$
f_6	f_6	f_7	$-\beta f_4$	βf_5	γf_2	$-\gamma f_3$	$-\beta\gamma$	$-\beta\gamma f_1$
f_7	f_7	αf_6	$-\beta f_5$	$\alpha\beta f_4$	γf_3	$-\alpha\gamma f_2$	$\beta\gamma f_1$	$\alpha\beta\gamma$

The algebra $\mathbb{O}(\alpha,\beta,\gamma)$ is a non-commutative and a non-associative algebra, but it is *alternative*, *flexible* and *power-associative*.

If $a \in \mathbb{O}(\alpha,\beta,\gamma)$, $a = a_0 + a_1f_1 + a_2f_2 + a_3f_3 + a_4f_4 + a_5f_5 + a_6f_6 + a_7f_7$, then $\bar{a} = a_0 - a_1f_1 - a_2f_2 - a_3f_3 - a_4f_4 - a_5f_5 - a_6f_6 - a_7f_7$ is called the *conjugate* of the element a. For $a \in \mathbb{O}(\alpha,\beta,\gamma)$, we define the elements:

$$\mathbf{t}(a) = a + \overline{a} \in K$$

and

$$\mathbf{n}(a) = a\overline{a} = a_0^2 - \alpha a_1^2 - \beta a_2^2 + \alpha\beta a_3^2 - \gamma a_4^2 + \alpha\gamma a_5^2 + \beta\gamma a_6^2 - \alpha\beta\gamma a_7^2 \in K.$$

These elements are called the *trace*, respectively, the *norm* of the element $a \in \mathbb{O}(\alpha,\beta,\gamma)$. It follows that

$$(a + \overline{a})\, a = a^2 + \overline{a}a = a^2 + \mathbf{n}(a) \cdot 1$$

and

$$a^2 - \mathbf{t}(a)\, a + \mathbf{n}(a) = 0, \forall a \in a \in \mathbb{O}(\alpha,\beta,\gamma),$$

therefore the generalized octonion algebra is a *quadratic* algebra.

The subset

$$\mathbb{O}(\alpha,\beta,\gamma)_0 = \{x \in \mathbb{O}(\alpha,\beta,\gamma) \mid \mathbf{t}(x) = 0\}$$

of $\mathbb{O}(\alpha,\beta,\gamma)$ is a subspace of the algebra $\mathbb{O}(\alpha,\beta,\gamma)$. It is obvious that

$$\mathbb{O}(\alpha,\beta,\gamma) = K \cdot 1 \oplus \mathbb{O}(\alpha,\beta,\gamma)_0,$$

therefore each element $x \in \mathbb{O}(\alpha,\beta,\gamma)$ has the form $x = x_0 \cdot 1 + \overrightarrow{x}$, with $x_0 \in K$ and $\overrightarrow{x} \in \mathbb{O}(\alpha,\beta,\gamma)_0$. For $K = \mathbb{R}$, we call x_0 *the scalar part* and $\overrightarrow{x}$ *the vector part* for the octonion x.

If, for $x \in \mathbb{O}(\alpha,\beta,\gamma)$, the relation $\mathbf{n}(x) = 0$ implies $x = 0$, then the algebra $\mathbb{O}(\alpha,\beta,\gamma)$ is a *division* algebra.(see [Sc; 54] and [Sc; 66])

A composition algebra A over the field K is an algebra, not necessarily associative, with a nondegenerate quadratic form N which satisfies the relation

$$N(xy) = N(x)N(y), \forall x, y \in A.$$

A unital composition algebras are called *Hurwitz algebras.*

Hurwitz's Theorem.[Ba; 01] $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ *and* $\mathbb{O}$ *are the only real alternative division algebras.*

Theorem ([Theorem 2.14, McC,80]) *A is a composition algebra if and only if A is an alternative quadratic algebra.*

1.3. **Algebras obtained by the Cayley-Dickson process**

As we remarked above, the Octonion algebra extends the Quaternion algebra and the dimension of the Octonion algebra is double that the dimension of Quaternion algebra. This procedure of doubling dimension of an algebra is called the Cayley-Dickson process. In the following, we briefly present the *Cayley-Dickson process* and the properties of the algebras obtained. (see [Sc; 66] and [Sc; 54]).

We consider A, a finite dimensional unitary algebra over a field K, with a *scalar involution*

$$^{-} : A \to A, a \to \overline{a},$$

i.e. it is a linear map with the following properties

$$\overline{ab} = \overline{b}\overline{a},\ \overline{\overline{a}} = a,$$

and

$$a + \overline{a}, a\overline{a} \in K \cdot 1 \text{ for all } a, b \in A.$$

An element $\overline{a}$ is called the *conjugate* of the element a, the linear form

$$\mathbf{t} : A \to K\,,\ \mathbf{t}\,(a) = a + \overline{a}$$

and the quadratic form

$$\mathbf{n} : A \to K,\ \mathbf{n}\,(a) = a\overline{a}$$

are called the *trace* and the *norm* of the element a, respectively. Hence an algebra A with a scalar involution is quadratic.

We consider $\gamma \in K$ a fixed non-zero element. We define the following algebra multiplication on the vector space

$$A \oplus A : (a_1, a_2)(b_1, b_2) = \left(a_1 b_1 + \gamma \overline{b}_2 a_2, a_2 \overline{b_1} + b_2 a_1\right). \tag{1.3.}$$

The obtained algebra structure over $A \oplus A$, denoted by (A, γ) is called the *algebra obtained from A by the Cayley-Dickson process.* We have $\dim(A, \gamma) = 2 \dim A$.

Let $x \in (A, \gamma)$, $x = (a_1, a_2)$. The map

$$^{-} : (A, \gamma) \to (A, \gamma)\ ,\ x \to \bar{x} = (\overline{a}_1, \text{-}a_2),$$

is a scalar involution of the algebra (A, γ), extending the involution $^{-}$ of the algebra A. Let

$$\mathbf{t}(x) = \mathbf{t}(a_1)$$

and

$$\mathbf{n}(x) = \mathbf{n}(a_1) - \gamma \mathbf{n}(a_2)$$

be the *trace* and the *norm* of the element $x \in (A, \gamma)$, respectively.

If we consider $A = K$ and we apply this process t times, $t \geq 1$, we obtain an algebra over K,

$$A_t = \left(\frac{\alpha_1, ..., \alpha_t}{K}\right). \tag{1.4.}$$

Using induction in this algebra, the set $\{1, f_2, ..., f_n\}, n = 2^t$, generates a basis with the properties:

$$f_i^2 = \gamma_i 1,\ _i \in K, \gamma_i \neq 0,\ i = 2, ..., n \tag{1.5.}$$

and

$$f_i f_j = -f_j f_i = \beta_{ij} f_k,\ \beta_{ij} \in K,\ \beta_{ij} \neq 0, i \neq j, i, j = 2, ...n, \tag{1.6.}$$

β_{ij} and f_k being uniquely determined by f_i and f_j.

From [Sc; 54], Lemma 4, it results that in any algebra A_t with the basis $\{1, f_2, ..., f_n\}$ satisfying relations (1.5) and (1.6) , we have:

$$f_i\left(f_i x\right) = \gamma_i x = \left(x f_i\right) f_i, \tag{1.7.}$$

for all $i \in \{1, 2, ..., n\}$ and for every $x \in A$

For $t = 2$, we obtain the generalized quaternion algebras and for $t = 3$,we obtain the generalized octonion algebras.

We remark that the field K is the center of the algebra A_t,for $t \geq 2$.(See [Sc; 54]). Algebras A_t of dimension 2^t obtained by the Cayley-Dickson process, described above, are central-simple, flexible and power associative for all $t \geq 1$ and, in general, are not division algebras for all $t \geq 1$. But there exist fields on which, if we apply the Cayley-Dickson process, the obtained algebras A_t are division algebras for all $t \geq 1$,as we can see in the next chapter (See [Br; 67], [Fl; 12]).

In 1878, W. K. Clifford discovered Clifford algebras. These algebras generalize the real numbers, complex numbers and quaternions(see [Le; 06]).

The theory of Clifford algebras is intimately connected with the theory of quadratic forms. In the following, we will consider K to be a field of characteristic not two. Let (V, q) be a quadratic $K-$vector space, equipped with a nondegenerate quadratic form over the field K. A *Clifford algebra* for (V, q) is a $K-$algebra C with a linear map $i : V \to C$ satisfying the property

$$i\left(x\right)^2 = q\left(x\right) \cdot 1_C, \forall x \in V,$$

such that for any $K-$algebra A and any K linear map $\gamma : V \to A$ with $\gamma^2\left(x\right) = q\left(x\right) \cdot 1_A, \forall x \in V$, there exists a unique K-algebra morphism $\gamma' : C \to A$ with $\gamma = \gamma' \circ i$.

Such an algebra can be constructed using the tensor algebra associated to a vector space V. Let $T(V) = K \oplus V \oplus (V \otimes V) \oplus ...$ be the tensor algebra associated to the vector space V and let $\mathcal{J}$ be the two-sided ideal of $T(V)$ generated by all elements of the form $x \otimes x - q\left(x\right) \cdot 1$, for all $x \in V$. The associated Clifford algebra is the factor algebra $C(V, q) = T\left(V\right)/\mathcal{J}$. ([Kn; 88], [La; 04])

Theorem Poincaré-Birkhoff-Witt. ([Kn; 88], p. 44)*If* $\{e_1, e_2, ..., e_n\}$ *is a basis of* V *, then the set* $\{1, e_{j_1}e_{j_2}...e_{j_s}, 1 \leq s \leq n, 1 \leq j_1 < j_2 < ... < j_s \leq n\}$ *is a basis in* $C(V, q)$.

We remark that $e_ie_j = -e_je_i$ and $e_i^2 = q^2(x)$. If V has dimension n, therefore the associated Clifford algebra has dimension 2^n. The most important Clifford algebras are those defined over real and complex vector spaces equipped with nondegenerate quadratic forms. Every nondegenerate quadratic form over a real vector space is equivalent with the following standard diagonal form:

$$q(x) = x_1^2 + ... + x_r^2 - x_{r+1}^2 - ... - x_s^2,$$

where $n = r + s$ is the dimension of the vector space. The pair of integers (r, s) is called *the signature* of the quadratic form. The real vector space with this quadratic form is usually denoted $\mathbb{R}_{r,s}$ and the Clifford algebra on $\mathbb{R}_{r,s}$ is denoted $Cl_{r,s}(\mathbb{R})$. For other details about Clifford algebras, the reader is referred to [Ki, Ou; 99], [Ko; 10], [Om; 62] and [Sm; 91].

Example 3.4.1.

i) For $p = q = 0$ we have $Cl_{0,0}(K) \simeq K$;

ii) For $p = 0, q = 1$, it results that $Cl_{0,1}(K)$ is a two-dimensional algebra generated by a single vector e_1 such that $e_1^2 = -1$ and therefore $Cl_{0,1}(K) \simeq K(e_1)$. For $K = \mathbb{R}$ it follows that $Cl_{0,1}(\mathbb{R}) \simeq \mathbb{C}$.

iii) For $p = 0, q = 2$, the algebra $Cl_{0,2}(K)$ is a four-dimensional algebra spanned by the set $\{1, e_1, e_2, e_1e_2\}$. Since $e_1^2 = e_2^2 = (e_1e_2)^2 = -1$ and $e_1e_2 = -e_2e_1$, we obtain that this algebra is isomorphic to the division quaternions algebra $\mathbb{H}$. We remark that the construction is similar with Cayley-Dickson process: $Cl_{0,1}(\mathbb{R}) \simeq \mathbb{C}, Cl_{0,2}(\mathbb{R}) \simeq \mathbb{H}$, but $Cl_{0,3}(\mathbb{R}) \simeq \mathcal{M}_2(\mathbb{C})$ is not isomorphic with $\mathbb{O}$, the octonions, since it is associative, $Cl_{1,3}(\mathbb{R}) \simeq \mathcal{M}_2(\mathbb{H})$.

iv) For $p = 1, q = 1$ or $p = 2, q = 0$, we obtain the algebra $Cl_{1,1}(K) \simeq Cl_{2,0}(K)$ which is isomorphic with a split quaternion algebra.([Gi, Mu; 91])

1.4. **Nonassociative quaternion algebras**

Let A be a quadratic separable algebra over the field K with a scalar involution $^- : A \to A, a \to \overline{a}$. Let $\gamma \in A - K$. Using relation (1.3) , the vector space $A \oplus A$ becomes a quaternion nonassociative algebra over K. Nonassociative quaternion algebras are not power-associative algebras and are not quadratic algebras. If A is a separable quadratic field extension of the field K, therefore a nonassociative quaternion algebra is a division algebra.(see [Wa; 87], [Pu, As; 06])

Quaternions, octonions and algebras obtained by the Cayley-Dickson process have at present many applications, as for example in physics, coding theory, computer vision, etc. For these reasons, these algebras are intense studied, see for example [Pu; 13], [Pu, St; 15], etc. and some of these applications will be presented in the next chapters. For other details about these algebras, the reader is referred to [St; 09] and [Vo; 14].

Chapter 2

Levels and sublevels of algebras obtained by the Cayley-Dickson process

As we can seen, the theory of quaternion algebras, octonion algebras and algebras obtained by the Cayley-Dickson process is closely related to the algebraic theory of quadratic forms.

In the following, we will present the generalization of the concepts of level and sublevel of a composition algebra to algebras obtained by the Cayley-Dickson process and we will show that, in the case of level for algebras obtained by the Cayley-Dickson process, the situation is similar as for the integral domains. For this purpose, we will prove that for any positive integer n, we can find an algebra A obtained by the Cayley-Dickson process which has the norm form anisotropic over a suitable field and has the level $n \in \mathbb{N}-\{0\}$.These results were obtained in the papers [Fl; 11] and [Fl; 13]

2.1. Quadratic forms

For the general notions of quadratic and symmetric bilinear spaces, we used [La; 04], [La, Ma; 01], [Om; 62], [Sch; 85].

Definition 2.1.1. [Sch;85] A *symmetric bilinear* space (V, b) over a field K is a vector space V with a symmetric bilinear form $b : V \times V \to K$. From now on, we will understand by a bilinear space a symmetric bilinear space.

Two symmetric bilinear spaces (V_1, b_1) and (V_2, b_2) are *isomorphic* (or *isometric*) if there is a bijective map $\tau : V_1 \to V_2$ such that $b_2(\tau(x), \tau(y)) = b_1(x, y)$. We denote this with $V_1 \cong V_2$. The map τ is called an *isometry*.

A symmetric bilinear space (V,b) is called *regular*(*nonsingular or nondegenerate*) if for each element $x \neq 0, x \in V$, there is an element $y \in V$ such that $b(x,y) \neq 0$.

A quadratic space (V,q) over a field K is a vector space V with a quadratic form $q : V \to K$.

Since

$$b_q = \frac{1}{2}\left(q(x+y) - q(x) - q(y)\right)$$

is the associated bilinear form of q, in the following, we will consider symmetric bilinear spaces and quadratic spaces as the similar objects and sometimes we will use the notation q,with q the quadratic form on V.

Let (V_1,b_1) and (V_2,b_2) be two bilinear spaces. Let $V = V_1 \oplus V_2 (V = V_1 \times V_2$ and $V_1 \cap V_2 = \{0\}, V_1, V_2$ considered as subspaces of $V)$, the direct sum, with the bilinear form

$$b : V_1 \oplus V_2 \to K, b\left(\left(x_1', x_2'\right), \left(x_1'', x_2''\right)\right) = b_1\left(x_1', x_1''\right) + b_2\left(x_2', x_2''\right).$$

V is called *the orthogonal sum* of (V_1,b_1) and (V_2,b_2), denoted by $V_1 \perp V_2$. If b_1 and b_2 are symmetric, it results that b is symmetric. Let q_1, q_2, q be the associated quadratic forms. We write sometimes $q = q_1 \perp q_2$ instead of $V = V_1 \perp V_2$.

We will denote $m \times q = \underbrace{q \perp ... \perp q}_{m-times}$,where $m \in \mathbb{N}$.

A quadratic form *represents* the scalar $\alpha \in K$ if there is an element $x \in V, x \neq 0$, such that $q(x) = \alpha$. The space (V,q) is called *universal* if q represent all nonzero scalars.

We call a quadratic form $q : V \to K$ *anisotropic* if $q(x) = 0$ implies $x = 0$,for all $x \in V$, otherwise q is called *isotropic*. A bilinear form $b : V \times V \to K$ is called anisotropic if $b(x,x) = 0$ implies $x = 0$,for all $x \in V$, otherwise b is called *isotropic*. A bilinear space (V,b) is called *isotropic* if its bilinear form is isotropic. A subspace V' of V is called *totally isotropic* if $b(x,y) = 0$, for all $x, y \in V'$.An isotropic bilinear space is universal.

Let (V,b) be a symmetric bilinear space of dimension n, with a basis $B = \{e_1, e_2, ..., e_n\}$. The matrix A associated to bilinear form b with respect to basis

B is a symmetric matrix. Every symmetric matrix is congruent to a diagonal matrix

$$\begin{pmatrix} \alpha_1 & 0 & ... & 0 & 0 \\ 0 & \alpha_2 & ... & 0 & 0 \\ 0 & 0 & ... & 0 & 0 \\ 0 & 0 & ... & \alpha_{n-1} & 0 \\ 0 & 0 & ... & 0 & \alpha_n \end{pmatrix},$$

therefore we will denote the vector space (V, b) with $< \alpha_1, ...\alpha_n >$.

Proposition 2.1.2. ([Sch; 85], Lemma 3.7.) *If $\sigma \in S_n$ is a permutation of degree n, therefore we have:*

1) $< \alpha_1, ...\alpha_n > \simeq < \alpha_{\sigma(1)}, ...\alpha_{\sigma(n)} >$;

2) For arbitrary non-zero elements $b_i \in K^*$, we have

$< \alpha_1, ...\alpha_n > \simeq < b_1^2\alpha_1, ...b_n^2\alpha_n >$.□

Definition. 2.1.3. [La; 04] A regular bilinear space (V, b) of dimension two isomorphic to $< 1, -1 >$ is called *hyperbolic plane.*

Proposition 2.1.4. ([Sch; 85], Theorem 4.5.) *Let (V, b) be a regular bilinear space of dimension $2n$. The following conditions are equivalent:*

i) V contains a totally isotropic subspace W of dimension n.

ii) $(V, b) \cong < 1, ..., 1, -1, ..., -1 > \simeq < 1, -1, ..., 1, -1 >$.□

A space which satisfies one of the equivalent conditions of the above proposition is called a *hyperbolic space.*

Proposition 2.1.5. ([Sch; 85], Corollary 4.6.) *Let (V, b) be a regular bilinear space of dimension 2. The following conditions are equivalent:*

i) (V, b) is isotropic;

ii) $(V, b) \simeq < 1, -1 >$.□

Definition 2.1.6. [La; 04] Let $A = (a_{ij}) \in \mathcal{M}_n(K), B = (b_{ij}) \in \mathcal{M}_m(K)$ be two square matrices. The matrix $A \otimes B \in \mathcal{M}_{mn}(K)$, defined as follows

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & a_{13}B & ... & a_{1n}B \\ ... & ... & ... & ... & ... \\ a_{m1}B & a_{m1}B & a_{m1}B & ... & a_{mn}B \end{pmatrix}$$

is called the *tensor product* of the matrix A and B.

Let φ be a $n-$dimensional quadratic irreducible form over the field K, $n \in N, n > 1$, which is not isometric to the *hyperbolic plane,*$< 1, -1 >$. We can consider φ as a homogeneous polynomial of degree 2,

$$\varphi(X) = \varphi(X_1, ...X_n) = \sum a_{ij} X_i X_j, a_{ij} \in K^*.$$

We define the *function field of* φ, denoted by $K(\varphi)$, as the quotient field of the integral domain

$$K[X_1, ..., X_n] / (\varphi(X_1, ..., X_n)).$$

Since $(X_1, ..., X_n)$ is a non-trivial zero, φ is isotropic over $K(\varphi)$.

Example 2.1.7. In the polynomial ring $K[X_1, X_2]$, we consider the ideal generated by the irreducible polynomial $\varphi(X_1, X_2) = X_1^2 + X_2^2$. Therefore, the function field of φ is the field $K(X_1)\left(\sqrt{-X_1^2}\right)$.

Considering $n \in \mathbb{N} - \{0\}$, we define a *$n-$fold Pfister form* over K a quadratic form of the type

$$< 1, a_1 > \otimes ... \otimes < 1, a_n >, a_1, ..., a_n \in K^*.$$

A Pfister form is denoted by $\ll a_1, a_2, ..., a_n \gg$. For $n \in N, n > 1,$ a Pfister form φ can be written as

$$< 1, a_1 > \otimes ... \otimes < 1, a_n > =< 1, a_1, a_2, ..., a_n, a_1a_2, ..., a_1a_2a_3, ..., a_1a_2...a_n > .$$

If $\varphi =< 1 > \perp \varphi'$, then φ' is called *the pure subform* of φ. It is known that a Pfister form is hyperbolic if and only if is isotropic. Therefore a Pfister form is isotropic if and only if its pure subform is isotropic.(See [Sch; 85])

For a field L, we define

$$L^\infty = L \cup \{\infty\},$$

where $x + \infty = x$, for $x \in L$, $x\infty = \infty$ for $x \in L^*, \infty\infty = \infty, \frac{1}{\infty} = 0, \frac{1}{0} = \infty$.

An *$L-$place* of the field K is a map $\lambda : K \to L^\infty$ with the properties:

$$\lambda(x + y) = \lambda(x) + \lambda(y), \lambda(xy) = \lambda(x)\lambda(y),$$

whenever the right sides are defined.

Theorem 2.1.8. ([Kn; 76], Theorem 3.3.) *Let F be a field of characteristic $\neq 2$, φ be a quadratic form over F and K an extension of the field F. If φ_K is isotropic, then there exist an $F-$place from $F(\varphi)$ to K.*

A subset P of K is called an *ordering* of K^* if

$$P + P \subset P, PP \subset P, P \cup -P = K^*.$$

A field K with an ordering is called an *ordered* field, the elements from P are called positive and from $-P$ are called negative. For $x, y \in K$, K an ordered field, we define $x > y$ if $(x - y) \in P$.

A field K is called a *formally real field* if -1 is not a sum of squares in K. Since each element from a finite field is a sum of squares (see Proposition 3.7. from [Sch, 85]), it results that a finite field is not a formally real field. Therefore, a formally real field has characteristic equal with 0.

A *quadratic semi-ordering* (or a *q-ordering*) of a field K is a subset P of K with the following properties:

$$P + P \subset P, K^2P \subset P, 1 \in P, P \cup -P = K, P \cap -P = \{0\}.$$

We define $x \geq y$ if $(x - y) \in P$. We remark that if the field K contains a q-ordering, therefore K is a formally real field.

Obviously, every ordering is a q-ordering ([La; 04],[Sch; 85]). A *q-preordering* is a subset P_0 of K such that

$$P_0 + P_0 \subset P_0, K^2P_0 \subset P_0, P_0 \cap -P_0 = \{0\}.$$

Then there is a q-ordering P such that $P_0 \subset P$ or $-P_0 \subset P$. (Lemma 7.3, [Sch; 85], p.133)

If $\varphi \simeq < a_1, ..., a_n >$ is a quadratic form over a formally real field K and P is an ordering on K, *the signature* of φ at P is

$$sgn(\varphi) = |\{i \mid a_i >_P 0\}| - |\{i \mid a_i <_P 0\}|.$$

The quadratic form q is *indefinite* at ordering P if $\dim \varphi > |sgn(\varphi)|$.

Proposition 2.1.9. ([Sch;85], p. 17, [La; 04], p.12)

i) Let (V_1, b_1) *and* (V_2, b_2) *be two isomorphic bilinear spaces with orthogonal decompositions* $V_1 = V_1' \perp V_1'', V_2 = V_2' \perp V_2''$, *such that* V_1' *and* V_2' *are regular subspaces and* $V_1' \simeq V_2'$. *Therefore* $V_1'' \simeq V_2''$.(The Witt Cancellation Law)

ii) For a bilinear subspace (V, b), *all its maximal totally isotropic subspaces have the same dimension.* □

Definition 2.1.10. For a regular bilinear space (V, b), the dimension of maximal totally isotropic subspaces is called *the Witt index* of (V, b) and will denote it by $i_W(V)$.

Proposition 2.1.11. ([Sch;85], Corollary 5.1, [La; 04] Corollary 4.4.) *If a bilinear space* (V, b) *has* $i_W(V) = m$, *therefore* V *has the following orthogonal decomposition*

$$V = H_1 \perp H_2 \perp ... \perp H_m \perp V',$$

where V' *is anisotropic, unique determined up an isomorphism, and* $H_1, H_2, ..., H_m$ *are hyperbolic planes.*□

A quadratic form ψ is a *subform* of the form φ if $\varphi \simeq \psi \perp \phi$, for some quadratic form ϕ. We denote $\psi < \varphi$.

From the above proposition, the *Witt index* of a quadratic form φ, denoted by $i_W(\varphi)$, is the dimension of a maximal totally isotropic subform of φ. Indeed, if

$$\varphi \simeq \varphi_{an} \perp \varphi_h,$$

with φ_{an} anisotropic and φ_h hyperbolic, the Witt index of φ is $\frac{1}{2}\dim \varphi_h$. The *first Witt index* of a quadratic form φ is the Witt index of φ over its function field and is denoted by $i_1(\varphi)$. The *essential dimension* of φ is

$$\dim_{es}(\varphi) = \dim(\varphi) - i_1(\varphi) + 1.$$

(see [Sch; 85])

2.2. Brown's construction of division algebras

Generally, algebras A_t of dimension 2^t obtained by the Cayley-Dickson process are not division algebras for all $t \geq 1$. But we can find fields on which, if we apply the Cayley-Dickson process, the resulting algebras A_t are division algebras for all $t \geq 1$. For example, we can consider the power-series field $K\{X_1, X_2, ..., X_t\}$ or the rational function field $K(X_1, X_2, ..., X_t)$, where $X_1, X_2, ..., X_t$ are t algebraically independent indeterminates over the field K.

In 1967, R. B. Brown constructed, for each t, a division algebra A_t of dimension 2^t over the power-series field $K\{X_1, X_2, ..., X_t\}$. We will present this construction, using polynomial rings over K and their field of fractions (the rational function field) instead of power-series fields over K (as it was used by R.B. Brown, see [Br; 67]).

For each t, we will construct a division algebra A_t over a field F_t, as follows. Let $X_1, X_2, ..., X_t$ be t algebraically independent indeterminates over the field K and

$$F_t = K(X_1, X_2, ..., X_t)$$

be the rational function field. For $i = 1, ..., t$, we building the algebra A_i over the rational function field $K(X_1, X_2, ..., X_i)$ by setting $\alpha_j = X_j$ for $j = 1, 2, ..., i$. Let $A_0 = K$. Using induction over i, supposing that A_{i-1} is a division algebra over the field $F_{i-1} = K(X_1, X_2, ..., X_{i-1})$, we can prove that the algebra A_i is a division algebra over the field $F_i = K(X_1, X_2, ..., X_i)$.

Let

$$A_{F_i}^{i-1} = F_i \otimes_{F_{i-1}} A_{i-1}.$$

For $\alpha_i = X_i$ we apply the Cayley-Dickson process to the algebra $A_{F_i}^{i-1}$. The resulting algebra, denoted by A_i, is an algebra over the field F_i with the dimension 2^i.

Let

$$x = a + bv_i,\ y = c + dv_i,$$

be nonzero elements in A_i such that $xy = 0$, where $v_i^2 = \alpha_i$. Since

$$xy = ac + X_i\bar{d}b + (b\bar{c} + da)\, v_i = 0,$$

we obtain

$$ac + X_i\bar{d}b = 0 \tag{2.2.1.}$$

and

$$b\bar{c} + da = 0. \tag{2.2.2.}$$

The elements $a, b, c, d \in A_{F_i}^{i-1}$ are non zero elements. Indeed, we have:

i) If $a = 0$ and $b \neq 0$, then $c = d = 0 \Rightarrow y = 0$, false;

ii) If $b = 0$ and $a \neq 0$, then $d = c = 0 \Rightarrow y = 0$, false;

iii) If $c = 0$ and $d \neq 0$, then $a = b = 0 \Rightarrow x = 0$, false;

iv) If $d = 0$ and $c \neq 0$, then $a = b = 0 \Rightarrow x = 0$, false.

It results that $b \neq 0, a \neq 0$, $d \neq 0$, $c \neq 0$. If $\{1, f_2, ..., f_{2^{i-1}}\}$ is a basis in A_{i-1}, then $a = \sum_{j=1}^{2^{i-1}} g_j(1 \otimes f_j) = \sum_{j=1}^{2^{i-1}} g_j f_j, g_j \in F_i, g_j = \frac{g_j'}{g_j''}, g_j', g_j'' \in K[X_1, ..., X_i]$, $g_j'' \neq 0$, $j = 1, 2, ...2^{i-1}$, where $K[X_1, ..., X_t]$ is the polynomial ring. Let a_2 be the less common multiple of $g_1'', ...g_{2^{i-1}}''$, then we can write

$a = \frac{a_1}{a_2}$, where $a_1 \in A_{F_i}^{i-1}, a_1 \neq 0$. Analogously, $b = \frac{b_1}{b_2}, c = \frac{c_1}{c_2}, d = \frac{d_1}{d_2}, b_1, c_1, d_1 \in A_{F_i}^{i-1} - \{0\}$ and $a_2, b_2, c_2, d_2 \in K[X_1, ..., X_t] - \{0\}$.

If we replace in relations (2.2.1.) and (2.2.2.), we obtain

$$a_1c_1d_2b_2 + X_i\bar{d}_1b_1a_2c_2 = 0 \tag{2.2.3.}$$

and

$$b_1\bar{c}_1d_2a_2 + d_1a_1b_2c_2 = 0. \tag{2.2.4.}$$

If we denote

$$a_3 = a_1b_2, b_3 = b_1a_2, c_3 = c_1d_2, d_3 = d_1c_2,$$

$a_3, b_3, c_3, d_3 \in A_{F_i}^{i-1} - \{0\}$, relations (2.2.3.) and (2.2.4.) become

$$a_3c_3 + X_i\bar{d}_3b_3 = 0 \tag{2.2.5.}$$

and

$$b_3\bar{c}_3 + d_3a_3 = 0. \tag{2.2.6.}$$

Since the algebra $A_{F_i}^{i-1} = F_i \otimes_{F_{i-1}} A_{i-1}$ is an algebra over F_{i-1} with basis $X^i \otimes f_j$, $i \in \mathbb{N}$ and $j = 1, 2, ...2^{i-1}$, we can write a_3, b_3, c_3, d_3 as

$$a_3 = \sum_{j \geq m} x_j X_i^j, b_3 = \sum_{j \geq n} y_j X_i^j, c_3 = \sum_{j \geq p} z_j X_i^j, d_3 = \sum_{j \geq r} w_j X_i^j,$$

where $x_j, y_j, z_j, w_j \in A_{i-1}, x_m, y_n, z_p, w_r \neq 0$. Since A_{i-1} is a division algebra, it follows that $x_m z_p \neq 0, w_r y_n \neq 0$, $y_n z_p \neq 0, w_r x_m \neq 0$. Using relations (2.2.5.) and (2.2.6.), we obtain that

$$2m + p + r = 2n + p + r + 1,$$

which is false. Therefore, the algebra A_i is a division algebra over the field $F_i = K(X_1, X_2, ..., X_i)$ of dimension 2^i.

2.3. Levels and sublevels of algebras obtained by the Cayley-Dickson process

In the following, we assume that all quadratic forms are nondegenerate.

Definition 2.3.1. We consider K a field. The *level* of the field K, denoted by $s(K)$, is the smallest natural number n such that -1 is a sum of n squares of K. If -1 is not a sum of squares of K, then $s(K) = \infty$.The definition is the same for the commutative rings.

The *level* of the algebra A, denoted by $s(A)$, is the least integer n such that -1 is a sum of n squares in A.

The *sublevel* of the algebra A, denoted by $\underline{s}(A)$, is the least integer n such that 0 is a sum of $n+1$ nonzero squares of elements in A.

If these numbers do not exist, then the level and sublevel are infinite. Obviously, $\underline{s}(A) \leq s(A)$.

A. Pfister, in [Pf; 65], proved that if a field has a finite level then this level is a power of 2 and any power of 2 can be realised as the level of a field. The level of division algebras is defined in the same manner as for the fields

and was intensively studied in several papers, as for example: [Le; 90], [Lew; 89], [Lew; 06] . In [Lew; 87], D. W. Lewis constructed quaternion division algebras of level 2^k and $2^k + 1$ for all $k \in \mathbb{N} - \{0\}$ and he asked if there exist quaternion division algebras whose levels are not of this form. Using function field techniques, these values were recovered for the quaternions by Laghribi and Mammone in [La,Ma; 01]. Using the same technique, in [Pu; 05], Susanne Pumplün constructed octonion division algebras of level 2^k and $2^k + 1$ for all $k \in \mathbb{N} - \{0\}$. In [Hoff; 08], D. W. Hoffman proved that there are many other values, other than 2^k or $2^k + 1$, which can be realised as a level of quaternion division algebras. In fact, he showed that for each $k \in \mathbb{N}$, $k \geq 2$, there exist quaternion division algebras D with level $s(D)$ bounded by the values $2^k + 2$ and $2^{k+1} - 1$ (i.e. $2^k + 2 \leq s(D) \leq 2^{k+1} - 1$). In [Kr, Wa; 91], M. Kűskemper and A. Wadsworth constructed the first example of a quaternion algebra of sublevel 3. Starting from this construction, in [O' Sh; 07(1)], J. O' Shea proved the existence of an octonion algebra of sublevel 3 and constructed an octonion algebra of sublevel 5. The existence of a quaternion algebra of sublevel 5 is still an open question. In [O' Sh; 10], Theorem 3.6., O'Shea proved the existence of an octonion division algebras of level 6 and 7. These values, 6 and 7, are still the only known exact values for the level of octonion division algebras, other than 2^k or $2^k + 1$, $k \in \mathbb{N} - \{0\}$. It is still not known which exact numbers could be realised as levels and sublevels of quaternion and octonion division algebras but, for the integral domains, this problem was solved in [Da, La, Pe; 80], when Z.D. Dai, T. Y. Lam and C. K. Peng proved that any positive integer n can be realised as the level of an integral domain, namely the ring

$$R_n = R[X_1, X_2, ..., X_n] / \left(1 + X_1^2 + X_2^2 + ... + X_n^2\right)$$

has the level n.

Cassels-Pfister Theorem. *Let $\varphi, \psi =< 1 > \perp \psi'$ be two quadratic forms over a field K with $charK \neq 2$. If φ is anisotropic over K and $\varphi_{K(\psi)}$ is hyperbolic, then $\alpha\psi < \varphi$ for any scalar represented by φ. In particular,* $\dim \varphi \geq \dim \psi$.(La, Ma;01, p.1823, Theorem 1.3.)

Springer's Theorem. *Let φ_1, φ_2 be two quadratic forms over a field K and $K(X)$ be the rational function field over K. Then, the quadratic form*

$\varphi_1 \perp X\varphi_2$ is isotropic over $K(X)$ if and only if φ_1 or φ_2 is isotropic over K.(La, Ma;01, p.1823, Theorem 1.1.)

Let A_t be an algebra obtained by the Cayley-Dickson process, with the set $\{1, f_2, ..., f_q\}, q = 2^t$ as a basis with the properties:

$$f_i^2 = \alpha_i 1,\ \alpha_i \in K, \alpha_i \neq 0,\ i = 2, ..., q$$

and

$$f_i f_j = -f_j f_i = \beta_{ij} f_k,\ \beta_{ij} \in K,\ \beta_{ij} \neq 0, i \neq j, i, j = 2, ...q,$$

β_{ij} and f_k being uniquely determined by f_i and f_j.

If

$$x \in A_t, x = x_1 1 + \sum_{i=2}^{q} x_i f_i,$$

then

$$\bar{x} = x_1 1 - \sum_{i=2}^{q} x_i f_i$$

and

$$\mathbf{t}(x) = 2x_1, \mathbf{n}(x) = x_1^2 - \sum_{i=2}^{q} \alpha_i x_i^2.$$

In the above decomposition of x, we call x_1 the *scalar part* of x and $x'' = \sum_{i=2}^{q} x_i f_i$ the *pure part* of x. If we compute

$$x^2 = x_1^2 + x''^2 + 2x_1 x'' =$$

$$= x_1^2 + \alpha_1 x_2^2 + \alpha_2 x_3^2 - \alpha_1\alpha_2 x_4^2 + \alpha_3 x_5^2 - ... - (-1)^t (\prod_{i=1}^{t} \alpha_i) x_q^2 + 2x_1 x'',$$

the scalar part of x^2 is represented by the quadratic form

$$T_C =< 1, \alpha_1, \alpha_2, -\alpha_1\alpha_2, \alpha_3, ..., (-1)^t (\prod_{i=1}^{t} \alpha_i) >=< 1, \beta_2, ..., \beta_q > \qquad (2.3.1.)$$

and, since

$$x''^2 = \alpha_1 x_2^2 + \alpha_2 x_3^2 - \alpha_1\alpha_2 x_4^2 + \alpha_3 x_5^2 - ... - (-1)^t (\prod_{i=1}^{t} \alpha_i) x_q^2 \in K,$$

is represented by the quadratic form $T_P = T_C \mid_{A_0} : A_0 \to K$,

$$T_P =< \alpha_1, \alpha_2, -\alpha_1\alpha_2, \alpha_3, ..., (-1)^t (\prod_{i=1}^{t} \alpha_i) >=< \beta_2, ..., \beta_q > . \qquad (2.3.2.)$$

The quadratic form T_C is called *the trace form*, and T_P *the pure trace form* of the algebra A_t. We remark that $T_C =< 1 > \perp T_P$, and the norm $\mathbf{n} = \mathbf{n}_C =< 1 > \perp -T_P$, resulting that

$$\mathbf{n}_C =< 1, -\alpha_1, -\alpha_2, \alpha_1\alpha_2, \alpha_3, ..., (-1)^{t+1} (\prod_{i=1}^{t} \alpha_i) >=< 1, -\beta_2, ..., -\beta_q > .$$

The norm form $\mathbf{n}_C$ has the form

$$\mathbf{n}_C =< 1, -\alpha_1 > \otimes ... \otimes < 1, -\alpha_t >$$

and it is a Pfister form.

Since the scalar part of any element $y \in A_t$ is $\frac{1}{2}\mathbf{t}(y)$, it follows that

$$T_C(x) = \frac{\mathbf{t}(x^2)}{2}.$$

Proposition 2.3.2.([Fl; 11] *For an algebra A obtained by the Cayley-Dickson process and with the above notations, we have:*

i) If $s(A) \leq n$ then -1 is represented by the quadratic form $n \times T_C$.

ii) -1 is a sum of n squares of pure elements in A if and only if the quadratic form $n \times T_P$ represents -1.

iii) For $n \in \mathbb{N} - \{0\}$, if the quadratic form $< 1 > \perp n \times T_P$ is isotropic over K, then $s(A) \leq n$.

Proof. i) Let $y \in A, y = x_1 + x_2 f_2 + ... + x_q f_q$, $x_i \in K$, for all $i \in \{1, 2, ..., q\}$. Using the notations given above, we get

$$y^2 = x_1^2 + \beta_2 x_2^2 + ... + \beta_q x_q^2 + 2x_1 y'',$$

where

$$y'' = x_2 f_2 + ... + x_q f_q.$$

If -1 is a sum of n squares in A, then

$$-1 = y_1^2 + ... + y_n^2 =$$

$$\begin{aligned} = \quad & \left(x_{11}^2+\beta_2 x_{12}^2+...+\beta_q x_{1q}^2+2x_{11}y_1''\right)+... \\ & +\left(x_{n1}^2+\beta_2 x_{n2}^2+...+\beta_q x_{nq}^2+2x_{n1}y_n''\right). \end{aligned}$$

Then we have

$$-1 = \sum_{i=1}^{n} x_{i1}^2 + \beta_2 \sum_{i=1}^{n} x_{i2}^2 + ... + \beta_q \sum_{i=1}^{n} x_{iq}^2$$

and

$$\sum_{i=1}^{n} x_{i1}x_{i2} = \sum_{i=1}^{n} x_{i1}x_{i3} = ... = \sum_{i=1}^{n} x_{i1}x_{in} = 0,$$

then $n \times T_C$ represents -1.

ii) With the same notations, if -1 is a sum of n squares of pure elements in A, then

$$-1 = y_1^2 + ... + y_n^2 =$$

$$\begin{aligned} = \quad & \left(\beta_2 x_{12}^2+...+\beta_q x_{1q}^2 + 2x_{11}y_1''\right)+... \\ & +\left(\beta_2 x_{n2}^2+...+\beta_q x_{nq}^2 + 2x_{n1}y_n''\right). \end{aligned}$$

We have

$$-1 = \beta_2 \sum_{i=1}^{n} x_{i2}^2 + ... + \beta_q \sum_{i=1}^{n} x_{iq}^2.$$

Therefore $n \times T_P$ represents -1. Reciprocally, if $n \times T_P$ represents -1, then

$$-1 = \beta_2 \sum_{i=1}^{n} x_{i2}^2 + ... + \beta_q \sum_{i=1}^{n} x_{iq}^2.$$

Let

$$u_i = x_{i2}^2 f_2 + ... + x_{iq}^2 f_q.$$

It results $\mathbf{t}(u_i) = 0$ and

$$u_i^2 = -\mathbf{n}(u_i) = \beta_2 x_{i2}^2 + ... + \beta_q x_{iq}^2,$$

for all $i \in \{1, 2, ..., n\}$. We obtain

$$-1 = u_1^2 + ... + u_n^2.$$

iii) **Case 1.** If $-1 \in K^{*2}$, then $s(A) = 1$.

Case 2. $-1 \notin K^{*2}$. Since the quadratic form $< 1 > \perp n \times T_P$ is isotropic then it is universal. It results that $< 1 > \perp n \times T_P$ represent -1. Then, we have the elements $\alpha \in K$ and $p_i \in A_0$, $i = 1, ..., n$, such that

$$-1 = \alpha^2 + \beta_2 \sum_{i=1}^{n} p_{i2}^2 + ... + \beta_q \sum_{i=1}^{n} p_{iq}^2,$$

and not all of them are zero.

i) If $\alpha = 0$, then

$$-1 = \beta_2 \sum_{i=1}^{n} p_{i2}^2 + ... + \beta_q \sum_{i=1}^{n} p_{iq}^2.$$

It results

$$\begin{aligned} -1 \quad = \quad & \left(\beta_2 p_{12}^2 + ... + \beta_q p_{1q}^2\right) + ... \\ & + \left(\beta_2 p_{n2}^2 + ... + \beta_q p_{nq}^2\right). \end{aligned}$$

Denoting

$$u_i = p_{i2} f_2 + ... + p_{iq} f_q,$$

we have that $\mathbf{t}(u_i) = 0$ and

$$u_i^2 = -\mathbf{n}(u_i) = \beta_2 p_{i2}^2 + ... + \beta_q p_{iq}^2,$$

for all $i \in \{1, 2, ..., n\}$. We obtain $-1 = u_1^2 + ... + u_n^2$.

ii) If $\alpha \neq 0$, then $1 + \alpha^2 \neq 0$ and

$$0 = 1 + \alpha^2 + \beta_2 \sum_{i=1}^{n} p_{i2}^2 + ... + \beta_q \sum_{i=1}^{n} p_{iq}^2.$$

Multiplying this relation with $1 + \alpha^2$, it follows that

$$0 = (1 + \alpha^2)^2 + \beta_2 \sum_{i=1}^{n} r_{i2}^2 + ... + \beta_q \sum_{i=1}^{n} r_{iq}^2.$$

Therefore

$$-1 = \beta_2 \sum_{i=1}^{n} r_{i2}'^2 + ... + \beta_q \sum_{i=1}^{n} r_{iq}'^2,$$

where

$$r_{ij}' = r_{ij}(1+\alpha)^{-1}, j \in \{2, 3, ..., q\}$$

and we apply case i). Therefore $s(A) \leq n$.□

Proposition 2.3.3.([Fl; 11] *For the algebra A, obtained by the Cayley-Dickson process, the following statements are true:*

a) If $n \in \mathbb{N} - \{0\}$, such that $n = 2^k - 1$, for $k > 1$, then $s(A) \leq n$ if and only if $< 1 > \perp n \times T_P$ is isotropic.

b) If -1 is a square in K, then $\underline{s}(A) = s(A) = 1$.

c) If $-1 \notin K^{*2}$, then $s(A) = 1$ if and only if T_C is isotropic.

Proof. a) From Proposition 2.3.2, supposing that $s(A) \leq n$, we have

$$-1 = \sum_{i=1}^{n} p_{i1}^2 + \beta_2 \sum_{i=1}^{n} p_{i2}^2 + ... + \beta_q \sum_{i=1}^{n} p_{iq}^2$$

such that

$$\sum_{i=1}^{n} p_{i1}p_{i2} = \sum_{i=1}^{n} p_{i1}p_{i3} = ... = \sum_{i=1}^{n} p_{i1}p_{iq} = 0.$$

For the level reasons, it results that

$$1 + \sum_{i=1}^{n} p_{i1}^2 \neq 0.$$

Putting $p_{2^k 1} = 1$ and $p_{2^k 2} = p_{2^k 3} = ... \; p_{2^k q} = 0$, we have

$$0 = \sum_{i=1}^{n+1} p_{i1}^2 + \beta_2 \sum_{i=1}^{n+1} p_{i2}^2 + ... + \beta_q \sum_{i=1}^{n+1} p_{iq}^2 \qquad (2.3.3.)$$

and

$$\sum_{i=1}^{n+1} p_{i1}p_{i2} = \sum_{i=1}^{n+1} p_{i1}p_{i3} = ... = \sum_{i=1}^{n+1} p_{i1}p_{iq} = 0.$$

Multiplying (2.3.3) by $\sum_{i=1}^{n+1} p_{i1}^2$, since $\left(\sum_{i=1}^{n+1} p_{i1}^2\right)^2$ is a square and using Lemma from [Sch; 85], p.151, for the products

$$\sum_{i=1}^{n+1} p_{i2}^2 \sum_{i=1}^{n+1} p_{i1}^2, ..., \sum_{i=1}^{n+1} p_{iq}^2 \sum_{i=1}^{n+1} p_{i1}^2,$$

we obtain

$$0 = \left(\sum_{i=1}^{n+1} p_{i1}^2\right)^2 + \beta_2 \sum_{i=1}^{n+1} r_{i2}^2 + ... + \beta_q \sum_{i=1}^{n+1} r_{iq}^2, \qquad (2.3.4.)$$

where

$$r_{i2}, ...r_{iq} \in K, n+1 = 2^k,$$

$$r_{12} = \sum_{i=1}^{n+1} p_{i1}p_{i2} = 0,\ r_{13} = \sum_{i=1}^{n+1} p_{i1}p_{i3} = 0, ..., r_{1q} = \sum_{i=1}^{n+1} p_{i1}p_{iq} = 0.$$

Therefore, in the sums $\sum_{i=1}^{n+1} r_{i2}^2$, ..., $\sum_{i=1}^{n+1} r_{iq}^2$ we have n factors. From (2.3.4), we get that $< 1 > \perp n \times T_P$ is isotropic.

b) If $-1 = a^2 \in K \subset A$, then $\underline{s}(A) = s(A) = 1$.

c) If $-1 \notin K^{*2}$ and $s(A) = 1$, then, there is an element $y \in A \backslash K$ such that $-1 = y^2$. Hence $y \in A_0$, so $\overline{y} = -y$. It results that

$$(1+y)^2 = 1 + 2y + y^2 = 2y$$

and

$$T_C(1+y) = \frac{1}{2} t\left((1+y)^2\right) = \frac{1}{2}\left(2y + \overline{2y}\right) = y - y = 0.$$

Therefore T_C is isotropic.

Conversely, if $T_C = < 1 > \perp T_P$ is isotropic, from Proposition 2.3.2., iii), we have then $s(A) = 1$.□

Proposition 2.3.4.([Fl; 11]) *The quadratic form $2^k \times T_C$ is isotropic if and only if $< 1 > \perp 2^k \times T_P$ is isotropic.*

Proof. Since the form $< 1 > \perp 2^k \times T_P$ is a subform of the form $2^k \times T_C$, if the form $< 1 > \perp 2^k \times T_P$ is isotropic, we have that $2^k \times T_C$ is isotropic.

For the converse, supposing that $2^k \times T_C$ is isotropic, then we get

$$\sum_{i=1}^{2^k} p_i^2 + \beta_2 \sum_{i=1}^{2^k} p_{i2}^2 + ... + \beta_q \sum_{i=1}^{2^k} p_{iq}^2 = 0, \tag{2.3.5.}$$

where $p_i, p_{ij} \in K, i = 1, ..., 2^k$, $j \in 2, ..., q$ and some of the elements p_i and p_{ij} are nonzero.

If $p_i = 0, \forall i = 1, ..., 2^k$, then $2^k \times T_P$ is isotropic, therefore $< 1 > \perp 2^k \times T_P$ is isotropic.

If

$$\sum_{i=1}^{2^k} p_i^2 \neq 0,$$

then, multiplying relation (2.3.5) with $\sum\limits_{i=1}^{2^k} p_i^2$ and using Lemma from [Sch; 85] p.151, for the products

$$\sum_{i=1}^{2^k} p_{i2}^2 \sum_{i=1}^{2^k} p_i^2, ..., \sum_{i=1}^{2^k} p_{iq}^2 \sum_{i=1}^{2^k} p_i^2,$$

we obtain

$$(\sum_{i=1}^{2^k} p_i^2)^2 + \beta_2 \sum_{i=1}^{2^k} r_{i2}^2 + ... + \beta_q \sum_{i=1}^{2^k} r_{iq}^2 = 0,$$

then $< 1 > \perp 2^k \times T_P$ is isotropic.

For the level reason, the relation $\sum\limits_{i=1}^{2^k} p_i^2 = 0$, for some $p_i \neq 0$, does not work. Indeed, supposing that $p_1 \neq 0$, we obtain

$$-1 = \sum_{i=2}^{2^k} (p_i p_1^{-1})^2,$$

false.□

Remark 2.3.5. i) If the algebra A, obtained by the Cayley-Dickson process, is a division algebra, then its norm form, $\mathbf{n}_C^A$, is anisotropic. However there are algebras A obtained by the Cayley-Dickson process with the norm

form $\mathbf{n}_C^A$ anisotropic which are not division algebras. For example, if $K = \mathbb{R}$ and $t = 4$, the real sedenion algebra

$$\left(\frac{-1,-1,-1,-1}{\mathbb{R}}\right)$$

with the basis $\{1, f_1, ..., f_{15}\}$ has the norm form anisotropic and is not a division algebra. For example, $(f_3 + f_{10})(f_6 - f_{15}) = 0$.

ii) Using Proposition 2.3.3, if the algebra A is an algebra obtained by the Cayley-Dickson process of dimension greater than 2 and if $\mathbf{n}_C^A$ is isotropic, then $s(A) = \underline{s}(A) = 1$. Indeed, if -1 is a square in K, the statement follows from the above. If $-1 \notin K^{*2}$, since $\mathbf{n}_C =< 1 > \perp -T_P$ and n_C is a Pfister form, we obtain that $-T_P$ is isotropic, therefore T_C is isotropic and, from the above proposition, it results that $s(A) = \underline{s}(A) = 1$.

In the following, we consider A, an algebra obtained by the Cayley-Dickson process over a field K, having dimension $q = 2^t$. For the algebra A,let T_C, T_P, $\mathbf{n}_C$ be its trace, pure trace and norm forms, respectively.

Theorem 2.3.6.([Fl; 13]) *We consider A an algebra of dimension 2^t obtained by the Cayley-Dickson process, of finite level, over a field K. Therefore*

$$\underline{s}(A) \leq s(A) \leq \underline{s}(A) + 1.$$

Proof. Denoting $n = \underline{s}(A)$, we find the nonzero elements

$$u_i = x_{i1} + x_{i2}f_2 + ... + x_{iq}f_q \in A,$$

with

$$u_i'' = x_{i2}f_2 + ... + x_{iq}f_q \in A$$

the pure part of u_i, where $x_{ij} \in K, i \in \{1, 2, ..., n+1\}, j \in \{1, 2, ..., q\}, q = 2^t$, such that $0 = u_1^2 + ... + u_{n+1}^2$. We obtain

$$\sum_{i=1}^{n+1}(x_{i1}^2 + (u_i'')^2 + 2x_{i1}u_i'') = 0,$$

therefore

$$\sum_{i=1}^{n+1} x_{i1}^2 + \sum_{i=1}^{n+1}(u_i'')^2 = 0$$

and

$$\sum_{i=1}^{n+1} x_{i1}u_i'' = 0.$$

Case 1. If $x_{i1} = 0, \forall\ i \in \{1, 2, ..., n+1\}$. It results that

$$\sum_{i=1}^{n+1} (u_i'')^2 = 0,$$

hence, it follows that $(n+1) \times T_P$ is isotropic, therefore it contains $< 1, -1 >$ as a subform. We obtain that -1 is represented by the form $(n+1) \times T_P$. Therefore, -1 is a sum of square of $(n+1)$ pure elements from A, hence $s(A) \leq n+1$.

Case 2. There are at least two elements $x_{i1} \neq 0$ such that

$$\sum_{i=1}^{n+1} x_{i1}^2 = 0.$$

Since the elements $(u_i'')^2 \in K$ for all $i \in \{1, 2, ..., n+1\}$, it results that $s(A) \leq s(K)$. But $\underline{s}(K) = s(K) \leq n$, hence $s(A) \leq n$.

Case 3. If

$$\sum_{i=1}^{n+1} x_{i1}^2 \neq 0,$$

we denote $d_i = \dfrac{x_{i1}}{D} \in K$, where

$$D = \sum_{i=1}^{n+1} x_{i1}^2.$$

It follows that

$$\sum_{i=1}^{n+1} d_i u_i = \frac{1}{D} \sum_{i=1}^{n+1} (x_{i1}^2 + x_{i1}u_i'') = 1,$$

since $\sum\limits_{i=1}^{n+1} x_{i1}u_i'' = 0$. We obtain

$$\sum_{i=1}^{n+1} \left(\left(\frac{D^{-1}+1}{2} \right) u_i - d_i \right)^2 =$$

$$= \left(\frac{D^{-1}+1}{2}\right)^2 \sum_{i=1}^{n+1} {u_i}^2 - \left(D^{-1}+1\right) \sum_{i=1}^{n+1} u_i d_i + \sum_{i=1}^{n+1} d_i^2 =$$
$$= -\left(D^{-1}+1\right) + D^{-1} = -1,$$

therefore $s(A) \leq n+1$.□

If A is a division algebra of dimension ≤ 8, the above result is a consequence of the main Theorem from [Hoff; 10].

Theorem 2.3.7.([Fl; 13]) *Let K be a field, X be an algebraically independent indeterminate over K, A be a finite-dimensional $K-$algebra with finite level $s(A)$ and the scalar involution $^-$. Let $k(A)$ be the least number such that the form $k \times \mathbf{n}_C^A$ is isotropic over K, where $\mathbf{n}_C^A$ is the norm form of the algebra A, let $A_1 = K(X) \otimes_K A$ and $B = (A_1, X)$. Then:*

i) If A is a division algebra, then B is a division algebra.

ii) $s(B) = \min\{s(A),\ k(A)\}$.

iii) If $k(A) > 1$, $\underline{s}(B) = \min\{\underline{s}(A), k(A) - 1\}$.

Proof. i) It results by straightforward calculations, using the same arguments as in Brown's construction at step i, described above.

ii) We have $s(B) \leq s(A)$. Let $k = k(A)$. If $k \times \mathbf{n}_C^A$ is isotropic, it results that $k \times \mathbf{n}_C^{A_1}$ is isotropic and therefore universal and it represents $-X^{-1}$. Hence, there are elements $z_1, ..., z_k \in A_1$ such that

$$\sum_{i=1}^{k} n_C^{A_1}(z_i) = -X^{-1}.$$

Let $w_i \in B$, $w_i = z_i u, u \in B, u^2 = X$. Since $\mathbf{t}(w_i) = 0$, it follows that

$$w_i^2 = -\mathbf{n}_C^B(w_i) = X \mathbf{n}_C^{A_1}(z_i)$$

and

$$\sum_{i=1}^{k} w_i^2 = \sum_{i=1}^{k} X \mathbf{n}_C^{A_1}(z_i) = -1.$$

It results that $s(B) \leq k$, therefore $s(B) \leq \min\{s(A),\ k(A)\}$.

Conversely, assuming that $s(B) = n$, we have $-1 = y_1^2 + ... + y_n^2$, where $y_i \in B$, $y_i = a_{i1} + a_{i2} u$, $u^2 = X$, $a_{i1}, a_{i2} \in A_1$ and we obtain

$$y_i^2 = a_{i1}^2 + X \overline{a}_{i2} a_{i2} + \left(a_{i2} \overline{a}_{i1} + a_{i2} a_{i1}\right) u,$$

for $i \in \{1, 2, ...n-1\}$. It follows that

$$-1 = \sum_{i=1}^{n} a_{i1}^2 + X \sum_{i=1}^{n} \overline{a}_{i2} a_{i2},$$

where $\psi = 1 \otimes^{-}$ is involution in $A_1, \psi(x) = \bar{x}$. We remark that $\overline{a}_{i2} a_{i2} \in K(X)$, $i \in \{1, ..., n\}$. Let $\{1, f_2, ..., f_q\}, q = 2^t$, be a basis in A, therefore

$$a_{i1} = \sum_{j=1}^{m} \frac{p_{ji1}(X)}{q_{ji1}(X)} (1 \otimes f_j),$$

with $\dfrac{p_{ji1}(X)}{q_{ji1}(X)} \in K(X)$, and

$$a_{i2} = \sum_{j=1}^{m} \frac{r_{ji2}(X)}{w_{ji2}(X)} (1 \otimes f_j),$$

with

$\dfrac{r_{ji2}(X)}{w_{ji2}(X)} \in K(X)$, $i \in \{1, 2, ..., n\}$, $j \in \{1, 2, ..., m\}$. It results that

$$\text{-1}=\sum_{i=1}^{n}(\sum_{j=1}^{m}\frac{p_{ji1}(X)}{q_{ji1}(X)}(1\otimes f_j))^2+X\sum_{i=1}^{n}(\sum_{j=1}^{m}\frac{r_{ji2}(X)}{w_{ji2}(X)}(1\otimes f_j))((\sum_{j=1}^{m}\frac{r_{ji2}(X)}{w_{ji2}(X)}(1\otimes\overline{f_j})).$$

After clearing denominators, we obtain

$$\text{-}v^2(X)=\sum_{i=1}^{n}(\sum_{j=1}^{m}p'_{ji1}(X)(1\otimes f_j))^2+X\sum_{i=1}^{n}(\sum_{j=1}^{m}r'_{ji2}(X)(1\otimes f_j))((\sum_{j=1}^{m}r'_{ji2}(1\otimes\overline{f_j})), \tag{2.3.6.}$$

where

$$v(X) = lcm\{q_{ji1}(X),\ w_{ji2}(X)\},\ i \in \{1, 2, ..., n\},\ j \in \{1, 2, ..., m\}$$

and

$$p'_{ji1}(X) = v(X)\, p_{ji1}(X), r'_{ji2}(X) = v(X)\, r_{ji2}(X),\ i \in \{1,..., n\},\ j \in \{1, 2,...,m\}.$$

Case 1. If $p'_{ji1}(X)$ are not divisible by X, for some i and j, taking residues modulo X in (2.3.6), denoted with two-sided arrow, we obtain

$$\overleftrightarrow{-v^2(X)} = \sum_{i=1}^{n}(\overleftrightarrow{\sum_{j=1}^{m}p'_{ji1}(X)(1\otimes f_j)})^2.$$

In this relation, if $v(X)$ is not divisible by X, it results that $s(A)\leq n$. If $v(X)$ is divisible by X, we have $\underline{s}(A)\leq n-1$ and, from Theorem 2.3.6, we obtain $s(A)\leq n$.

Case 2. If $p'_{ji1}(X)$ are divisible by X, for all i and j, it results that $v(X)$ is divisible by X, then dividing relation (2.3.6) by X and taking residues modulo X, we obtain

$$\overleftrightarrow{0} = \sum_{i=1}^{n}(\overleftrightarrow{\sum_{j=1}^{m}r'_{ji2}(X)(1\otimes f_j)})((\sum_{j=1}^{m}r'_{ji2}(1\otimes\overline{f_j})).$$

It follows that the form $n\times\mathbf{n}_C^A$ is isotropic, therefore $k(A)\leq n$.

It results that $s(B)=\min\{s(A),\ k(A)\}$.

iii) Since $\underline{s}(B)\leq s(B)\leq s(A)$, then $\underline{s}(B)\leq\underline{s}(A)$. Let $k=k(A)$. We have that $k\times\mathbf{n}_C^A$ is isotropic, therefore $k\times\mathbf{n}_C^{A_1}$ is isotropic. Hence, there are the elements $z_1,...,z_k\in A_1$ such that $\sum\limits_{i=1}^{k}n_C^{A_1}(z_i)=0$. Let $w_i\in B$, $w_i=z_iu, u\in B, u^2=X$. Since $\mathbf{t}(w_i)$=0, we obtain w_i^2=$-\mathbf{n}_C^B(w_i)$=$X\mathbf{n}_C^{A_1}(z_i)$ and $\sum\limits_{i=1}^{k}w_i^2$=$\sum\limits_{i=1}^{k}X\mathbf{n}_C^{A_1}(z_i)$=0. It results that $\underline{s}(B)\leq k-1$, therefore

$$\underline{s}(B)\leq\min\{\underline{s}(A),k(A)-1\}.$$

Conversely, assuming that $\underline{s}(B)=n$, there are $y_1,...,y_{n+1}\in B$, non zero elements, such that $0=y_1^2+...+y_{n+1}^2$, $y_i=a_{i1}+a_{i2}u$, $u^2=X$, $a_{i1},a_{i2}\in A_1$. Using the same notations as in ii), after straightforward calculations, we obtain

$$\sum_{i=1}^{n+1}(\sum_{j=1}^{m}p'_{ji1}(X)(1\otimes f_j))^2+X\sum_{i=1}^{n+1}(\sum_{j=1}^{m}r'_{ji2}(X)(1\otimes f_j))((\sum_{j=1}^{m}r'_{ji2}(1\otimes\overline{f_j}))=0. \tag{2.3.7.}$$

Case 1. If $p'_{ji1}(X)$ are not divisible by X, for some i and j, taking residues

modulo X in relation (2.3.7), we obtain

$$\overleftrightarrow{0} = \sum_{i=1}^{n+1} (\overleftarrow{\sum_{j=1}^{m}} p'_{ji1}(X)(1 \otimes f_j))^2,$$

therefore $\underline{s}(A) \leq n$.

Case 2. If $p'_{ji1}(X)$ are divisible by X, for all i and j, then dividing relation (2.3.7) by X and taking residues modulo X, we obtain

$$\overleftrightarrow{0} = \sum_{i=1}^{n+1} (\overleftarrow{\sum_{j=1}^{m}} r'_{ji2}(X)(1 \otimes f_j))((\sum_{j=1}^{m} r'_{ji2}(1 \otimes \overline{f_j})),$$

therefore $k(A) \leq n+1$. It results that $\underline{s}(B) = \min\{\underline{s}(A), k(A) - 1\}$.□

Since $\underline{s}(B) \leq s(B) \leq s(A)$, in the above Theorem, we remark that if $k(A) = 1$ then $\underline{s}(B) = s(B) = s(A) = 1$. Results analogous to those in Theorem 2.3.7 are obtained for composition algebras in [Ti, Va; 87] and [O' Sh; 11].

Let A_t be a division algebra over the field $K = K_0(X_1, ..., X_t)$, obtained by the Cayley-Dickson process and Brown's construction of dimension $q = 2^t$, where K_0 is a formally real field, $X_1, ..., X_t$ are algebraically independent indeterminates over the field K_0, T_C and T_P are its trace and pure trace forms. Let

$$\varphi_n =< 1 > \perp n \times T_P, \psi_m =< 1 > \perp m \times T_C, n \geq 1,$$

$$A_t(n) = A_t \otimes_K K(< 1 > \perp n \times T_P), n \in \mathbb{N} - \{0\}. \quad (2.3.8.)$$

We denote $K_n = K(< 1 > \perp n \times T_P) = K(\varphi_n)$, and let $\mathbf{n}_C^{A_t}$ be the norm form of the algebra A_t.

Proposition 2.3.8.([Fl; 13])
i) The norm form $\mathbf{n}_C^{A_t(n)}$ is anisotropic over K_n.
ii) With the above notations, for $t \geq 2$, if $n = 2^k + 1$ then $2^k \times \mathbf{n}_C^{A_t(n)}$ is anisotropic over $K_0(X_1, X_2, ..., X_t)(\varphi_{2^k+1})$.

Proof. i) First, we consider $n > 1$. Since $\mathbf{n}_C^{A_t(n)}$ is a Pfister form and a Pfister form is isotropic if and only if it is hyperbolic, if $\mathbf{n}_C^{A_t(n)}$ is isotropic over

K_n, then it is hyperbolic. Since A_t is a division algebra, it follows that $\mathbf{n}_C^{A_t}$ is anisotropic. From Cassels-Pfister Theorem, for some $\alpha \in K^*$, we obtain that $\alpha\varphi_n$ is a subform of the norm form $\mathbf{n}_C^{A_t(n)}$. Since $\dim \varphi_n = 1 + n(2^t - 1)$ and $\dim \mathbf{n}_C^{A_t(n)} = 2^t$, therefore $\dim \varphi_n > \dim \mathbf{n}_C^{A_t(n)}$, false.

If $n = 1$, using the Cassels-Pfister Theorem, for some $\alpha \in K^*$, it results that $\alpha\varphi_1$ is a subform of the norm form $\mathbf{n}_C^{A_t(1)}$. Since $\dim \varphi_1 = \dim \mathbf{n}_C^{A_t(1)} = 2^t$ and the forms φ_1 and $\mathbf{n}_C^{A_t(1)}$ are not similar, we obtain a contradiction.

ii) We denote

$$\alpha_k = (2^k + 1) \times < 1, -X_1 > .$$

It results that $X_2\alpha_k$ is a subform of φ_{2^k+1}, then

$$K_0(X_1, X_2, ..., X_t)(\alpha_k) \simeq K_0(X_1, X_2, ..., X_t)(X_2\alpha_k).$$

If $2^k \times \mathbf{n}_C$ is isotropic over $K_0(X_1, X_2, ..., X_t)(\varphi_{2^k+1})$ there is a map

$$K_0(X_1, X_2, ..., X_t)\text{-place: } K_0(X_1, X_2, ..., X_t)(\varphi_{2^k+1}) \to K_0(X_1, X_2, ..., X_t)(\alpha_k),$$

and $2^k \times \mathbf{n}_C$ is isotropic over $K_0(X_1, X_2, ..., X_t)(\alpha_k)$ from [Kn; 76, Theorem 3.3.]. By repeatedly applying of Springer's Theorem, it results that the quadratic form $2^k \times < 1, -X_1 >$ is isotropic over $K_0(X_1)(\alpha_k)$, in contradiction with Proposition 2.2. from [La,Ma; 01]. □

Remark. 2.3.9. i) The algebra $A_t(n)$ has dimension 2^t and is not necessarily a division algebra, but, using Remark 2.3.5, this algebra is of level greater than 1.

ii) From Proposition 2.3.2 i) and iii), if ψ_m is anisotropic and φ_n is isotropic over K_n, then $s(A_t(n)) \in [m + 1, n]$.

Example 2.3.10. Using the same notations as those in Theorem 2.3.7, let F be a field of level 2^k. If $A = A_0 = F$, $K = F, A_1 = K(X_1) \otimes_K A_0$, since $k(A) \geq 2^k + 1$, we obtain the division $K(X_1)-$algebra B of dimension 2 and level and sublevel 2^k. Using the same Theorem, we can continue the induction steps. Assuming that $A = A_{t-1}$ is a division algebra of dimension 2^{t-1} and level 2^k over the field $K = F(X_1, ..., X_{t-1})$, then, from Springer's Theorem, it results that $k(A_{t-1}) \geq 2^k + 1$. If $A = A_{t-1}$, $A_1 = K(X_t) \otimes_K A_{t-1}$ and B is the $K(X_t)-$algebra obtained by application of the Cayley-Dickson process with

$\alpha = X_t$ to the $K(X_t)-$algebra A_1, then B is a division algebra of dimension 2^t and level and sublevel 2^k. This is an example of a division algebra of level and sublevel 2^k and dimension $2^t, t, k \in \mathbb{N} - \{0\}$.

Proposition 2.3.11. ([Fl; 13]) *$i_1(< 1 > \perp n \times T_P) = 1$ for all $n \in \mathbb{N} - \{0\}$, where T_P is the pure trace form for the algebra $A_t, t \geq 2$.*

Proof. Let P be an arbitrary ordering over K such that $\beta_2, ..., \beta_q <_P 0$. We remark that such an ordering always exists. Indeed, since φ_n is anisotropic over K (from Springer's Theorem), it follows that $P_0 = \{a \mid a = 0$ or a is represented by $\varphi_n \}$ is a $q-$preordering, therefore there is a $q-$ordering P containing P_0 or $-P_0$. We have

$$|sgn\varphi_n| = |sgn(< 1 > \perp n \times T_P)| = \left(2^t - 1\right) n - 1 < (2^t - 1)n + 1 = \dim \varphi_n.$$

It results that φ_n is indefinite at P over K, then P extends to K_n, from [Hoff; 08], Lemma 2.5. Since φ_n is isotropic over K_n, we obtain that

$$\dim((\varphi_n)_{K_n})_{an} \leq \left(2^t - 1\right) n - 1.$$

Since

$$\dim((\varphi_n)_{K_n})_{an} \geq |sgn\varphi_n| = \left(2^t - 1\right) n - 1,$$

then

$$\dim((\varphi_n)_{K_n})_{an} = \left(2^t - 1\right) n - 1 = \dim \varphi_n - 2$$

and therefore $i_1(\varphi_n) = \frac{1}{2}2 = 1$. □

Theorem 2.3.12. ([Fl; 13]) *With the above notations, we have*

$$s(A_t(n)) \in [n - [\frac{n}{2^t}], n],$$

for $t \geq 2$.

Proof. From Proposition 2.3.11, we have that

$$\dim \varphi_n - i_1(\varphi_n) = (2^t - 1)n + 1 - i_1(\varphi_n) = (2^t - 1)n.$$

For the quadratic form ψ_m, the relation

$$\dim \psi_m - i_1(\psi_m) = 2^t n + 1 - i_1(\psi_m)$$

holds. The forms φ_n and ψ_m are anisotropic over $K = K_0(X_1, ..., X_t)$, by Springer's Theorem. From [Ka, Me; 03], Theorem 4.1, if

$$\dim \psi_m - i_1(\psi_m) < \dim \varphi_n - i_1(\varphi_n) \tag{2.3.9.}$$

it results that ψ_m is anisotropic over K_n. From Proposition 2.3.11, we have $i_1(\varphi_n) = 1$ for all $n \in \mathbb{N} - \{0\}$, therefore, since $i_1(\psi_m) \geq 1$, if $\dim \psi_m < \dim \varphi_n$, we obtain relation (2.3.9). By straightforward calculations in relation (2.3.9), we obtain

$$2^t m + 1 - i_1(\psi_m) < (2^t - 1)n$$

and we remark that $n - [\frac{n}{2^t}] - 1$ is the highest value of $m \in \mathbb{N}$ such that the relation $\dim \psi_m < \dim \varphi_n$ holds. Hence, ψ_m is anisotropic over K_n for $m = n - [\frac{n}{2^t}] - 1$. From Remark 2.3.9, it results $s(A_t(n)) \geq n - [\frac{n}{2^t}]$.□

Theorem 2.3.13. ([Fl; 13]) *With the above notations, we have*

$$\underline{s}(A_t(n)) \in [n - [\frac{n + 2^t - 1}{2^t}], n],$$

where $n \in \mathbb{N} - \{0\}$, $t \geq 2$.

Proof. Using Proposition 2.3.2 i), if the quadratic form $\phi_m = (m + 1) \times T_C$ is anisotropic, then $\underline{s}(A_t(n)) \geq m + 1$ and if φ_n is isotropic, then $\underline{s}(A_t(n)) \leq n$. Using the same arguments as in the proof of Theorem 2.3.12, if

$$2^t(m + 1) - i_1(\phi_m) < (2^t - 1)n, \tag{2.3.10.}$$

we have ϕ_m is anisotropic over K_n, therefore

$$\underline{s}(A_t(n)) \in [m + 1, n].$$

Since $i_1(\phi_m) \geq 1$, the highest value of m such that relation (2.3.10) holds is $n - [\frac{n+2^t-1}{2^t}] - 1$. Indeed, relation (2.3.10) implies

$$2^t(m + 1) - 1 < (2^t - 1)n,$$

therefore

$$m < n\frac{2^t - 1}{2^t} + \frac{1}{2^t} - 1 = n - \frac{n + 2^t - 1}{2^t}$$

and we obtain

$$m \leq n - [\frac{n + 2^t - 1}{2^t}] - 1.$$

□

Theorem 2.3.12 and Theorem 2.3.13 generalize Theorem 3.8. from [O' Sh; 10].

Theorem 2.3.14. ([Fl; 13]) *With the above notation, for each* $n \in \mathbb{N} - \{0\}$ *there is an algebra* $A_t(n)$ *such that* $s(A_t(n)) = n$ *and* $\underline{s}(A_t(n)) \in \{n-1, n\}$.

Proof. Let $n \in \mathbb{N} - \{0\}$ and m be the least positive integer such that $n \leq 2^m$. For $n = 2^m$, there are quaternion $(A_2(n))$ and octonion $(A_3(n))$ division algebras of level $n = 2^m$, (see [La,Ma; 01] and [Pu; 05]). We assume that $n < 2^m$. With the above notations, for $t = m$, let $A_t(n)$ be the algebra of dimension $q = 2^t$. From Theorem 2.3.12, this algebra is of level

$$s(A_t(n)) \in [n - [\frac{n}{2^t}], n]$$

and sublevel

$$\underline{s}(A_t(n)) \in [n - [\frac{n + 2^t - 1}{2^t}], n], n \in \mathbb{N} - \{0\}.$$

Since $n < 2^t$, it results that $[\frac{n}{2^t}] = 0$ and $[\frac{n+2^t-1}{2^t}] = 1$, therefore $s(A_t(n)) = n$ and $\underline{s}(A_t(n)) \in \{n-1, n\}$.□

Remark. 2.3.15. Theorem 2.3.14 gives a positive partial answer to the question if any number $n \in \mathbb{N} - \{0\}$ can be realised as a level of composition algebras. The answer becomes positive if we replace "composition algebras" with "algebras obtained by the Cayley-Dickson process". Therefore, we can say that any number $n \in \mathbb{N} - \{0\}$ can be realised as a level of an algebra obtained by the Cayley-Dickson process with the norm form anisotropic over a suitable field.

Example 2.3.16. If $n \in \{6, 7\}$, for $t \geq 3$, from Theorem 2.3.12 and Theorem 2.3.13, it follows that the algebra $A_t(n)$ has level 6 and 7, respectively. This remark generalizes the results obtained by O'Shea in [O' Sh; 10] for the octonion division algebras.

Theorem 2.3.17. *With the above notations, we have that* $s\left(A_t\left(n\right)\right)=n$, *for* $n=2^k+1$.

Proof. First, we prove that the form

$$\varkappa_n = n\times <1> \perp (n-1)\times T_P^{A_t}$$

is anisotropic over K_n. If the form $\varkappa_n$ is isotropic over K_n, since the form

$$\varphi_n' = <1> \perp n \times T_P^{A_{t-1}}$$

is a subform of the form φ_n and the norm φ_n' is isotropic over its function field $K\left(\varphi_n'\right)$, then φ_n is isotropic over $K\left(\varphi_n'\right)$. From [Kn; 76, Theorem 3.3.], we have that there is a $K-$place from K_n to $K\left(\varphi_n'\right)$. Let

$$\varkappa_n' = n\times <1> \perp (n-1)\times T_P^{A_{t-1}}.$$

Then, over K, we can write

$$\varkappa_n = \varkappa_n' \perp X_t(n-1)\mathbf{n}_C^{A_{t-1}}.$$

If $\varkappa_n$ is isotropic over K_n, then $\varkappa_n$ is isotropic over $K\left(\varphi_n'\right)$. We obtain that $\varkappa_n'$ or $(n-1)\mathbf{n}_C^{A_{t-1}}$ are isotropic over $K\left(\varphi_n'\right)$. Using the induction steps and the same arguments as in [La; Ma, 01], Proposition 2.2, for $A_{t-1}=A_2$, we have that $\varkappa_n'$ is anisotropic over $K\left(\varphi_n'\right)$ and from Proposition 2.3.8, ii), we obtain that $(n-1)\mathbf{n}_C^{A_{t-1}}$ is anisotropic over $K\left(\varphi_n'\right)$. Therefore $\varkappa_n$ is anisotropic over K_n.

Now, from Remark 2.3.9 ii), we have $s\left(A_t\left(n\right)\right)\leq n$. If $s\left(A_t\left(n\right)\right)<n$, then the form $\varkappa_n$ is isotropic over K_n, false.□

The above result generalizes Theorem 3.1. from [Pu; 05].

Chapter 3

Properties of algebras obtained by the Cayley-Dickson process and some of their applications

3.1.Preliminaries

As we remarked in the previous chapters, quaternions, octonions and algebras obtained by the Cayley-Dickson process have at present many applications, as for example in physics, coding theory, computer vision, etc. For this reasons these algebras are intense studied. Since the algebras obtained by the Cayley-Dickson process are poor in properties when their dimension increase, losing commutativity, associativity and alternativity, the study of all kind of identities on these algebras is one of the direction of the study. In [Ra; 88], the author proved that in a generalized Octonion algebra over a field of characteristic different from $2, 3, 5$ any polynomial identity of degree less than 5 is not satisfied and he found the type of polynomial identities of degree 5. In [Is; 84], the author considered generalized Octonion algebras C over finite fields and found a finite basis for the ideal I of all identities in C. In [He; 97], the authors studied identities on generalized Octonion algebras and found all homogeneous multilinear polynomials of degree ≤ 6 which are identities for all generalized Octonion algebras. It is very interesting to extend this study to all algebras obtained by the Cayley-Dickson process, since this kind of relation can be helpful to replace the missing commutativity, associativity and alternativity. For example, in [Ha; 43], Hall proved that the identity $(xy - yx)^2 z = z (xy - yx)^2$ holds for all elements x, y, z in a quaternion algebra. This identity is called *Hall identity*. Moreover, he also proved the

converse: if the Hall identity is true in a skew-field F, then F is a quaternion division algebra. In [Smi; 50], Smiley proved that the Hall identity is true for the octonions and he also proved the converse: if the Hall identity is true in an alternative division algebra A, then A is an octonion division algebra.

In [Fl, Sh; 13(1)], authors proved that the Hall identity is true in all algebras obtained by the Cayley-Dickson process and, in some conditions, the converse is true for split quaternion algebras and split octonion algebras. As we remarked, these algebras are poor in properties, therefore any supplementary relation, identity or property can be very useful for the study of these algebras. For example, we are looking for a similar relation as Hall identity, to characterize some type $\mathcal{N}$ of nonassociative algebras, $\mathcal{N}$ ={alternative algebras, quadratic algebras, quaternion algebras, octonions algebras, algebras obtained by the Cayley-Dickson process, etc.}: *The property P is true on the algebra A if and only if $A \in \mathcal{N}$.* Such kind of results are Proposition 2.9. and Theorem 2.10, from [Fl, Sh; 13(1)], presented here in Proposition 3.2.9 and Theorem 3.2.10.

In the paper [Ba; 09], the author, by using *exclusive or* operation and a *twist map*, described an easy way to multiply the elements from a basis in algebras obtained by the Cayley-Dickson process. Using this algorithm, we found some very interesting relations and properties of the elements from a basis in such algebras, relations which are used to provide an example of a left hyperholomorphic function in generalized Cayley-Dickson algebras (Theorem 2.12). Moreover, in the Theorem 2.10, we proved that for the study of left A_t-holomorphic functions in generalized Cayley-Dickson algebras $A_t = \left(\frac{\gamma_1,\ldots,\gamma_t}{\mathbb{R}}\right)$ with $\gamma_1 < 0, \ldots, \gamma_t < 0$. it is suffices to consider left A_t-holomorphic functions only in the algebras $\left(\frac{-1,\ldots,-1}{\mathbb{R}}\right)$.

From Fundamental Theorem of Algebra, we know that each polynomial of degree n with coefficients in a field K has at most n roots in K. If we consider the coefficients in $\mathbb{H}$ (the division real quaternion algebra), the above result is not true. For the division real quaternion algebra, there is a kind of a fundamental theorem of algebra: *If a given polynomial has only one term of the greatest degree in $\mathbb{H}$ then it has at least one root in $\mathbb{H}$.* (see [Ei, Ni; 44], [Ni; 41], [Sm; 04]).

The similar results was obtained for octonions in [Sm; 04]. From this

reason, some type of equations, with one or more than one greatest term, over algebras obtained by the Cayley-Dickson process were studied. In this process, as a good examples, appeared the notions of Fibonacci elements, Fibonacci-Narayana, Fibonacci-Lucas elements on Quaternion and Octonion algebras. (see [Fl, Sh; 13], [Po, Ke; 15], [Fl, Sh; 15(3)], [Ram; 15], [Ta, Yi, Sa; 16]) These elements are very useful, since they provide sets of invertible elements, when the Quaternion and Octonion algebras are split.
(https://groups.google.com/forum/#!topic/sci.physics/T2zSvt_AjSQ).

3.2. Hall identity in algebras obtained by the Cayley-Dickson process

Let A be an algebra obtained by the Cayley-Dickson process with the basis $\{e_0 = 1, e_1, ..., e_n\}$ such that, $e_m e_r = -e_r e_m$, $r \neq m, e_m^2 = \gamma_m \in K, m \in \{1, 2, ..., n\}$. For elements $a = \sum\limits_{m=0}^{n} a_m e_m, b = \sum\limits_{m=0}^{n} b_m e_m$ we define an element in K, denoted by $T(a,b)$, $T(a,b) = \sum\limits_{m=0}^{n} e_m^2 a_m b_m$. We denote by $\overrightarrow{A}$ the set of the elements $\{\overrightarrow{a} \mid \overrightarrow{a} = \sum\limits_{m=1}^{n} a_m e_m, a_m \in K\}$. It results that the conjugate of the element a can be written as $\overline{a} = a_0 - \overrightarrow{a}$. Obviously, $\overrightarrow{(\overrightarrow{a})} = \overrightarrow{a}$ and $\overrightarrow{e_m} = e_m$.

Lemma 3.2.1. ([Fl, Sh; 13(1)]) *We consider A an algebra obtained by the Cayley-Dickson process. The following equalities are fulfilled:*

1) $T(a,b) = T(b,a)$, *for all* $a, b \in A$.

2) $T(\lambda a, b) = \lambda T(a,b)$, *for all* $\lambda \in K,\ a, b \in A$.

3) $T(a, b+c) = T(a,b) + T(a,c)$, *for all* $a, b, c \in A$.

4) $T(a, \overline{a}) = a\overline{a} = n(a)$, *for all* $a \in A$

5)

$$\overrightarrow{a}\,\overrightarrow{b} = 2T\left(\overrightarrow{a}, \overrightarrow{b}\right) - \overrightarrow{b}\,\overrightarrow{a}, \tag{3.2.1.}$$

$$ab = ba - 2\overrightarrow{b}\,\overrightarrow{a} + 2T\left(\overrightarrow{a}, \overrightarrow{b}\right), \tag{3.2.2.}$$

$$\overrightarrow{\overrightarrow{a}\,\overrightarrow{b}} = -T\left(\overrightarrow{a},\,\overrightarrow{b}\right) + \overrightarrow{a}\,\overrightarrow{b}. \tag{3.2.3.}$$

$$(\overrightarrow{a})^2 \in K, \tag{3.2.4.}$$

for all $a, b \in A$.

Proof. 5) For $\overrightarrow{a} = \sum_{m=1}^{n} a_m e_m$, $\overrightarrow{b} = \sum_{m=1}^{n} b_m e_m$ we obtain

$$\overrightarrow{a}\,\overrightarrow{b} = \sum_{m=1}^{n} a_m e_m \cdot \sum_{m=1}^{n} b_m e_m = \sum_{m=1}^{n} e_m^2 a_m b_m + \alpha = T\left(\overrightarrow{a},\,\overrightarrow{b}\right) + \alpha, \alpha \in \overrightarrow{A}. \tag{3.2.2.}$$

Computing $\overrightarrow{b}\,\overrightarrow{a}$, it follows that

$$\overrightarrow{b}\,\overrightarrow{a} = T\left(\overrightarrow{a},\,\overrightarrow{b}\right) - \alpha, \alpha \in \overrightarrow{A}. \tag{3.2.6.}$$

If we add relations (3.2.5) and (3.2.6), it results $\overrightarrow{a}\,\overrightarrow{b} + \overrightarrow{b}\,\overrightarrow{a} = 2T\left(\overrightarrow{a},\,\overrightarrow{b}\right)$, therefore relation (3.2.1) is obtained.

For $a = a_0 + \overrightarrow{a}$ and $b = b_0 + \overrightarrow{b}$, we compute

$$ab = (a_0 + \overrightarrow{a})\left(b_0 + \overrightarrow{b}\right) = a_0 b_0 + a_0\,\overrightarrow{b} + b_0\,\overrightarrow{a} + \overrightarrow{a}\,\overrightarrow{b}$$

and

$$ba = \left(b_0 + \overrightarrow{b}\right)(a_0 + \overrightarrow{a}) = b_0 a_0 + b_0\,\overrightarrow{a} + a_0\,\overrightarrow{b} + \overrightarrow{b}\,\overrightarrow{a}.$$

Subtracting the last two relations and using relation (3.2.1), we obtain $ab - ba = \overrightarrow{a}\,\overrightarrow{b} - \overrightarrow{b}\,\overrightarrow{a} = 2T\left(\overrightarrow{a},\,\overrightarrow{b}\right) - 2\,\overrightarrow{b}\,\overrightarrow{a}$, then relation (3.2.2) is proved. Relation (3.2.3) is obvious. For $\overrightarrow{a} = \sum_{m=1}^{n} a_m e_m$, it results that $(\overrightarrow{a})^2 = \sum_{m=1}^{n} (a_m)^2 \in K$.□

For quaternion algebras, the above result was proved in [Sz; 09].

Proposition 3.2.2. *We consider* A *an algebra obtained by the Cayley-Dickson process such that* $e_m^2 = -1$, *for all* $m \in \{1, 2, ...n\}$. *If* $n-1 \in K - \{0\}$, *then, for all* $x \in A$, *we have*

$$\overline{x} = \frac{1}{1-n} \sum_{m=0}^{n} e_m x e_m.$$

Proof. Let $x = \sum\limits_{m=0}^{n} e_m x_m$. From Lemma 3.2.1, we obtain

$\sum\limits_{m=0}^{n} e_m x e_m = x + \sum\limits_{m=1}^{n} e_m x e_m =$

$= x + \sum\limits_{m=1}^{n} e_m \left(e_m x - 2e_m \overrightarrow{x} + 2T\left(e_m, \overrightarrow{x}\right)\right) =$

$= x + \sum\limits_{m=1}^{n} e_m^2 x - 2\sum\limits_{m=1}^{n} e_m^2 \overrightarrow{x} + 2\sum\limits_{m=1}^{n} e_m^2 e_m x_m =$

$= x - nx + 2n\overrightarrow{x} - 2\sum\limits_{m=1}^{n} e_m x_m =$

$= (1-n)\, x - 2(1-n)\overrightarrow{x} = (1-n)\left(x - 2\overrightarrow{x}\right) =$

$= (1-n)\,\overline{x}.\square$

Theorem 3.2.3. *We consider A an algebra obtained by the Cayley-Dickson process. Then for all $x, y, z \in A$, it results that*

$$(xy - yx)^2 z = z(xy - yx)^2. \tag{3.2.7.}$$

Proof.

We will compute both members of the equality $(xy - yx)^2 z = z(xy - yx)^2$. Using relation (3.2.2.) from Lemma 3.2.1 and since $T\left(\overrightarrow{x}, \overrightarrow{y}\right) \in K$, we obtain

$\left(-2\overrightarrow{y}\,\overrightarrow{x} + 2T\left(\overrightarrow{x}, \overrightarrow{y}\right)\right)^2 z = z\left(-2\overrightarrow{y}\,\overrightarrow{x} + 2T\left(\overrightarrow{x}, \overrightarrow{y}\right)\right)^2 \Rightarrow$

$\Rightarrow \left[4\left(\overrightarrow{y}\,\overrightarrow{x}\right)^2 + 4T^2\left(\overrightarrow{x}, \overrightarrow{y}\right) - 8\left(\overrightarrow{y}\,\overrightarrow{x}\right)T\left(\overrightarrow{x}, \overrightarrow{y}\right)\right] z =$

$= z\left[4\left(\overrightarrow{y}\,\overrightarrow{x}\right)^2 + 4T^2\left(\overrightarrow{x}, \overrightarrow{y}\right) - 8\left(\overrightarrow{y}\,\overrightarrow{x}\right)T\left(\overrightarrow{x}, \overrightarrow{y}\right)\right] \Rightarrow$

$\Rightarrow 4\left(\overrightarrow{y}\,\overrightarrow{x}\right)^2 z + 4T^2\left(\overrightarrow{x}, \overrightarrow{y}\right) z - 8T\left(\overrightarrow{x}, \overrightarrow{y}\right)\left(\overrightarrow{y}\,\overrightarrow{x}\right) z =$

$= 4z\left(\overrightarrow{y}\,\overrightarrow{x}\right)^2 + 4T^2\left(\overrightarrow{x}, \overrightarrow{y}\right) z - 8T\left(\overrightarrow{x}, \overrightarrow{y}\right) z\left(\overrightarrow{y}\,\overrightarrow{x}\right).$

Dividing this last relation by 4 and after reducing the terms, it results

$\left(\overrightarrow{y}\,\overrightarrow{x}\right)^2 z - 2T\left(\overrightarrow{x}, \overrightarrow{y}\right)\left(\overrightarrow{y}\,\overrightarrow{x}\right) z = z\left(\overrightarrow{y}\,\overrightarrow{x}\right)^2 - 2T\left(\overrightarrow{x}, \overrightarrow{y}\right) z\left(\overrightarrow{y}\,\overrightarrow{x}\right).$

We denote

$$\begin{aligned} E \;=\; & \left[\left(\overrightarrow{y}\,\overrightarrow{x}\right)^2 z - z\left(\overrightarrow{y}\,\overrightarrow{x}\right)^2\right] - \\ & - \left[2T\left(\overrightarrow{x}, \overrightarrow{y}\right)\left(\overrightarrow{y}\,\overrightarrow{x}\right) z - 2T\left(\overrightarrow{x}, \overrightarrow{y}\right) z\left(\overrightarrow{y}\,\overrightarrow{x}\right)\right] \end{aligned}$$

and we will prove that $E = 0$.

We denote

$$E_1 = \left(\overrightarrow{y}\,\overrightarrow{x}\right)^2 z - 2T\left(\overrightarrow{x}, \overrightarrow{y}\right)\left(\overrightarrow{y}\,\overrightarrow{x}\right) z$$

and

$$E_2 = z\left(\overrightarrow{y}\,\overrightarrow{x}\right)^2 - 2T\left(\overrightarrow{x}, \overrightarrow{y}\right) z\left(\overrightarrow{y}\,\overrightarrow{x}\right).$$

First, we compute E_1. We obtain
$E_1 = [(\overrightarrow{y}\,\overrightarrow{x})^2 - 2T(\overrightarrow{x}, \overrightarrow{y})(\overrightarrow{y}\,\overrightarrow{x})]z$.
From Lemma 3.2.1., relation (3.2.3), we have $\overrightarrow{y}\,\overrightarrow{x} = T(\overrightarrow{y}, \overrightarrow{x}) + \overrightarrow{\overrightarrow{y}\,\overrightarrow{x}}$.
Then $(\overrightarrow{y}\,\overrightarrow{x})^2 = T^2(\overrightarrow{y}, \overrightarrow{x}) + \left(\overrightarrow{\overrightarrow{y}\,\overrightarrow{x}}\right)^2 + 2T(\overrightarrow{y}, \overrightarrow{x})\ \overrightarrow{\overrightarrow{y}\,\overrightarrow{x}}$.
Therefore
$E_1 = [T^2(\overrightarrow{y}, \overrightarrow{x}) + \left(\overrightarrow{\overrightarrow{y}\,\overrightarrow{x}}\right)^2 +$
$+2T(\overrightarrow{y}, \overrightarrow{x})\ \overrightarrow{\overrightarrow{y}\,\overrightarrow{x}} - 2T(\overrightarrow{x}, \overrightarrow{y})(\overrightarrow{y}\,\overrightarrow{x})]z =$
$= [T^2(\overrightarrow{y}, \overrightarrow{x}) + \left(\overrightarrow{\overrightarrow{y}\,\overrightarrow{x}}\right)^2 +$
$+2T(\overrightarrow{y}, \overrightarrow{x})(\overrightarrow{\overrightarrow{y}\,\overrightarrow{x}} - \overrightarrow{y}\,\overrightarrow{x})]z$.
Since $\overrightarrow{\overrightarrow{y}\,\overrightarrow{x}} - \overrightarrow{y}\,\overrightarrow{x} = -T(\overrightarrow{y}, \overrightarrow{x})$, it results that
$[(\overrightarrow{y}\,\overrightarrow{x})^2 - 2T(\overrightarrow{x}, \overrightarrow{y})(\overrightarrow{y}\,\overrightarrow{x})] =$
$= [\left(\overrightarrow{\overrightarrow{y}\,\overrightarrow{x}}\right)^2 - T^2(\overrightarrow{y}, \overrightarrow{x})] = \alpha \in K$,
from Lemma 3.2.1, relation (3.2.4). Hence $E_1 = \alpha z$.
Now, we compute E_2. We obtain
$E_2 = z[(\overrightarrow{y}\,\overrightarrow{x})^2 - 2T(\overrightarrow{x}, \overrightarrow{y})(\overrightarrow{y}\,\overrightarrow{x})] =$
$= z\alpha = \alpha z$ since $\alpha \in K$.

It follows that $E = E_1 - E_2 = 0$, therefore relation (3.2.7.) is proved. □

Remark 3.2.4. 1) Identity (3.2.7) is called the *Hall identity*. From the above theorem, we remark that Hall identity is true for all algebras obtained by the Cayley-Dickson process.

2) Relation (3.2.7) can be written: $[x, y]^2 z = z[x, y]^2$ or $\left[[x, y]^2, z\right] = 0$, where $[x, y] = xy - yx$ is the commutator of two elements. If $A = \mathbb{H}$, then the identity (3.2.7.) is proved by Hall in [Ha; 43].

Proposition 3.2.5. *For an arbitrary algebra A over the field K such that the relation* (3.2.7.) *holds for all $x, y, z \in A$, we have the following relations:*

$$[[x, y][u, y], z] + [[x, y][x, v], z] + [[u, y][x, y], z] + [[x, v][x, y], z] = 0, \qquad (3.2.8.)$$

$$[[x, v][u, y], z] + [[u, y][x, v], z] + [[x, y][u, v], z] + [[u, v][x, y], z] = 0, \qquad (3.2.9.)$$

$$[[u, y][u, v], z] + [[x, v][u, v], z] + [[u, v][u, y], z] + [[u, v][x, v], z] = 0 \qquad (3.2.10.)$$

for all $x, y, z, u, v \in A$.

Proof. We linearize relation (3.2.7.) . Let $x, y, z \in A$ be three arbitrary elements such that $(xy - yx)^2 z = z (xy - yx)^2$.
For $x + \lambda u, y + \lambda v, z$ we obtain
$[(x + \lambda u)(y + \lambda v) - (y + \lambda v)(x + \lambda u)]^2 z =$
$= z[(x + \lambda u)(y + \lambda v) - (y + \lambda v)(x + \lambda u)]^2.$
It results
$[xy - yx + \lambda(uy + xv - yu - vx) + \lambda^2 (uv - vu)]^2 z =$
$= z \left[xy - yx + \lambda(uy + xv - yu - vx) + \lambda^2 (uv - vu)\right]^2 .$
We obtain
$(xy - yx)^2 z + \lambda^2[(uy - yu) + (xv - vx)]^2 z +$
$+ \lambda^4 (uv - vu)^2 z +$
$+ \lambda[(xy - yx)((uy - yu) + (xv - vx))]z +$
$+ \lambda[((uy - yu) + (xv - vx))(xy - yx)]z +$
$+ \lambda^2[(uv - vu)(xy - yx)]z +$
$+ \lambda^2[(xy - yx)(uv - vu)]z +$
$+ \lambda^3[[(uy - yu) + (xv - vx)](uv - vu)]z +$
$+ \lambda^3[(uv - vu)[(uy - yu) + (xv - vx)]]z =$
$z(xy - yx)^2 + \lambda^2 z[(uy - yu) + (xv - vx)]^2 +$
$+ \lambda^4 z(uv - vu)^2 +$
$+ \lambda z[(xy - yx)((uy - yu) + (xv - vx))] +$
$+ \lambda z[((uy - yu) + (xv - vx))(xy - yx)] +$
$+ \lambda^2 z[(uv - vu)(xy - yx)] +$
$+ \lambda^2 z[(xy - yx)(uv - vu)] +$
$+ \lambda^3 z[[(uy - yu) + (xv - vx)](uv - vu)] +$
$+ \lambda^3 z[(uv - vu)[(uy - yu) + (xv - vx)]]$, for all $x, y, z, u, v \in A$.
Since the coefficients of λ are equal in both members of the equality, we obtain:
$[(xy - yx)((uy - yu) + (xv - vx))]z +$
$+ [((uy - yu) + (xv - vx))(xy - yx)]z =$
$= z[(xy - yx)((uy - yu) + (xv - vx))] +$
$+ z[((uy - yu) + (xv - vx))(xy - yx)].$
We can write this last relation under the form:
$\{[x, y][u, y]\}z + \{[x, y][x, v]\}z +$
$+ \{[u, y][x, y]\}z + \{[x, v][x, y]\}z =$
$= z\{[x, y][u, y]\} + z\{[x, y][x, v]\} +$

$+z\{[u,y]\,[x,y]\}+z\{[x,v]\,[x,y]\}$.
It results
$[[x,y]\,[u,y]\,,z]+[[x,y][x,v],z]+[[u,y][x,y],z]+[[x,v][x,y],z]=0$
and we obtain relation (3.2.8.) .
Since the coefficients of λ^2 are equal in both members of the equality, we obtain:
$[(uy-yu)+(xv-vx)]^2z+$
$+[(uv-vu)\,(xy-yx)]z+$
$+[(xy-yx)\,(uv-vu)]z=$
$=z[(uy-yu)+(xv-vx)]^2+$
$+z[(uv-vu)\,(xy-yx)]+$
$+z[(xy-yx)\,(uv-vu)]$.
It results that
$[(uy-yu)\,(xv-vx)]z+[(xv-vx)\,(uy-yu)]z+$
$+[(uv-vu)\,(xy-yx)]z+[(xy-yx)\,(uv-vu)]z=$
$z[(uy-yu)\,(xv-vx)]+z[(xv-vx)\,(uy-yu)]+$
$+z[(uv-vu)\,(xy-yx)]+z[(xy-yx)\,(uv-vu)]$.
We can write this last relation under the form:
$[[x,v]\,[u,y]\,,z]+[[u,y]\,[x,v]\,,z]+[[x,y]\,[u,v]\,,z]+[[u,v]\,[x,y]\,,z]=0$
and we obtain relation (3.2.9.) .
Since the coefficients of λ^3 are equal in both members of the equality, we obtain:
$[[(uy-yu)+(xv-vx)]\,(uv-vu)]z+$
$+[(uv-vu)\,[(uy-yu)+(xv-vx)]]z=$
$=z[[(uy-yu)+(xv-vx)]\,(uv-vu)]+$
$+z[(uv-vu)\,[(uy-yu)+(xv-vx)]]$.
We can write this last relation under the form:
$[[u,y][u,v],z]+[[x,v][u,v],z]+[[u,v][u,y],z]+[[u,v][x,v],z]=0$
and we obtain relation (3.2.10.) . □

Remark 3.2.6.

1) In [Ti; 99] and [Fl; 01] some equations over division quaternion algebra and octonion algebra are solved. Let A be such an algebra. For example, equation

$$ax=xb, a,b,x\in A, \tag{3.2.11.}$$

for $a \neq \overline{b}$ has general solution under the form $x = \overrightarrow{a}p + p\overrightarrow{b}$, for arbitrary $p \in A$.

2) In [Fl, Şt; 09], authors studied equation $x^2a = bx^2 + c, a, b, c \in A$, where A is a generalized quaternion division algebra or an generalized octonion division algebra. If A is an arbitrary algebra obtained by the Cayley-Dickson process and $a, b, c \in A$ with $a = b$ and $c = 0$, then, from Theorem 3.2.3, it results that this equation has infinity of solutions of the form $x = vw - wv$, where $v, w \in A$.

Proposition 3.2.7. *Let A be a quaternion algebra or an octonion algebra. Then for all $x, y \in A$, there are the elements z, w such that $(xy - yx)^2 = \overrightarrow{z}w + w\overrightarrow{z}$.*

Proof. Let z be an arbitrary element in $A - K$. From Theorem 3.2.3, we have that $(xy - yx)^2 z = z(xy - yx)^2$, for all $x, y, z \in A$. Since $z \neq \overline{z}$ and $(xy - yx)^2$ is a solution for the equation (3.2.11), from Remark 3.2.6, it results that there is an element $w \in A$ such that $(xy - yx)^2 = \overrightarrow{z}w + w\overrightarrow{z}$.□

Proposition 3.2.8. *Let A be a finite dimensional unitary algebra with a scalar involution*

$$^- : A \to A, a \to \overline{a},$$

such that for all $x, y \in A$, the following equality holds:

$$(x\overline{y} + y\overline{x})^2 = 4(x\overline{x})(y\overline{y}). \tag{3.2.12.}$$

Then the algebra A has dimension 1.

Proof. We remark that $x\overline{y} + y\overline{x} = x\overline{y} + \overline{x\overline{y}} \in K$. First, we prove that $[x\overline{y} + y\overline{x}]^2 = 4(x\overline{x})(y\overline{y}), \forall x, y \in A$, if and only if $x = ry$, $r \in K$. If $x = ry$, then relation (3.2.12.) is proved. Conversely, assuming that relation (3.2.12.) is true and supposing that there is not an element $r \in K$ such that $x = ry$, then for each two non zero elements $a, b \in K$, we have $ax + by \neq 0$. Indeed, if $ax + by = 0$, it results $x = -\frac{b}{a}y$, false. We obtain that

$$(ax + by)\overline{(ax + by)} \neq 0. \tag{3.2.13.}$$

Computing relation (3.2.13), it follows

$$a^2(x\overline{x}) + abx\overline{y} + bay\overline{x} + b^2y\overline{y} \neq 0. \qquad (3.2.14.)$$

If we put $a = y\overline{y}$ in relation (3.2.14) and then simplify by a, it results

$$(y\overline{y})(x\overline{x}) + bx\overline{y} + by\overline{x} + b^2 \neq 0. \qquad (3.2.15.)$$

Let $b = -\frac{1}{2}(x\overline{y} + y\overline{x}) \in K, b \neq 0$. If we replace this value in relation (3.2.15), we obtain $4(x\overline{x})(y\overline{y}) - (x\overline{y} + y\overline{x})^2 \neq 0$, which it is false. Therefore, there is an element $r \in K$ such that $x = ry$.

Assuming that the algebra A has dimension greater or equal with 2, it results that there are two linearly independent vectors, v and w, respectively. Since relation (3.2.12) is satisfies for v and w, we obtain that there is an element $s \in K$ such that $v = sw$, which it is false. Hence $\dim A = 1$.□

Proposition 3.2.9. *Let A be an alternative division algebra over the field K whose center is K. If $(xy - yx)^2 z = z(xy - yx)^2$ for all $x, y, z \in A$ and $(xy - yx)^2$ associate with all elements from A, then A is a quadratic algebra.*

Proof. Let $x, y \in A - \{0\}$ such that $xy \neq yx$. If we denote $z = xy - yx$, it follows that z^2 commutes and associate with all elements from A, then z^2 is in the center of A. We obtain $z^2 = \alpha \in K^*$. For $t = x^2y - yx^2$, it results that $t^2 = (x^2y - yx^2)^2 \in K$ and $t = (xy - yx)x + x(xy - yx) = zx + xz$. We have $zt = z(zx + xz) = z^2x + zxz = \alpha x + zxz$ and $tz = (zx + xz)z = zxz + xz^2 = \alpha x + zxz$. Therefore $tz = zt$. For $z + t = \left(x^2 + x\right)y - y\left(x^2 + x\right)$, we have that $(z + t)^2 = \beta \in K$, then $z^2 + t^2 + 2tz = \beta$, hence $tz = \gamma \in K$. Since each alternative algebra is a flexible algebra, we have $zx = x(yx) - (yx)x$. From here, it follows that $(zx)^2 = \delta \in K$. If we multiply relation $(zx)(zx) = \delta$ with z in the left side, we obtain $z((zx)(zx)) = \delta z$. Using alternativity and then flexibility, it results $\left(z^2x\right)(zx) = \delta z$, therefore $\alpha(xzx) = \delta z$, hence $xzx = \theta z$, where $\theta = \alpha^{-1}\delta$. It follows that $z(xzx) = \theta z^2 = \theta\alpha \in K$. Since $z(xzx) = (zxz)x$, from Moufang identities, we have that $(zxz)x = \theta\alpha \in K$. It results that $\gamma x = (tz)x = (\alpha x + zxz)x = \alpha x^2 + (zxz)x = \alpha x^2 + \theta\alpha$, hence $x^2 = ax + b$, where $a = \alpha^{-1}\gamma, b = -\theta$. We obtain that A is a quadratic algebra.□

When A is a division associative algebra, this proposition was proved by Hall in [Ha; 43].

Theorem 3.2.10. *Let A be an alternative simple algebra such that the center of A is K, $(xy-yx)^2 z = z(xy-yx)^2$, for all $x, y, z \in A$ and $(xy-yx)^2$ associate with all elements from A.*

1) If A is a division algebra, then $A = K$ or $A = A_t, t \in \{1,2,3\}$, where A_t is a division algebra obtained by the Cayley-Dickson process.

2) If A is not a division algebra, $\dim A = 4$, and if there are two elements $y, z \in A$ such that $y^2, z^2 \in K$, $yz = -zy$, then A is a generalized split quaternion algebra.

Proof. 1) From Proposition 3.2.9., it results that A is a quadratic algebra, therefore, from [Al; 49], Theorem 1, we have $\dim A \in \{1, 2, 4, 8\}$. If $\dim A = 1$, then $A = K$. If $\dim A = 2$, since the center is K, then we can find an element $x \in A - K$ such that $x^2 \in K$. It results that the set $\{1, x\}$ is a basis in A, therefore $A = K(x)$ is a quadratic field extension of the field K. If $\dim A = 4$, from [Al; 39], p. 145, we have that there are two elements $x, y \in A$ such that $x^2 = x + a$ with $4a + 1 \neq 0$, $xy = y(1-x), y^2 = b, a, b \in K$. Denoting $z = x - \frac{1}{2}$, we obtain that $z^2 = \left(x - \frac{1}{2}\right)^2 = a - \frac{1}{4} \in K$. and $zy = -yz$. Since $zy = \left(x - \frac{1}{2}\right) y = xy - \frac{y}{2} = y - yx - \frac{y}{2} = \frac{y}{2} - yx$ and $yz = y\left(x - \frac{1}{2}\right) = yx - \frac{1}{2}$, we have $yz = -zy$ then $(yz)^2 \in K$. It follows that in the algebra A we can find the elements y, z such that $y^2, z^2, (yz)^2 \in K$ and $yz = -zy$. Therefore, from [Al; 49], Lemma 4, it results that A is a generalized division quaternion algebra.

2) From the above, it results that $A = Q = K + yK + zK + yzK$ is a generalized quaternion algebra, which is split from hypothesis.□

3.3. Multiplication table in algebras obtained by the Cayley-Dickson process

In this section, for a generalized Cayley-Dickson algebra A_t, writing the elements of the basis in a convenient way, we can obtain multiplication tables

for certain elements of the basis. Using these results, in the next section, we provide an example of a left hyperholomorphic function in generalized Cayley-Dickson algebras.The results presented below, were obtained especially in the paper [Fl, Sh; 15(1)].

The current trend in hypercomplex analysis is a systematic search for all possible function theories associated to Dirac operator in various algebras. In this paper we investigated such as holomorphic functions for real Cayley–Dickson algebras. We generalized the notion of left A_t-holomorphic functions from quaternions to all algebras obtained by the Cayley-Dickson process and we provided an algorithm to find examples of left A_t-hyperholomorphic functions, using the *shuffling* procedure given by Bales.

The theory of the right A_t-holomorphic functions and the theory of the right A_t-hyperholomorphic functions are similarly to the corresponding theories for the left functions and can be easy treated, using the above ideas and procedures.

Remark 3.3.1. For $\gamma_1 = ... = \gamma_t = -1$ and $K = \mathbb{R}$, in [Ba; 09], the author described how we can multiply the basis vectors in the algebra $A_t, \dim A_t = 2^t = n$. He used the binary decomposition for the subscript indices.

Let e_p, e_q be two vectors in the basis B with p, q representing the binary decomposition for the indices of the vectors, that means p, q are in $\mathbb{Z}_2^n$. We have that $e_p e_q = \gamma_n (p, q) e_{p \otimes q}$, where:

i) $p \otimes q$ are the sum of p and q in the group $\mathbb{Z}_2^n$ or, more precisely, the "*exclusive or*" for the binary numbers p and q;

ii) γ_n is a function $\gamma_n : \mathbb{Z}_2^n \times \mathbb{Z}_2^n \to \{-1, 1\}$.

The map γ_n is called the *twist map.*

The elements of the group $\mathbb{Z}_2^n$ can be considered as integers from 0 to $2^n - 1$ with multiplication "*exclusive or*" of the binary representations. Obviously, this operation is equivalent with the addition in $\mathbb{Z}_2^n$.

From now on, in this section, we will consider $K = \mathbb{R}$. Using the same notations as in the Bales's paper, we consider the following matrices:

$$A_0 = A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}. \quad (3.3.1.)$$

In the same paper, [Ba;09], the author find the properties of the twist map

γ_n and put the signs of this map in a table. He partitioned the twist table for $\mathbb{Z}_2^n$ into 2×2 matrices and obtained the following result:

Theorem 3.3.2. ([Ba;09], Theorem 2.2., p. 88-91) *For $n > 0$, the Cayley-Dickson twist table γ_n can be partitioned in quadratic matrices of dimension 2 of the form $A, B, C, -B, -C$, defined in the relation* (3.3.1). *Relations between them can be found in the below twist trees*:

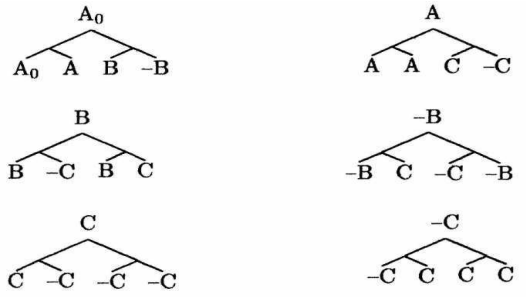

Fig. 1: Twist trees([1], Table 9)

□

Definition 3.3.3. Let $x = x_0, x_1, x_2, ...$ and $y = y_0, y_1, y_2, ...$ be two sequences of real numbers. The ordered pair

$$(x, y) = x_0, y_0, x_1, y_1, x_2, y_2, ...$$

is a sequence obtained by *shuffling* the sequences x and y.

In [Ba;09], is provided the below algorithm for find $\gamma_n(s, r)$, where $s, r \in \mathbb{Z}_2^n$:

i) We find the shuffling sequence (s, r).

ii) Starting with the root A_0, we can find $\gamma_n(s, r)$ using the twist tree. We remark that "00"= unchanged, "01" =left $\rightarrow$right, "10"=right$\rightarrow$ left, "11"=right $\rightarrow$ right.

The multiplication table in $\mathbb{H}(-1, -1)$, the quaternion division algebra, is given below.

$$\begin{pmatrix} A_0 & A \\ B & -B \end{pmatrix}$$

Quaternion twist table using above notations

Example 3.3.4. Let A_4 be the real sedenion algebra. That means $\dim A_4 = 16$ with $\{1, e_1, ..., e_{15}\}$ a basis in this algebra. Let compute $e_7 e_{13} = \gamma_4(7_2, 13_2) e_{7 \otimes 13}$. We have the following binary decompositions:

$$\begin{aligned} 7_2 &= 0111, \text{ since } 7 = 2^2 + 2 + 1 \text{ and} \\ 13_2 &= 1101, \text{ since } 13 = 2^3 + 2^2 + 1. \end{aligned}$$

Since $0111 \otimes 1101 = 1010 (= 2^3 + 2 = 10)$, it results that $7 \otimes 13 = 10$.

Now, we compute $\gamma_4 (e_7, e_{13})$. First, we shuffle the sequences 0111 and 1101. We obtain 01 11 10 11. Starting with A_0, it results: $A_0 \overset{01}{\to} A \overset{11}{\to} -C \overset{10}{\to} C \overset{11}{\to} -C$, then $\gamma_4 (e_7, e_{13}) = -1$ and $e_7 e_{13} = -e_{10}$.

Remark 3.3.5. i) In the generalized quaternion algebra, $\mathbb{H}(\gamma_1, \gamma_2)$, the basis can be written as

$$\{1 = e_0, e_1, e_2, e_1 e_2\}.$$

For the generalized octonion algebra, $\mathbb{O}(\gamma_1, \gamma_2, \gamma_3)$, the basis can be written

$$\{1 = e_0, e_1, e_2, e_1 e_2, e_4, e_1 e_4, e_2 e_4, (e_1 e_2) e_4\}.$$

Therefore $e_3 = e_1 e_2, e_7 = e_3 e_4 = (e_1 e_2) e_4$, $e_2 e_4 = e_6$ and, when compute them, in these products do not appear any of the elements $\gamma_1, \gamma_2, \gamma_3$, or products of some of them at the end.

We remark that in the algebra $A_t = \left(\frac{\gamma_1, ..., \gamma_t}{\mathbb{R}}\right)$ in the products of the form

$$e_1 e_2, (e_1 e_2) e_4, ..., ((e_{2^r} e_{2^{r+1}}) \dots e_{2^k}) e_{2^i},$$

when compute them, do not appear any of the elements $\gamma_1, \gamma_2, ..., \gamma_t$ or products of some of them at the end.

ii) Let $\{1 = e_0, e_1, e_2, \dots, e_{2^t - 1}\}$ be a basis in the algebra A_t. Using above remarks, the basis in the algebra $A_t = \left(\frac{\gamma_1, ..., \gamma_t}{\mathbb{R}}\right)$ can be written under the form

$$\{1 = e_0, e_1, e_2, \dots, e_{2^{t-1}-1}, e_{2^{t-1}}, e_1 e_{2^{t-1}}, e_2 e_{2^{t-1}}, e_3 e_{2^{t-1}}, \dots, e_{2^{t-1}-1} e_{2^{t-1}}\} \tag{3.3.2.}$$

with

$$e_i e_{2^{t-1}} = -e_{2^{t-1}} e_i = e_{2^{t-1}} \overline{e}_i, \quad i \in \{1, 2, \ldots, 2^{t-1} - 1\}. \tag{3.3.3.}$$

Proposition 3.3.6. ([Fl, Sh; 15(1)]) *Let* $A_t = \left(\frac{\gamma_1,\ldots,\gamma_t}{\mathbb{R}}\right)$ *be an algebra obtained by the Cayley-Dickson process and* $\{e_0 = 1, e_1, ..., e_{n-1}\}$, $n = 2^t$ *be a basis. Let* $r \geq 1$, $r < k \leq i < t$. *Therefore*

$$((e_{2^r} e_{2^{r+1}}) \ldots e_{2^k}) e_{2^i} = (-1)^{k-r+2} e_T, \tag{3.3.4.}$$

$$((e_1 e_{2^r}) e_{2^{r+1}}) \ldots e_{2^k}) e_{2^i} = (-1)^{k-r+3} e_{T+1}, \tag{3.3.5.}$$

where $T = 2^r + 2^{r+1} + \ldots + 2^k + 2^i$ *and*

$$e_1 e_{2^i} = e_{2^i+1}. \tag{3.3.6.}$$

.

Proof. From Remark 3.3.5, it results that we can use Theorem 3.3.2 for $\gamma_1, \gamma_2, \ldots, \gamma_t$ arbitrary. For $T = 2^r + 2^{r+1} + \ldots + 2^k + 2^i$, we have the binary decomposition

$$T_2 = 1\underbrace{00\ldots0}_{i-k-1}\underbrace{111\ldots1}_{k-r+1}\underbrace{0\ldots0}_{r}.$$

Using the same remark, we obtain $e_{2^r} e_{2^{r+1}} = \gamma_n \left(\underbrace{01\ldots0}_{r+2}, \underbrace{10\ldots0}_{r+2}\right) e_{2^r+2^{r+1}}$. We "shuffling" $\underbrace{01\ldots0}_{r+2}$ and $\underbrace{10\ldots0}_{r+2}$ and we obtain $01\ 10\ \underbrace{00\ 00\ldots00\ 00}_{r \text{ pairs}}$. Starting with A_0, it results

$$A_0 \overset{01}{\to} A \overset{10}{\to} C,$$

then $\gamma_n \left(\underbrace{01\ldots0}_{r+2}, \underbrace{10\ldots0}_{r+2}\right) = 1$ and $e_{2^r} e_{2^{r+1}} = e_{2^r+2^{r+1}}$.

We compute $(e_{2^r} e_{2^{r+1}}) e_{2^{r+2}}$. We obtain

$$(e_{2^r} e_{2^{r+1}}) e_{2^{r+2}} = e_{2^r+2^{r+1}} e_{2^{r+2}} = \gamma_n \left(\underbrace{011\ldots0}_{r+3}, \underbrace{10\ldots0}_{r+3}\right) e_{2^r+2^{r+1}+2^{r+2}}.$$

Shuffling $\underbrace{011...0}_{r+3}$ and $\underbrace{10...0}_{r+3}$, we get 01 10 $1\underbrace{000\ 00...00\ 00}_{r \text{ pairs}}$. Starting with A_0, it results: $A_0 \overset{01}{\to} A \overset{10}{\to} C \overset{10}{\to} -C$, then

$$\gamma_n\left(\underbrace{011...0}_{r+3}, \underbrace{10...0}_{r+3}\right) = -1,$$

therefore $e_{2^r+2^{r+1}} e_{2^{r+2}} = -e_{2^r+2^{r+1}+2^{r+2}}$. Continuing this procedure, we remark that the number of "1" in the "shuffling" obtained influences the sign. Since $T = 2^r + 2^{r+1} + ... + 2^k + 2^i$ has binary decomposition

$$T_2 = 1\underbrace{00...0}_{i-k-1}\underbrace{111..1}_{k-r+1}\underbrace{0...0}_{r},$$

in which we have $k - r + 2$ elements equal with 1, we obtain relation (3.3.4). In the same way it results relations (3.3.5) and (3.3.6). □

Proposition 3.3.7. ([Fl, Sh; 15(1)]) *With the same notations as in Proposition 3.3.6, for the algebra* $A_t = \left(\frac{-1,...,-1}{\mathbb{R}}\right)$, *we have:*

$\cdot$	e_T	e_{T+1}
e_{T_1}	$(-1)^{k-r+1} e_{2^i}$	$-(-1)^{k-r+1} e_{2^i+1}$
e_{T_1+1}	$-(-1)^{k-r+1} e_{2^i+1}$	$-(-1)^{k-r+1} e_{2^i}$

(3.3.7.)

for $r < k$, *where* $T = 2^r + 2^{r+1} + ... + 2^k + 2^i$, $T_1 = 2^r + 2^{r+1} + ... + 2^k$ *and*

$\cdot$	e_T	e_{T+1}
e_{2^k}	e_M	$-e_{M+1}$
e_{2^k+1}	$-e_{M+1}$	$-e_M$

, (3.3.8.()

where $M = 2^k + 2^i$.

Proof. *Case 1*: $r < k$. We compute $e_{T_1} e_T$. We have $e_{T_1} e_T = \gamma(s, q)\, e_M$, where s, q are the binary decomposition of T_1 and T. The binary decomposition of M is $M_2 = T_1 \otimes T$. It results $M = 2^i$,

$$s = \underbrace{00...0}_{i-k}\underbrace{111...1}_{k-r+1}\underbrace{0...0}_{r}, \quad q = \underbrace{100...0}_{i-k}\underbrace{111...1}_{k-r+1}\underbrace{0...0}_{r}.$$

By "shuffling" $s \otimes q$, we obtain

$$\underbrace{01\ 00\ 00...00}_{(i-k)\text{ pairs}}\ \underbrace{11\ 11\ 11\ ...11}_{(k-r+1)\text{ pairs}}\ \underbrace{00\ 00\ ...00\ 00}_{r\text{ pairs}}.$$

Starting with A_0, we get:

$$\underbrace{A_0 \overset{01}{\to} A \overset{00}{\to} ... \overset{00}{\to} A}_{i-k} \overset{11}{\to} \underbrace{-C \overset{11}{\to} C \overset{11}{\to} -C \overset{11}{\to} C \overset{11}{\to} ... \overset{11}{\to} (-1)^{k-r+1} C}_{k-r+1} \underbrace{\overset{00}{\to} ... \overset{00}{\to} (-1)^{k-r+1} C}_{r}.$$

Therefore $\gamma(s,q) = (-1)^{k-r+1}$.

Now, we compute $e_{T_1} e_{T+1}$. For this, we will "shuffling" $\underbrace{00...0}_{i-k}\underbrace{111...10}_{k-r+1}\underbrace{...0}_{r}$ with $\underbrace{100...0}_{i-k}\underbrace{111...10}_{k-r+1}\underbrace{...1}_{r}$. It results

$$\underbrace{01\ 00\ 00...00}_{(i-k)\text{ pairs}}\ \underbrace{11\ 11\ 11...11}_{(k-r+1)\text{ pairs}}\ \underbrace{00\ 00...00\ 01}_{r\text{ pairs}}.$$

Starting with A_0, we get:

$$\underbrace{A_0 \overset{01}{\to} A \overset{00}{\to} ... \overset{00}{\to} A}_{i-k} \overset{11}{\to} \underbrace{-C \overset{11}{\to} C \overset{11}{\to} -C \overset{11}{\to} C \overset{11}{\to} ... \overset{11}{\to} (-1)^{k-r+1} C}_{k-r+1} \underbrace{\overset{00}{\to} ... \overset{01}{\to} -(-1)^{k-r+1} C}_{r}.$$

For $e_{T_1+1} e_T$, "shuffling" $\underbrace{00...0}_{i-k}\underbrace{111...10}_{k-r+1}\underbrace{...1}_{r}$ with $\underbrace{100...0}_{i-k}\underbrace{111...10}_{k-r+1}\underbrace{...0}_{r}$, it results

$$\underbrace{01\ 00\ 00...00}_{(i-k)\text{ pairs}}\ \underbrace{11\ 01\ 01...01}_{(k-r+1)\text{ pairs}}\ \underbrace{00\ 00...00\ 10}_{r\text{ pairs}}.$$

Starting with A_0,we get:

$$\underbrace{A_0 \overset{01}{\to} A \overset{00}{\to} ... \overset{00}{\to} A}_{i-k} \overset{11}{\to} \underbrace{-C \overset{11}{\to} C \overset{11}{\to} -C \overset{11}{\to} C \to ... \overset{11}{\to} (-1)^{k-r+1} C}_{k-r+1} \underbrace{\overset{00}{\to} ... \overset{10}{\to} -(-1)^{k-r+1} C}_{r}.$$

For $e_{T_1+1} e_{T+1}$, we compute first $(T_1+1) \otimes (T+1)$. We obtain:

$$\left(2^r + 2^{r+1} + ... + 2^k + 1\right) \otimes \left(2^r + 2^{r+1} + ... + 2^k + 2^i + 1\right) =$$

$$= \left(\underbrace{00...0111...10...1}_{i-k \quad k-r+1 \quad r}\right) \otimes \left(\underbrace{100...0111...10...1}_{i-k \quad k-r+1 \quad r}\right) =$$

$$= \underbrace{10...0000...00...0}_{i-k \quad k-r+1 \quad r} = 2^i.$$

Now, "shuffling" $\underbrace{00...0111...10...1}_{i-k \quad k-r+1 \quad r}$ with $\underbrace{100...0111...10...1}_{i-k \quad k-r+1 \quad r}$, it results

$$\underbrace{01\ 00\ 00...00}_{(i-k)\text{ pairs}}\ \underbrace{11\ 01\ 01...01}_{(k-r+1)\text{ pairs}}\ \underbrace{00\ 00...00\ 11}_{r\text{ pairs}}.$$

Starting with A_0, we get:

$$\underbrace{A_0 \overset{01}{\to} A \overset{00}{\to} ... \overset{00}{\to} A}_{i-k} \underbrace{\overset{11}{\to} -C \overset{11}{\to} C \overset{11}{\to} -C \overset{11}{\to} C \overset{11}{\to} ... \overset{11}{\to} (-1)^{k-r+1} C}_{k-r+1} \underbrace{\overset{00}{\to} ... \overset{11}{\to} -(-1)^{k-r+1} C}_{r}.$$

Case 2: $r = k$. We have $M = 2^k \otimes T = 2^i + 2^k$. For $e_{2^k} e_T$, "shuffling" $\underbrace{00...010...0}_{i-k \quad k+1}$ with $\underbrace{100...00...0}_{i-k \quad k+1}$, it results

$$\underbrace{01\ 00\ 00...00}_{(i-k)\text{ pairs}}\ \underbrace{10\ 00\ 00\ ...00}_{(k+1)\text{ pairs}}.$$

Starting with A_0, we get:

$$\underbrace{A_0 \overset{01}{\to} A \overset{00}{\to} ..... \overset{00}{\to} A}_{i-k} \underbrace{\overset{10}{\to} C \overset{00}{\to} C \overset{00}{\to} ... \overset{00}{\to} C}_{k+1}.$$

For $e_{2^k} e_{T+1}$, "shuffling" $\underbrace{00...010...0}_{i-k \quad k+1}$ with $\underbrace{100...00...1}_{i-k \quad k+1}$, it results

$$\underbrace{01\ 00\ 00...00}_{(i-k)\text{ pairs}}\ \underbrace{10\ 00\ 00\ ...01}_{(k+1)\text{ pairs}}.$$

Starting with A_0, we get:

$$\underbrace{A_0 \overset{01}{\to} A \overset{00}{\to}}_{i-k} ... \overset{00}{\to} \underbrace{A \overset{10}{\to} C \overset{00}{\to} C \overset{00}{\to} ... \overset{01}{\to} -C}_{k+1}.$$

etc.□

Proposition 3.3.8. ([Fl, Sh; 15(1)]) *Let* $A_t = \left(\frac{\gamma_1,...,\gamma_t}{\mathbb{R}}\right)$ *be an algebra obtained by the Cayley-Dickson process. For any* $x_1, x_2, ..., x_t \in \mathbb{R} - \{0\}$, *we have that*

$$\left(\frac{\gamma_1, ..., \gamma_t}{\mathbb{R}}\right) \simeq \left(\frac{\gamma_1 x_1^2, ..., \gamma_t x_t^2}{\mathbb{R}}\right).$$

Proof. Let $A_t = \left(\frac{\gamma_1,...,\gamma_t}{\mathbb{R}}\right)$ with the basis $\{e_0 = 1, e_1, ..., e_{n-1}\}$, $n = 2^t$ and let $A_t' = \left(\frac{\gamma_1 x_1^2,...,\gamma_t x_t^2}{\mathbb{R}}\right)$ with the basis $\{e_0' = 1, e_1', ..., e_{n-1}'\}$ such that $(e_i')^2 = \gamma_i x_i^2$, $i \in \{1, 2, ..., n-1\}$. We remark that $(x_i e_i)^2 = x_i^2 \gamma_i$ and from here, it results that the map $\tau : A_t' \to A_t$, $\tau(e_i') = e_i x_i$ is an algebra isomorphism. □

The above proposition generalized Proposition 1.1, p. 52 from [La; 04].

Remark 3.3.9. From the above proposition, it results that for each $n = 2^t$ there are only n non-isomorphic algebras A_t. These algebras are of the form $A_t = \left(\frac{\gamma_1,...,\gamma_t}{\mathbb{R}}\right)$, with $\gamma_1, ..., \gamma_t \in \{-1, 1\}$.

Proposition 3.3.10 ([Fl; 14]) *Let* $A_t = \left(\frac{-1,...,-1}{\mathbb{R}}\right)$ *be an algebra obtained by the Cayley-Dickson process with* $\{e_0 = 1, e_1, ..., e_{n-1}\}$, $n = 2^t$ *a basis in* A_t. *Let* $r \geq 1$, $r < k \leq i < t$. *We have*

$$\begin{array}{c|cc} \cdot & e_T & e_{T+1} \\ \hline e_{2^{k-r+1}} & (-1)^{r+2} e_M & -(-1)^{r+2} e_{M+1} \\ e_{2^{k-r+1}+1} & -(-1)^{r+2} e_{M+1} & -(-1)^{r+2} e_M \end{array}, \qquad (3.3.9.)$$

where the binary decomposition of M *is* $M_2 = 2^k \otimes T$, *with* $T = 2^r + 2^{r+1} + ... + 2^k + 2^i$.

Proof. We compute $e_{2^{k-r+1}} e_T$. We have $e_{2^{k-r+1}} e_T = \gamma(s, q) e_M$, where the binary decomposition of M is $M_2 = 2^{k-r+1} \otimes T$ and s is the binary decomposition for 2^{k-r+1} and q is the binary decomposition for T,

$$s = \underbrace{00...0}_{i-k+r-1}\ \underbrace{100...0}_{k-r+2}, q = 1\underbrace{00...0}_{i-k-1}\underbrace{111..1}_{k-r+1}\underbrace{0...0}_{r}.$$

By "shuffling" $s \otimes q$, it results

$$\underbrace{01\ 00\ 00...00}_{i-k}\ \underbrace{01\ 01\ 01\ ...01}_{k-2r-1}\ \underbrace{11\ 01\ 01\ ...01}_{r+2}\ \underbrace{00\ 00\ ...00\ 00}_{r}.$$

Starting with A_0,we get:

$$\underbrace{A_0 \overset{01}{\to} A \overset{00}{\to} ... \overset{00}{\to}}_{i-k} \underbrace{A \overset{01}{\to} A \overset{01}{\to} ... \overset{01}{\to}}_{k-2r-1} \underbrace{A \overset{11}{\to} -C \overset{01}{\to} C \overset{01}{\to} -C \overset{01}{\to} C ... \overset{01}{\to} (-1)^{r+2} C}_{r+2} \underbrace{\overset{00}{\to} ... \overset{00}{\to} (-1)^{r+2} C}_{r}.$$

Therefore $\gamma(s,q) = (-1)^{k-r+1}$.

Now, we compute $e_{2^{k-r+1}} e_{T+1}$. For this, we will "shuffling" $\underbrace{00...0}_{i-k+r-1}\ \underbrace{100...0}_{k-r+2}$ with $1\underbrace{00...0}_{i-k-1}\underbrace{111..10}_{k-r+1}\underbrace{...1}_{r}$. It results

$$\underbrace{01\ 00\ 00...00}_{i-k}\ \underbrace{01\ 01\ 01\ ...01}_{k-2r-1}\ \underbrace{11\ 01\ 01\ ...01}_{r+2}\ \underbrace{00\ 00\ ...00\ 01}_{r}.$$

Starting with A_0,we get:

$$\underbrace{A_0 \overset{01}{\to} A \overset{00}{\to} ... \overset{00}{\to}}_{i-k} \underbrace{A \overset{01}{\to} A \overset{01}{\to} ... \overset{01}{\to}}_{k-2r-1} \underbrace{A \overset{11}{\to} -C \overset{01}{\to} C \overset{01}{\to} -C \overset{01}{\to} C ... \overset{01}{\to} (-1)^{r+2} C}_{r+2} \underbrace{\overset{00}{\to} ... \overset{01}{\to} (-1)^{r+3} C}_{r}.$$

For $e_{2^{k-r+1}+1} e_T$, "shuffling" $\underbrace{00...0}_{i-k+r-1}\ \underbrace{100...1}_{k-r+2}$ with $1\underbrace{00...0}_{i-k-1}\underbrace{111..10}_{k-r+1}\underbrace{...0}_{r}$, it results

$$\underbrace{01\ 00\ 00...00}_{i-k}\ \underbrace{01\ 01\ 01\ ...01}_{k-2r-1}\ \underbrace{11\ 01\ 01\ ...01}_{r+2}\ \underbrace{00\ 00\ ...00\ 10}_{r}.$$

Starting with A_0,we get:

$$\underbrace{A_0 \overset{01}{\to} A \overset{00}{\to} ... \overset{00}{\to}}_{i-k} \underbrace{A \overset{01}{\to} A \overset{01}{\to} ... \overset{01}{\to}}_{k-2r-1} \underbrace{A \overset{11}{\to} -C \overset{01}{\to} C \overset{01}{\to} -C \overset{01}{\to} C ... \overset{01}{\to} (-1)^{r+2} C}_{r+2} \underbrace{\overset{00}{\to} ... \overset{10}{\to} (-1)^{r+3} C}_{r}.$$

For $e_{2^{k-r+1}+1} e_{T+1}$, we compute first $\left(2^{k-r+1}+1\right) \otimes (T+1)$. We obtain:

$$\left(2^{k-r+1}+1\right) \otimes (T+1) =$$

$$= \left(\underbrace{00...0}_{i-k+r-1}\ \underbrace{100...1}_{k-r+2} \right) \otimes \left(1\underbrace{00...0}_{i-k-1}\underbrace{111..10}_{k-r+1}\underbrace{...1}_{r} \right) =$$

$$= \underbrace{10...0}_{i-k}\underbrace{11..10}_{r-1}\ \underbrace{1...1}_{k-2r+1}\ \underbrace{0...0}_{r} = 2^{k-r+1} \otimes T = M.$$

Now, "shuffling" $\underbrace{00...0}_{i-k+r-1}\ \underbrace{100...1}_{k-r+2}$ with $1\underbrace{00...0}_{i-k-1}\underbrace{111..1}_{k-r+1}\underbrace{0...1}_{r}$, it results

$$\underbrace{01\ 00\ 00...00}_{i-k}\ \underbrace{01\ 01\ 01\ ...01}_{k-2r-1}\ \underbrace{11\ 01\ 01\ ...01}_{r+2}\ \underbrace{00\ 00\ ...00\ 11}_{r}$$

Starting with A_0,we get:

$$\underbrace{A_0 \overset{01}{\to} A \overset{00}{\to} ... \overset{00}{\to} A}_{i-k} \underbrace{\overset{01}{\to} A \overset{01}{\to} ... \overset{01}{\to} A}_{k-2r-1} \underbrace{\overset{11}{\to} -C \overset{01}{\to} C \overset{01}{\to} -C \overset{01}{\to} C... \overset{01}{\to} (-1)^{r+2} C}_{r+2} \underbrace{\overset{00}{\to} ... \overset{11}{\to} (-1)^{r+3} C}_{r}.$$

3.4. An example of A_t-holomorphic functions

Let $\mathbb{C}$ be the complex field and let S be a subset of $\mathbb{C}$.A complex number w is called a limit point of S if and only if for any $\delta > 0$, there is an element $z \in S$ such that $0 < |z - w| < \delta$.

We consider the map $f : S \to \mathbb{C}$ a function with S a subset of $\mathbb{C}$. Let w be a limit point of S. A complex number l is said to be *the limit* of the function f when z tends to w in S if for an arbitrary real number ε such that $\varepsilon > 0$, there is a real number $\delta,\ \delta > 0$ such that $|f(z) - l| < \varepsilon$, for all elements $z \in S$ such that $0 < |z - w| < \delta$. We write this

$$\lim_{z \to w} f\,(z) = l.$$

With the above notations, the function f is said to be *continuous* in w if for an arbitrary real number ε such that $\varepsilon > 0$, there is a real number $\delta,\ \delta > 0$ such that $|f(z) - f\,(w)\,| < \varepsilon$ for all elements $z \in S$ such that $|z - w| < \delta$.

Let w be a complex number and let r be a non-negative real number. We define the set

$$B(w,r) = \{z \in \mathbb{C} \ / \ |z-w| < r\}$$

called the open disk of radius r about w. A subset W of the complex plane is called *an open subset* if and only if for any element $w \in W$ there is $\delta > 0$ such that $B(w,r) \subset V$.([Wi; 08])

Let S be an open subset of $\mathbb{C}$. The function f *is differentiable* in a point $z_0 \in S$ if the limit

$$f'(z_0) = \lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0}$$

exist. This limit is called *the derivative* of f in z_0. If f is differentiable in all points of D, then f is called holomorphic in S.

Let $f : S \to \mathbb{C}$ be a complex function $f(x+iy) = u(x,y) + iv(x,y)$, with $u(x,y), v(x,y)$ a real functions. If f is differentiable in $z_0 = x_0 + iy_0$, then we have

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}$$

in (x_0, y_0). The above relation are called *the Cauchy–Riemann equations*. Denoting with

$$\frac{\partial f}{\partial x} = \frac{\partial u}{\partial x} + i\frac{\partial v}{\partial x}, \frac{\partial f}{\partial y} = \frac{\partial u}{\partial y} + i\frac{\partial v}{\partial y},$$

we obtain $\frac{\partial f}{\partial y} = -i\frac{\partial f}{\partial x}$, therefore $\frac{\partial f}{\partial x} + i\frac{\partial f}{\partial y} = 0$. We call the operator $D = \frac{\partial}{\partial x} + i\frac{\partial}{\partial y}$ the Dirac operator. If u and v satisfy the Cauchy–Riemann equations and have continuous first partial derivatives, then f is holomorphic. Therefore if

$$Df = 0 \qquad (3.4.1,)$$

and u and v have continuous first partial derivatives, then f is holomorphic.

In an Euclidean space the Dirac operator has the form

$$D = \sum_{k=1}^{n} e_k \frac{\partial}{\partial x_k}$$

where $e_1, e_2, ..., e_n$ is an orthonormal basis in $\mathbb{R}^n$ and $\mathbb{R}^n$ is considered to be embedded in a Clifford algebra.

How we can generalize the definition of holomorphic functions to all algebras obtained by the Cayley-Dickson process? The real vector space $\mathbb{R}^3$ can be included in the generalized quaternion algebra $\mathbb{H}(\alpha, \beta)$ if we identify $(x, y, z) \in \mathbb{R}^3$ with a pure quaternion $z = xi + yj + zk$, with $z^2 = -\mathbf{n}(z) \in K$. Therefore, to a domain $\Omega \subset \mathbb{R}^3$ we will associate the domain $\Omega_\zeta := \{\zeta = x_1e_1 + x_2e_2 + x_3e_3 \ / \ (x_1, x_2, x_3) \in \Omega\}$ included in $\mathbb{H}(\alpha, \beta)$. Consider a function $\Phi : \Omega_\zeta \to \mathbb{H}(\alpha, \beta)$ of the form

$$\Phi(\zeta) = \sum_{k=1}^{3} \Phi_k(x_1, x_2, x_3)e_k, \tag{3.4.2.}$$

where $(x_1, x_2, x_3) \in \Omega$ and $\Phi_k : \Omega \to \mathbb{R}$.

We say that this function is *hyperholomorphic* in a domain Ω_ζ if the first partial derivatives $\partial\Phi_k/\partial x_k$ exist in Ω and the following equality is fulfilled in every point of Ω_ζ

$$D[\Phi](\zeta) = \sum_{k=1}^{3} e_k \frac{\partial \Phi}{\partial x_k} = 0.$$

Definition 3.4.2. Let $\{e_0 = 1, e_1, ..., e_{n-1}\}$ be a basis in $A_t = \left(\frac{\gamma_1,...,\gamma_t}{\mathbb{R}}\right)$, $n = 2^t$. To domain $\Omega \subset \mathbb{R}^{2^t-1}$, we will associate the domain $\Omega_\zeta = \{\zeta = x_1e_1 + \ldots + x_{n-1}e_{n-1}/(x_1, x_2, \ldots, x_{n-1}) \in \Omega\}$ included in A_t.

Consider a function $\Phi : \Omega_\zeta \to A_t$ of the form

$$\Phi(\zeta) = \sum_{k=1}^{n-1} \Phi_k(x_1, x_2, \ldots, x_{n-1})e_k, \tag{3.4.3.}$$

where $(x_1, x_2, \ldots, x_{n-1}) \in \Omega$ and $\Phi_k : \Omega \to \mathbb{R}$. The domain Ω_ζ is called *congruent* with the domain Ω.

We say that a function of the form (3.4.3) is *left A_t-holomorphic* in a domain Ω_ζ if the first partial derivatives $\partial\Phi_k/\partial x_k$ exist in Ω and the following equality is fulfilled in every point of Ω_ζ

$$D[\Phi](\zeta) = \sum_{k=1}^{2^t-1} e_k \frac{\partial \Phi}{\partial x_k} = 0.$$

The operator D is called *Dirac operator*.

Remark 3.4.3. Let $\mathbb{H}(\gamma_1, \gamma_2)$ be the generalized quaternion algebra with the basis $\{1, e_1, e_2, e_3\}$, $\gamma_1 < 0$, $\gamma_2 < 0$ and $\mathbb{H}(-1, -1)$ be the usual quaternion

division algebra with the basis $\{1, i, j, k\}$. Let Ω be a domain in $\mathbb{R}^3$, and let $\Omega_\zeta := \{\zeta = xi + yj + zk : (x, y, z) \in \Omega\}$ be a corresponding domain in $\mathbb{H}(-1, -1)$. The function $\Phi : \Omega_\zeta \to \mathbb{H}(-1, -1)$ of the form

$$\Phi(\zeta) = u_1(x, y, z) + u_2(x, y, z)\, i + u_3(x, y, z)\, j + u_4(x, y, z)\, k.$$

is hyperholomorphic in the domain Ω if

$$D[\Phi](\zeta) = i\frac{\partial \Phi}{\partial x} + j\frac{\partial \Phi}{\partial y} + k\frac{\partial \Phi}{\partial z} = 0$$

and the first partial derivatives $\partial u_k / \partial x_k$ exist in Ω.

For another domain $\Delta \subset \mathbb{R}^3$, we associate the domain $\Delta_{\widetilde{\zeta}} := \{\widetilde{\zeta} = \widetilde{x}e_1 + \widetilde{y}e_2 + \widetilde{z}e_3 : (\widetilde{x}, \widetilde{y}, \widetilde{z}) \in \Delta\}$ in the algebra $\mathbb{H}(\gamma_1, \gamma_2)$. The Dirac operator in $\mathbb{H}(\gamma_1, \gamma_2)$, denoted by $\widetilde{D}$, is

$$\widetilde{D} = e_1\frac{\partial}{\partial \widetilde{x}} + e_2\frac{\partial}{\partial \widetilde{y}} + e_3\frac{\partial}{\partial \widetilde{z}}.$$

The elements of bases in $\mathbb{H}(-1, -1)$ and $\mathbb{H}(\gamma_1, \gamma_2)$ satisfy the following equalities:

$$e_1 = i\sqrt{-\gamma_1}, \quad e_2 = j\sqrt{-\gamma_2}, \quad e_3 = k\sqrt{\gamma_1\gamma_2}. \tag{3.4.4.}$$

Now we establish a connection between hyperholomorphic functions in the algebras $\mathbb{H}(-1, -1)$ and $\mathbb{H}(\gamma_1, \gamma_2)$, where $\gamma_1 < 0,\ \gamma_2 < 0$. For this, we denote

$$x = \frac{1}{\sqrt{-\gamma_1}}\widetilde{x}, \quad y = \frac{1}{\sqrt{-\gamma_2}}\widetilde{y}, \quad z = \frac{1}{\sqrt{\gamma_1\gamma_2}}\widetilde{z}.$$

These relations give us the operator equalities:

$$\frac{\partial}{\partial \widetilde{x}} = \frac{1}{\sqrt{-\gamma_1}}\frac{\partial}{\partial x}, \quad \frac{\partial}{\partial \widetilde{y}} = \frac{1}{\sqrt{-\gamma_2}}\frac{\partial}{\partial y}, \quad \frac{\partial}{\partial \widetilde{z}} = \frac{1}{\sqrt{\gamma_1\gamma_2}}\frac{\partial}{\partial z}. \tag{3.4.5.}$$

Now, using relations (3.4.4) and (3.4.5), we obtain

$$\widetilde{D}[\Phi](\widetilde{\zeta}) = e_1\frac{\partial \Phi}{\partial \widetilde{x}} + e_2\frac{\partial \Phi}{\partial \widetilde{y}} + e_3\frac{\partial \Phi}{\partial \widetilde{z}} =$$

$$= i\frac{\partial \Phi}{\partial x}\frac{1}{\sqrt{-\gamma_1}}\sqrt{-\gamma_1} + j\frac{\partial \Phi}{\partial y}\frac{1}{\sqrt{-\gamma_2}}\sqrt{-\gamma_2} + k\frac{\partial \Phi}{\partial z}\frac{1}{\sqrt{\gamma_1\gamma_2}}\sqrt{\gamma_1\gamma_2} =$$

$$= i\frac{\partial \Phi}{\partial x} + j\frac{\partial \Phi}{\partial y} + k\frac{\partial \Phi}{\partial z} = D[\Phi](\zeta) = 0.$$

Using the above notations, we obtain the following theorem:

Theorem 3.4.4. *Let Ω be an arbitrary domain in $\mathbb{R}^3$ and Δ be a domain in $\mathbb{R}^3$ such that the coordinates of the corresponding points $\zeta = xi + yj + zk \in \Omega_\zeta$ and $\widetilde{\zeta} = \widetilde{x}e_1 + \widetilde{y}e_2 + \widetilde{z}e_3 \in \Delta_{\widetilde{\zeta}}$ satisfy the following relations:*

$$x = \frac{1}{\sqrt{-\gamma_1}}\widetilde{x}, \ \ y = \frac{1}{\sqrt{-\gamma_2}}\widetilde{y}, \ \ z = \frac{1}{\sqrt{\gamma_1\gamma_2}}\widetilde{z}.$$

Then if the function $\Phi : \Omega_\zeta \to \mathbb{H}(-1,-1)$ is hyperholomorphic in the domain Ω_ζ, then the same function Φ, of $\widetilde{\zeta}$, is hyperholomorphic in the domain $\Delta_{\widetilde{\zeta}} \in \mathbb{H}(\gamma_1,\gamma_2)$ with $\gamma_1 < 0$, $\gamma_2 < 0$. The converse is also true.

Proof. It results directly from Remark 3.4.3.□

Remark 3.4.5. (i) The above Theorem tell us that for studying hyperholomorphic functions in generalized quaternion algebras $\mathbb{H}(\gamma_1,\gamma_2)$ with $\gamma_1 < 0$, $\gamma_2 < 0$ it is suffices to consider hyperholomorphic functions only in the usual quaternion algebra $\mathbb{H}(-1,-1)$.

(ii) The result similar to the previous remark was established in the paper [Pl, Sh; 11], Theorem 5, in a three-dimensional commutative associative algebra.

Theorem 3.4.6. *Let $A_t = \left(\frac{\gamma_1,\ldots,\gamma_t}{\mathbb{R}}\right)$ be a generalized Cayley-Dickson algebra with $\gamma_1 < 0, \ldots, \gamma_t < 0$. Let Ω be an arbitrary domain in $\mathbb{R}^{2^t-1}$ and Δ be a domain in $\mathbb{R}^{2^t-1}$ such that the coordinates of the corresponding points $\zeta = x_1e_1 + \ldots + x_{2^t-1}e_{2^t-1} \in \Omega_\zeta$ and $\widetilde{\zeta} = \widetilde{x}_1\widetilde{e}_1 + \widetilde{x}_2\widetilde{e}_2 + \ldots + \widetilde{x}_{2^t-1}\widetilde{e}_{2^t-1} \in \Delta_{\widetilde{\zeta}}$ satisfy the following relations*

$$x_1 = \frac{1}{\sqrt{-\gamma_1}}\widetilde{x}_1, \quad x_2 = \frac{1}{\sqrt{-\gamma_2}}\widetilde{x}_2, \ \ \ldots, \ \ x_n = \frac{1}{\sqrt{(-1)^t\gamma_1\ldots\gamma_t}}\widetilde{x}_n.$$

If the function $\Phi : \Omega_\zeta \to \left(\frac{-1,\ldots,-1}{\mathbb{R}}\right)$ is left A_t-holomorphic in the domain Ω_ζ, then the same function Φ, but depending of $\widetilde{\zeta}$ is left A_t-holomorphic in the domain $\Delta_{\widetilde{\zeta}} \in A_t$. The converse is also true.

Proof. Let $\{1, e_1, ..., e_{n-1}\}$ be a basis in $\left(\frac{-1,\ldots,-1}{\mathbb{R}}\right)$ and $\{1, \widetilde{e}_1, ..., \widetilde{e}_{n-1}\}$ be a basis in $A_t = \left(\frac{\gamma_1,\ldots,\gamma_t}{\mathbb{R}}\right)$.

Since

$$\widetilde{e}_1 = e_1\sqrt{-\gamma_1}, \quad \widetilde{e}_2 = e_2\sqrt{-\gamma_2}, \ldots,$$

$$\ldots, \widetilde{e}_{n-1} = e_{n-1}\sqrt{(-1)^t \gamma_1 \ldots \gamma_t}\,,$$

the result is obtained from a simple computation as in Remark 3.4.3.□

Remark 3.4.7. Using above Theorem, it is obvious that, for studying left A_t-holomorphic functions in generalized Cayley-Dickson algebras $A_t = \left(\frac{\gamma_1,\ldots,\gamma_t}{\mathbb{R}}\right)$ with $\gamma_1 < 0, \ldots, \gamma_t < 0$. it is suffices to consider left A_t-holomorphic functions only in the algebras $\left(\frac{-1,\ldots,-1}{\mathbb{R}}\right)$.

Now we consider another class of differentiable functions. Let $A_t = \left(\frac{\gamma_1,\ldots,\gamma_t}{\mathbb{R}}\right)$, with $\gamma_1 = ... = \gamma_t = -1$, and the domain $\Omega \subset \mathbb{R}^{2^t}$. We denote with $\Omega_\zeta := \{\zeta = x_0 + x_1 e_1 + \ldots + x_{n-1}e_{n-1} : (x_0, x_1, \ldots, x_{n-1}) \in \Omega\}$ a domain in A_t. This domain is *congruent* with the domain Ω.

We consider a function $\Phi : \Omega_\zeta \to A_t$ of the form

$$\Phi(\zeta) = \sum_{k=0}^{n-1} \Phi_k(x_0, x_1, \ldots, x_{n-1}) e_k, \tag{3.4.6.}$$

where $(x_0, x_1, \ldots, x_{n-1}) \in \Omega$ and $\Phi_k : \Omega \to \mathbb{R}$.

We say that a function of the form (3.4.6) is *left A_t-hyperholomorphic* in a domain Ω_ζ if the first partial derivatives $\partial\Phi_k/\partial x_k$ exist in Ω and the following equality is fulfilled in every point of Ω_ζ

$$\sum_{k=0}^{2^t-1} e_k \frac{\partial \Phi}{\partial x_k} = 0.$$

In the following, we will provide an algorithm to constructing a left A_t-hyperholomorphic function. Using the above notations, let $v\,(x, y)$ be a rational function defined in a domain $G \subset \mathbb{R}^2$. In the following, using some ideas given in Theorem 3 from [Xi, Zh, Li; 05], we will give an example of left A_t-hyperholomorphic function, for all $t \geq 1,\ t \in \mathbb{N}$. For this, we consider the following functions:

$$\phi_1 = x_0 + e_1 x_1, \quad \phi_2 = \frac{1}{e_1}(x_0 + e_1 x_1),$$

$$\rho_{2s-1} = x_{2s} - e_1 x_{2s+1}, \quad \rho_{2s} = -\frac{1}{e_1}(x_{2s} - e_1 x_{2s+1}), \ \ s \in \{1, 2, ..., 2^{t-1} - 1\},$$

$$F_t\,(\zeta) = v\,(\phi_1, \phi_2) + v\,(\rho_1, \rho_2)\,e_2 + v\,(\rho_3, \rho_4)\,e_4 + [v\,(\rho_5, \rho_6)\,e_2]\,e_4 +$$

$$+v\,(\rho_7, \rho_8)\,e_8 + (v\,(\rho_9, \rho_{10})\,e_2)\,e_8 + (v\,(\rho_{11}, \rho_{12})\,e_4)\,e_8 + [(v\,(\rho_{13}, \rho_{14})\,e_2)\,e_4]\,e_8 + ...$$

$$...+\sum_{i=4}^{t-1}(\sum_{k=1}^{i}(\sum_{r=1}^{k-1}v\left(\rho_{M_{rki}-1},\rho_{M_{rki}}\right)e_{2^r})e_{2^{r+1}}...)e_{2^k})e_{2^i})+\sum_{i=1}^{t-1}\left(v\left(\rho_{2^i-1},\rho_{2^i}\right)e_{2^i}\right),$$

where $M_{rki}=2^r+2^{r+1}+...+2^k+2^i$.

It results

$$F_t\left(\zeta\right)=v\left(\phi_1,\phi_2\right)+$$

$$+\sum_{i=1}^{t-1}(\sum_{k=1}^{i}(\sum_{r=1}^{k-1}v\left(\rho_{M_{rki}-1},\rho_{M_{rki}}\right)e_{2^r})e_{2^{r+1}}...)e_{2^k})e_{2^i})+\sum_{i=1}^{t-1}\left(v\left(\rho_{2^i-1},\rho_{2^i}\right)e_{2^i}\right),$$

or

$$F_t\left(\zeta\right)=F_{t-1}\left(\zeta\right)+$$

$$+(\sum_{k=1}^{t-2}(\sum_{r=1}^{k-1}v\left(\rho_{M_{rk(t-1)}-1},\rho_{M_{rk(t-1)}}\right)e_{2^r})e_{2^{r+1}}...)e_{2^k})e_{2^{t-1}})+v\left(\rho_{2^{t-1}-1},\rho_{2^{t-1}}\right)e_{2^{t-1}}.$$

We denote with $\mathbb{C}_{2s}$ the "complex" planes $\{x_{2s}+e_1x_{2s+1}\ /\ x_{2s},x_{2s+1}\in\mathbb{R}\}$ and with $D_{2s}=\{(x_{2s},x_{2s+1})\ /\ x_{2s}+e_1x_{2s+1}\in\mathbb{C}_{2s}\}$, $s\in\{0,1,2,...,2^{t-1}-1\}$ the Euclidian planes. Let G_{2s} be domains in $\mathbb{C}_{2s}$ and let $\widetilde{G}_{2s}$ be the corresponded domains in D_{2s}. We have the following theorem

Theorem 3.4.8. *With the above notations, we consider the functions $v\left(\phi_1,\phi_2\right)$ and $v\left(\rho_{2s-1},\rho_{2s}\right)$ defined in the corresponding domains $G_0\subset\mathbb{C}_0$ and $G_{2s}\subset\mathbb{C}_{2s}$, $s\in\{1,2,...,2^{t-1}-1\}$. Then the map $F_t\left(\zeta\right)$ is a left A_t-hyperholomorphic function in the domain $\Theta\subset A_t$ which is congruent with the domain $\widetilde{G}_0\times\widetilde{G}_2\times\widetilde{G}_4\times...\times\widetilde{G}_{2^{t-1}-1}\subset\mathbb{R}^{2^t}$, for $t\geq 1$..*

Proof. For $t=1$, we have $F_1\left(\zeta\right)=v\left(\phi_1,\phi_2\right)$, which is an holomorphic function in $D_0\subset\mathbb{C}_0$, as we can see in [Xi, Zh, Li; 05], Theorem 3.

For $t=2$, we obtain $F_2\left(\zeta\right)=v\left(\phi_1,\phi_2\right)+v\left(\rho_1,\rho_2\right)e_2$ and for $t=3$, we get $F_3\left(\zeta\right)=v\left(\phi_1,\phi_2\right)+v\left(\rho_1,\rho_2\right)e_2+v\left(\rho_3,\rho_4\right)e_4$. $F_2\left(\zeta\right)$ and $F_3\left(\zeta\right)$ are hyperholomorphic, respectively octonionic hyperholomorphic function, from Remark 2.1 and Theorem 3 from [Xi, Zh, Li; 05].

For $t\geq 4$, using induction steps, supposing that $F_{t-1}\left(\zeta\right)$ is a left A_{t-1}-hyperholomorphic function, we will prove that $F_t\left(\zeta\right)$ is A_t-hyperholomorphic.

That means $D[F_t]=0$. We have that

$$D[F_t]=\sum_{k=0}^{2^t-1}e_k\frac{\partial F_t}{\partial x_k}=\sum_{k=0}^{2^{t-1}-1}e_k\frac{\partial F_t}{\partial x_k}+\sum_{k=2^{t-1}}^{2^t-1}e_k\frac{\partial F_t}{\partial x_k}=$$

$$=D[F_{t-1}]+e_{2^{t-1}}\sum_{k=0}^{2^{t-1}-1}\overline{e}_k\frac{\partial F_t}{\partial x_{k+2^{t-1}}}.$$

From induction steps, we obtain $D[F_{t-1}]=0$. We will prove that $\sum\limits_{k=0}^{2^{t-1}-1}\overline{e}_k\dfrac{\partial F_t}{\partial x_{2^{t-1}+k}}=0$. This sum has 2^{t-1} terms. First two terms are:

$$(\frac{\partial F_t}{\partial x_{2^{t-1}}}-e_1\frac{\partial F_t}{\partial x_{2^{t-1}+1}})=$$

$$=\frac{\partial v}{\partial\rho_{2^{t-1}-1}}\frac{\partial\rho_{2^{t-1}-1}}{\partial x_{2^{t-1}}}+\frac{\partial v}{\partial\rho_{2^{t-1}}}\frac{\partial\rho_{2^{t-1}}}{\partial x_{2^{t-1}}}-e_1\left(\frac{\partial v}{\partial\rho_{2^{t-1}-1}}\frac{\partial\rho_{2^{t-1}-1}}{\partial x_{2^{t-1}+1}}+\frac{\partial v}{\partial\rho_{2^{t-1}}}\frac{\partial\rho_{2^{t-1}}}{\partial x_{2^{t-1}+1}}\right)=$$

$$=\frac{\partial v}{\partial\rho_{2^{t-1}-1}}+\frac{\partial v}{\partial\rho_{2^{t-1}}}\left(\frac{-1}{e_1}\right)-e_1\left(\frac{\partial v}{\partial\rho_{2^{t-1}-1}}(-e_1)+\frac{\partial v}{\partial\rho_{2^{t-1}}}\right)=$$

$$=\frac{\partial v}{\partial\rho_{2^{t-1}-1}}+\frac{\partial v}{\partial\rho_{2^{t-1}}}e_1-\frac{\partial v}{\partial\rho_{2^{t-1}-1}}-e_1\frac{\partial v}{\partial\rho_{2^{t-1}}}=0.$$

Since $e_1^2=\gamma_1$, $\gamma_1^2=1$, $\frac{\partial v}{\partial\rho_{2^{t-1}-1}}$ and $\frac{\partial v}{\partial\rho_{2^{t-1}}}$ can be written as $a_{2^{t-1}-1}(\zeta)+b_{2^{t-1}-1}(\zeta)e_1$, respectively $a_{2^{t-1}}(\zeta)+b_{2^{t-1}}(\zeta)e_1$ where $a_{2^{t-1}-1}(\zeta)$, $b_{2^{t-1}-1}(\zeta)$, $a_{2^{t-1}}(\zeta)$, $b_{2^{t-1}}(\zeta)$ are real valued functions.

Case 1: $r<k$. In the general case, we denote $T=2^r+2^{r+1}+...+2^k+2^{t-1}$ and $T_1=2^r+2^{r+1}+...+2^k$, for $r<k$. We will compute the terms

$$-e_{T_1}\frac{\partial F_t}{\partial x_T}-e_{T_1+1}\frac{\partial F_t}{\partial x_{T+1}}.$$

We compute first $\frac{\partial F_t}{\partial x_T}$. It results

$$\frac{\partial F_t}{\partial x_T}=(...\left(\frac{\partial v}{\partial\rho_{T-1}}\frac{\partial\rho_{T-1}}{\partial x_T}+\frac{\partial v}{\partial\rho_T}\frac{\partial\rho_T}{\partial x_T}\right)e_{2^r})e_{2^{r+1}})...e_{2^k})e_{2^{t-1}}=$$

$$= (... \left(\frac{\partial v}{\partial \rho_{T-1}} + \frac{\partial v}{\partial \rho_T} \frac{-1}{e_1} \right) e_{2^r}) e_{2^{r+1}}) ... e_{2^k}) e_{2^{t-1}} =$$

$$= (... \left(\frac{\partial v}{\partial \rho_{T-1}} + \frac{\partial v}{\partial \rho_T} e_1 \right) e_{2^r}) e_{2^{r+1}}) ... e_{2^k}) e_{2^{t-1}}.$$

Since we can write $\frac{\partial v}{\partial \rho_{T-1}}$ under the form $a_{T-1}(\zeta) + b_{T-1}(\zeta) e_1$ and $\frac{\partial v}{\partial \rho_T}$ under the form $a_T(\zeta) + b_T(\zeta) e_1$, where a_{T-1}, b_{T-1}, a_T, b_T are real valued functions, using Proposition 3.3.6, we obtain:

$$\frac{\partial F_t}{\partial x_T} = (... \left(\frac{\partial v}{\partial \rho_{T-1}} + \frac{\partial v}{\partial \rho_T} e_1 \right) e_{2^r}) e_{2^{r+1}}) ... e_{2^k}) e_{2^{t-1}} =$$

$$= (...(a_{T-1}(\zeta) e_{2^r}) e_{2^{r+1}}) ... e_{2^k}) e_{2^{t-1}} + (...(b_{T-1}(\zeta) e_1) e_{2^r}) e_{2^{r+1}}) ... e_{2^k}) e_{2^{t-1}} +$$

$$+(...(a_T(\zeta) e_1) e_{2^r}) e_{2^{r+1}}) ... e_{2^k}) e_{2^{t-1}} + (...(b_T(\zeta) e_1) e_1) e_{2^r}) e_{2^{r+1}}) ... e_{2^k}) e_{2^{t-1}} =$$

$$= a_{T-1}(\zeta)(-1)^{k-r+2} e_T + b_{T-1}(\zeta)(-1)^{k-r+3} e_{T+1} +$$

$$+a_T(\zeta)(-1)^{k-r+3} e_{T+1} - b_T(\zeta)(-1)^{k-r+2} e_T.$$

Using Proposition 3.3.7, we compute $-e_{T_1} \frac{\partial F_t}{\partial x_T}$.

$$-e_{T_1} \frac{\partial F_t}{\partial x_T} = -e_{T_1} (a_{T-1}(\zeta)(-1)^{k-r+2} e_T + b_{T-1}(\zeta)(-1)^{k-r+3} e_{T+1} +$$

$$+a_T(\zeta)(-1)^{k-r+3} e_{T+1} - b_T(\zeta)(-1)^{k-r+2} e_T) =$$

$$= -\left(a_{T-1}(\zeta)(-1)^{k-r+2}(-1)^{k-r+1} e_{2^i} - b_{T-1}(\zeta)(-1)^{k-r+3}(-1)^{k-r+1} e_{2^i+1} \right) -$$

$$-\left(- a_T(\zeta)(-1)^{k-r+3}(-1)^{k-r+1} e_{2^i+1} - b_T(\zeta)(-1)^{k-r+2}(-1)^{k-r+1} e_{2^i} \right) =$$

$$= -\Big(a_{T-1}(\zeta)(-1)^{2k-2r+3}e_{2^i} - b_{T-1}(\zeta)(-1)^{2k-2r+4}e_{2^i+1}\Big) -$$

$$-\Big(- a_T(\zeta)(-1)^{2k-2r+4}e_{2^i+1} - b_T(\zeta)(-1)^{2k-2r+3}e_{2^i}\Big).$$

Now, we compute $\frac{\partial F_t}{\partial x_{T+1}}$. We obtain

$$\frac{\partial F_t}{\partial x_{T+1}} = \Big(...\Big(\frac{\partial v}{\partial \rho_{T-1}}\frac{\partial \rho_{T-1}}{\partial x_{T+1}} + \frac{\partial v}{\partial \rho_T}\frac{\partial \rho_T}{\partial x_{T+1}}\Big)e_{2^r})e_{2^{r+1}})...e_{2^k})e_{2^{t-1}} =$$

$$= \Big(...\Big(- \frac{\partial v}{\partial \rho_{T-1}}e_1 + \frac{\partial v}{\partial \rho_T}\Big)e_{2^r})e_{2^{r+1}})...e_{2^k})e_{2^{t-1}}.$$

Since we can write $\frac{\partial v}{\partial \rho_{T-1}}$ under the form $a_{T-1}(\zeta) + b_{T-1}(\zeta)e_1$ and $\frac{\partial v}{\partial \rho_T}$ under the form $a_T(\zeta) + b_T(\zeta)e_1$, where a_{T-1}, b_{T-1}, a_T, b_T are real valued functions, using Proposition 3.3.6, we obtain:

$$\frac{\partial F_t}{\partial x_{T+1}} = \Big(...\Big(- \frac{\partial v}{\partial \rho_{T-1}}e_1 + \frac{\partial v}{\partial \rho_T}\Big)e_{2^r})e_{2^{r+1}})...e_{2^k})e_{2^{t-1}} =$$

$$= (...(-a_{T-1}(\zeta)e_1)e_{2^r})e_{2^{r+1}})...e_{2^k})e_{2^{t-1}} - (...(b_{T-1}(\zeta)e_1e_1)e_{2^r})e_{2^{r+1}})...e_{2^k})e_{2^{t-1}} +$$

$$+(...(a_T(\zeta))e_{2^r})e_{2^{r+1}})...e_{2^k})e_{2^{t-1}} + (...(b_T(\zeta)e_1))e_{2^r})e_{2^{r+1}})...e_{2^k})e_{2^{t-1}} =$$

$$= -a_{T-1}(\zeta)(-1)^{k-r+3}e_{T+1} + b_{T-1}(\zeta)(-1)^{k-r+2}e_T +$$

$$+a_T(\zeta)(-1)^{k-r+2}e_T + b_T(\zeta)(-1)^{k-r+3}e_{T+1}.$$

Using Proposition 3.3.7, we compute $-e_{T_1+1}\frac{\partial F_t}{\partial x_{T+1}}$.

$$-e_{T_1+1}\frac{\partial F_t}{\partial x_{T+1}} = -e_{T_1+1}\Big(- a_{T-1}(\zeta)(-1)^{k-r+3}e_{T+1} + b_{T-1}(\zeta)(-1)^{k-r+2}e_T +$$

$$+a_T(\zeta)(-1)^{k-r+2}e_T + b_T(\zeta)(-1)^{k-r+3}e_{T+1}\Big) =$$

$$= -\Big(a_{T-1}(\zeta)(-1)^{k-r+3}(-1)^{k-r+1}e_{2^i} - b_{T-1}(\zeta)(-1)^{k-r+2}(-1)^{k-r+1}e_{2^i+1}\Big) -$$

$$-\Big(- a_T(\zeta)(-1)^{k-r+2}(-1)^{k-r+1}e_{2^i+1} - b_T(\zeta)(-1)^{k-r+3}(-1)^{k-r+1}e_{2^i}\Big) =$$

$$= -\Big(a_{T-1}(\zeta)(-1)^{2k-2r+4}e_{2^i} - b_{T-1}(\zeta)(-1)^{2k-2r+3}e_{2^i+1}\Big) -$$

$$-\Big(- a_T(\zeta)(-1)^{2k-2r+3}e_{2^i+1} - b_T(\zeta)(-1)^{2k-2r+4}e_{2^i}\Big).$$

Now, we can compute $-e_{T_1}\frac{\partial F_t}{\partial x_T} - e_{T_1+1}\frac{\partial F_t}{\partial x_{T+1}}$. It results

$$-e_{T_1}\frac{\partial F_t}{\partial x_T} - e_{T_1+1}\frac{\partial F_t}{\partial x_{T+1}} =$$

$$= -\Big(a_{T-1}(\zeta)(-1)^{2k-2r+3}e_{2^i} - b_{T-1}(\zeta)(-1)^{2k-2r+4}e_{2^i+1}\Big) -$$

$$-\Big(- a_T(\zeta)(-1)^{2k-2r+4}e_{2^i+1} - b_T(\zeta)(-1)^{2k-2r+3}e_{2^i}\Big) -$$

$$-\Big(a_{T-1}(\zeta)(-1)^{2k-2r+4}e_{2^i} - b_{T-1}(\zeta)(-1)^{2k-2r+3}e_{2^i+1}\Big) -$$

$$-\Big(- a_T(\zeta)(-1)^{2k-2r+3}e_{2^i+1} - b_T(\zeta)(-1)^{2k-2r+4}e_{2^i}\Big) = 0.$$

Case 2: $r = k$, we use Proposition 3.3.6 and Proposition 3.3.7 and it easy to show that

$$-e_{2^k}\frac{\partial F_t}{\partial x_T} - e_{2^k+1}\frac{\partial F_t}{\partial x_{T+1}} = 0.$$

□

Remark 3.4.9. The above proposition generalizes Theorem 3 from [Xi, Zh, Li; 05].

The Algorithm

1) Input t.

2) Input functions v, ϕ_1, ϕ_2.

3) For $i \in \{1, ..., t-1\}$, $k \in \{1, ..., i\}$, $r \in \{1, ..., k-1\}$, compute $M_{rki} = 2^r + ... + 2^k + 2^i$, $v(\rho_{M_{rki}-1}, \rho_{M_{rki}}) = \alpha_{M_{rki}} + \beta_{M_{rki}} e_1$.

4) For $i \in \{1, ..., t-1\}$, $k \in \{1, ..., i\}$, $r \in \{1, ..., k-1\}$,

-if $r < k$, we compute

$$(...(\alpha_{M_{rki}} + \beta_{M_{rki}} e_1) e_{2^r}) e_{2^{r+1}} ...) e_{2^k}) e_{2^i}) =$$

$$= (-1)^{k-r+2} (\alpha_{M_{rki}} e_{M_{rki}} - \beta_{M_{rki}} e_{M_{rki}-1})$$

-if $r = k$, we compute

$$v(\rho_{2^i-1}, \rho_{2^i}) e_{2^i} = (\alpha_{2^i-1} + \beta_{2^i-1} e_1) e_{2^i} =$$

$$= \alpha_{2^i-1} e_{2^i} + \beta_{2^i-1} e_{2^i+1}.$$

5) Output function

$$F_t(\zeta) = v(\phi_1, \phi_2) + \sum_{i=4}^{t-1} \left(\sum_{k=1}^{i} \left(\sum_{r=1}^{k-1} (-1)^{k-r+2} (\alpha_{M_{rki}}(\zeta) e_{M_{rki}} - \beta_{M_{rki}}(\zeta) e_{M_{rki}-1}) \right) \right) +$$

$$+ \sum_{i=1}^{t-1} (\alpha_{2^i-1}(\zeta) e_{2^i} + \beta_{2^i-1}(\zeta) e_{2^i+1}).$$

3.5. Some equations in algebras obtained by the Cayley-Dickson process

In the following, we reduced the study of an algebraic equation in an arbitrary algebra $\mathbb{H}(\gamma_1, \gamma_2)$ with $\gamma_1, \gamma_2 \in \mathbb{R} \setminus \{0\}$ to the study of the corresponding algebraic equation in one of the following two algebras: division quaternion algebra or split quaternion algebra. Moreover, De Moivre's formula and Euler's formula in generalized quaternion algebras, founded in [Ma, Ja; 13], was proved using this new method, for $\gamma_1, \gamma_2 < 0$. With this technique, the above mentioned results were also obtained for the octonions.The results presented below, were obtained especially in the paper [Fl, Sh; 15(2)].

We denote with $\gamma_1' = sign(\gamma_1)\gamma_1$, $\gamma_2' = sign(\gamma_2)\gamma_2$. An isomorphism between the algebras $\mathbb{H}(\gamma_1, \gamma_2)$ and $\mathbb{H}(-1, -1)$ or between the algebras $\mathbb{H}(\gamma_1, \gamma_2)$ and $\mathbb{H}(1, -1)$ is given by the operator A and its inverse A^{-1}, where

$$A: \quad e_1 \mapsto i\sqrt{\gamma_1'}, \quad e_2 \mapsto j\sqrt{\gamma_2'}, \quad e_3 \mapsto k\sqrt{\gamma_1'\gamma_2'}. \tag{3.5.1.}$$

Depending on the sign of γ_1 and γ_2, we obtain four distinct operators. It is easy to prove the following properties for the operator A :

1) $A(\lambda x) = \lambda A(x), \forall\, \lambda \in \mathbb{R}, \forall\, x \in \mathbb{H}(\gamma_1, \gamma_2)$;

2) $A(x + y) = A(x) + A(y), \forall\, x, y \in \mathbb{H}(\gamma_1, \gamma_2)$;

3) $A(xy) = A(x)\, A(y), \forall\, x, y \in \mathbb{H}(\gamma_1, \gamma_2)$.

From here, it results that the operators A and A^{-1} are additive and multiplicative.

Proposition 3.5.1. *The operators A and A^{-1} are continuous and their norms are equal with* 1.

Proof. We denote by $\| \ \|_{\mathbb{H}(\gamma_1,\gamma_2)}$ the Euclidian norm in $\mathbb{H}(\gamma_1, \gamma_2)$. Since the spaces $\mathbb{H}(\gamma_1, \gamma_2)$ and $\mathbb{H}(-1, -1)$ are normed spaces, then the continuity of A is equivalent with the boundedness of A, i.e. there is a real constant c such that for all $x \in \mathbb{H}(\gamma_1, \gamma_2)$, we have $\frac{\|A(x)\|_{\mathbb{H}(-1,-1)}}{\|x\|_{\mathbb{H}(\gamma_1,\gamma_2)}} \leq c$. Supposing that γ_1,

$\gamma_2 < 0$, it results that
$\frac{\left\|x_0+x_1 i\sqrt{-\gamma_1}+x_2 j\sqrt{-\gamma_2}+x_3 k\sqrt{\gamma_1\gamma_2}\right\|}{\|x_0+x_1e_1+x_2e_2+x_3e_3\|} =$
$= \frac{\sqrt{x_0^2-x_1^2\gamma_1-x_2^2\gamma_2+x_3^2\gamma_3}}{\sqrt{x_0^2-x_1^2\gamma_1-x_2^2\gamma_2+x_3^2\gamma_3}} = 1.$
□

Since each algebra $\mathbb{H}(\gamma_1, \gamma_2)$ is isomorphic with division algebra of quaternions or with algebra of split quaternions, it results that the above operators provide us a simple way to generalize known results in these two algebras to generalized quaternion algebra.

Let $x = x_0 + x_1e_1 + x_2e_3 + x_3e_3 \in \mathbb{H}(\gamma_1, \gamma_2)$ and let $f : \mathbb{H}(\gamma_1, \gamma_2) \to \mathbb{H}(\gamma_1, \gamma_2)$ be a continuous function of the form $f(x) = f_0(x_0, x_1, x_2, x_3) + f_1(x_0, x_1, x_2, x_3)e_1 + f_2(x_0, x_1, x_2, x_3)e_2 + f_3(x_0, x_1, x_2, x_3)e_3$. Let F be the one of the operators given by the relation (3.5.1), depending on the signs of γ_1 and γ_2. We define the operator $\mathfrak{F}$ which for any continuous function f, taking values in $\mathbb{H}(\gamma_1, \gamma_2)$, maps it in the continuous function $\mathfrak{F}f$, taking values in $\mathbb{H}(-1, -1)$ or $\mathbb{H}(1, -1)$ by the rule:

$$\mathfrak{F}f := f_0 + f_1\, F(e_1) + f_2\, F(e_2) + f_3\, F(e_3).$$

Theorem 3.5.2. *Let $x^0 \in \mathbb{H}(\gamma_1, \gamma_2)$ be a root of the equation $f(x) = 0$ in $\mathbb{H}(\gamma_1, \gamma_2)$. Then $F(x^0)$ is a root of the equation $\mathfrak{F}f(F(x)) = 0$ in $\mathbb{H}(-1, -1)$ or $\mathbb{H}(1, -1)$, depending on the signs of γ_1 and γ_2. The converse is also true.*

Proof. Let $\gamma_1, \gamma_2 > 0$. Applying operator A to the equality $f(x^0) = 0$ and using the continuity of A, we obtain

$$A(f(x^0)) = Af(A(x^0)) = A(0) = 0.$$

To prove the converse statement we apply the operator A^{-1} to the equality $f(x^0) = 0$. The remaining cases can be proved similarly. □

Therefore, all results from division algebra of quaternions or algebra of split quaternions can be generalized in $\mathbb{H}(\gamma_1, \gamma_2)$.

It is known that each polynomial of degree n with coefficients in a field K has at most n roots in K. If we consider the coefficients in $\mathbb{H}(-1, -1)$, the situation is not the same. For the real division quaternion algebra over the real

field, there is a kind of a fundamental theorem of algebra: *If a polynomial has only one term of the greatest degree, then it has at least one root in* $\mathbb{H}(-1,-1)$. ([Sm; 04], Theorem 65; [Ei, Ni; 44], Theorem 1).

We consider the polynomial of degree n of the form

$$f(x) = a_0xa_1x\dots a_{n-1}xa_n + \varphi(x), \tag{3.5.2.}$$

where x, a_0, $a_1,\dots,a_{n-1}$, $a_n \in \mathbb{H}(-1,-1)$, with $a_\ell \neq 0$ for $\ell \in \{0,1,\dots,n\}$ and $\varphi(x)$ is a sum of a finite number of monomials of the form $b_0xb_1x\dots b_{t-1}xb_t$ where $t < n$. From the above, it results that the equation $f(x) = 0$ has at least one root. Applying operator A^{-1} to this last equality, the equation $(A^{-1}f)(A^{-1}(x)) = 0$, with $x = x_0 + x_1e_1 + x_2e_2 + x_3e_3$, has at least one root in $\mathbb{H}(\gamma_1,\gamma_2)$. Therefore, we proved the following result:

Theorem 3.5.3. *In the generalized quaternion algebra* $\mathbb{H}(\gamma_1,\gamma_2)$, *any polynomial of the form* (3.5.2) *has at least one root.* □

In the following, we will use some ideas and notations from [Ch; 98]. Let $q = q_0 + q_1e_1 + q_2e_2 + q_3e_3 \in \mathbb{H}(\gamma_1,\gamma_2)$, $\gamma_1,\gamma_2 > 0$, $q_0,q_1,q_2,q_3 \in \mathbb{R}$ and $|\mathbf{n}(q)| = \sqrt{q_0^2 + \gamma_1q_1^2 + \gamma_2q_2^2 + \gamma_1\gamma_2q_3^2}$.Consider the sets

$$\mathcal{S}_G^3 = \{q \in \mathbb{H}(\gamma_1,\gamma_2), \gamma_1,\gamma_2 < 0 : \mathbf{n}(q) = 1\},$$
$$\mathcal{S}_G^2 = \{q \in \mathbb{H}(\gamma_1,\gamma_2), \gamma_1,\gamma_2 < 0 : q_0 = 0, \mathbf{n}(q) = 1\}.$$

Any $q \in \mathcal{S}_G^3$ can be expressed as $q = \cos\theta + \varepsilon\sin\theta$, where

$$\cos\theta = q_0, \quad \varepsilon = \frac{q_1e_1 + q_2e_2 + q_3e_3}{\sqrt{\gamma_1q_1^2 + \gamma_2q_2^2 + \gamma_1\gamma_2q_3^2}}.$$

Using Proposition 2 from [Ch; 98] and applying the operator A^{-1} we will find De Moivre's formula for $\mathbb{H}(\gamma_1,\gamma_2), \gamma_1,\gamma_2 < 0$.

Theorem 3.5.4. *Let* $q = \cos\theta + \varepsilon\sin\theta \in \mathcal{S}_G^3$, $\theta \in \mathbb{R}$. *Then* $q^n = \cos n\theta + \varepsilon\sin n\theta$, *for every integer* n.

Theorem 3.5.4 is the same with Theorem 7 from the paper [Ma, Ja; 13], obtained with another proof.□

Using Corollary 3 from [Ch; 98] and Theorem 3.5.2, we obtain the next statement.

Proposition 3.5.5. *i) In* $\mathbb{H}(\gamma_1,\gamma_2)$, $\gamma_1,\gamma_2<0$ *the equation* $x^n=1$ *whit* n *integer and* $n\geq 3$ *has infinity of roots, namely*

$$q=\cos\frac{2\pi}{n}+\varepsilon\sin\frac{2\pi}{n}\in\mathcal{S}_G^3,\ \varepsilon\in\mathcal{S}_G^2.$$

ii) In $\mathbb{H}(\gamma_1,\gamma_2)$, $\gamma_1,\gamma_2<0$ *the equation* $x^n=a$, $n\in\mathbb{N}$, $a\in\mathbb{R}$ *has infinity of roots, namely* $\sqrt[n]{a}\,q$, *where* $q=\cos\frac{2\pi}{n}+\varepsilon\sin\frac{2\pi}{n}\in\mathcal{S}_G^3$, *with* $\varepsilon\in\mathcal{S}_G^2$. *If* n *is even it is necessary that* $a>0$.□

In the following, we will generalize in a natural way De Moivre formula and Euler's formula for the division octonion algebra $\mathbb{O}(-1,-1,-1)$. For this, we will use some ideas and notations from [Ch; 98]. We consider the sets

$$\mathcal{S}^3=\{a\in\mathbb{O}(-1,-1,-1):\ \mathbf{n}(a)=1\},$$

$$\mathcal{S}_G^3=\{a\in\mathbb{O}(\alpha,\beta,\gamma):\ \mathbf{n}(a)=1\},$$

$$\mathcal{S}^2=\{a\in\mathbb{O}(-1,-1,-1):\ t(a)=0,\mathbf{n}(a)=1\}.$$

$$\mathcal{S}_G^2=\{a\in\mathbb{O}(-1,-1,-1):\ t(a)=0,\mathbf{n}(a)=1\}.$$

We remark that for all elements $a\in\mathcal{S}^2$, we have $a^2=-1$. Let $a\in\mathcal{S}^3, a=a_0+a_1f_1+a_2f_2+a_3f_3+a_4f_4+a_5f_5+a_6f_6+a_7f_7$. This element can be written under the form

$$a=\cos\lambda+w\sin\lambda,$$

where $\cos\lambda=a_0$ and

$$w=\frac{a_1f_1+a_2f_2+a_3f_3+a_4f_4+a_5f_5+a_6f_6+a_7f_7}{\sqrt{a_1^2+a_2^2+a_3^2+a_4^2+a_5^2+a_6^2+a_7^2}}=$$

$$=\frac{a_1f_1+a_2f_2+a_3f_3+a_4f_4+a_5f_5+a_6f_6+a_7f_7}{\sqrt{1-a_0^2}}.$$

Since $w^2=-1$, we obtain the following Euler's formula:

$$\begin{aligned}e^{\lambda w} &= \sum_{i=1}^{\infty}\frac{(\lambda w)^n}{n!}=\sum_{i=1}^{\infty}\frac{(-1)^n\lambda^{2n}}{(2n)!}+w\sum_{i=1}^{\infty}\frac{(-1)^{n-1}\lambda^{2n-1}}{(2n-1)!}=\\ &= \cos\lambda+w\sin\lambda.\end{aligned}$$

Proposition 3.5.3. *The cosinus function is constant for all elements in* $\mathcal{S}^2$.

Proof. Indeed, $\cos w = \sum\limits_{i=1}^{\infty} \frac{(-1)^n w^{2n}}{(2n)!} = \cos i.\square$

Proposition 3.5.4. For $w \in \mathcal{S}^2$, we have $(\cos\lambda_1 + w\sin\lambda_1)(\cos\lambda_2 + w\sin\lambda_2) = \cos(\lambda_1+\lambda_2) + w\sin(\lambda_1+\lambda_2)$.

Proof. By straightforward calculations $\square$

Proposition 3.5.5. (De Moivre formula for octonions) *With the above notations, we have that*

$$a^n = e^{n\lambda w} = (\cos\lambda + w\sin\lambda)^n = \cos n\lambda + w\sin n\lambda,$$

where $a \in \mathcal{S}^3$, $n \in \mathbb{Z}$ *and* $\lambda \in \mathbb{R}$.

Proof. For $n > 0$, by induction. We obtain

$$\begin{aligned} a^{n+1} &= (\cos\lambda + w\sin\lambda)^{n+1} = \\ &= (\cos\lambda + w\sin\lambda)^n (\cos\lambda + w\sin\lambda) = \\ &= (\cos n\lambda + w\sin n\lambda)(\cos\lambda + w\sin\lambda) = \\ &= \cos(n+1)\lambda + w\sin(n+1)\lambda. \end{aligned}$$

Since $a^{-1} = \cos\lambda - w\sin\lambda = \cos(-\lambda) + w\sin(-\lambda)$, it results the asked formula for all $n \in \mathbb{Z}.\square$

Remark 3.5.6. We know that any polynomial of degree n with coefficients in a field K has at most n roots in K. If we consider the coefficients in $\mathbb{O}(-1,-1,-1)$, there is a kind of a fundamental theorem of algebra: If a polynomial has only one term of the higher degree, then it has at least one root in $\mathbb{O}(-1,-1,-1)$ (see [Ch; 98], Theorem 65).

Theorem 3.5.7. *Equation* $x^n = a$, *where* $a \in \mathbb{O}(-1,-1,-1) \setminus \mathbb{R}$, *has* n *roots.*

Proof. The octonion a can be written under the form $a = \sqrt{\mathbf{n}(a)}\frac{a}{\sqrt{\mathbf{n}(a)}}$. The octonion $b = \frac{a}{\sqrt{\mathbf{n}(a)}}$ is in $\mathcal{S}^3$, then we can find the elements $w \in \mathcal{S}^2$ and $\lambda \in \mathbb{R}$ such that $b = \cos\lambda + w\sin\lambda$. From Proposition 3.5.5, we have that

the solutions of the above equation are $x_r = \sqrt[n]{Q}\left(\cos\frac{\lambda+2r\pi}{n} + w\sin\frac{\lambda+2r\pi}{n}\right)$, where $Q = \sqrt{\mathbf{n}(a)}$ and $r \in \{0, 1, ..., n-1\}$.□

Corollary 3.5.8. *If $a \in \mathbb{R}$, therefore the equation $x^n = a$ has an infinity of roots.*

Proof. Indeed, if $a \in \mathbb{R}$, we can write $a = a \cdot 1 = a(\cos 2\pi + w\sin 2\pi)$, where $w \in \mathcal{S}^2$ is an arbitrary element. □

In the following, we will consider the generalized real octonion algebra $\mathbb{O}(\alpha, \beta, \gamma)$ and the algebras $\mathbb{O}(-1, -1, -1)$ and $\mathbb{O}(1, 1, -1)$. Let $\{1, f_1, \ldots, f_7\}$ be a basis in $\mathbb{O}(\alpha, \beta, \gamma)$, and $\{1, \widetilde{f}_1, \ldots, \widetilde{f}_7\}$ be the canonical basis in $\mathbb{O}(-1, -1, -1)$ and $\{1, \widehat{f}_1, \ldots, \widehat{f}_7\}$ be the canonical basis in $\mathbb{O}(1, 1, -1)$.

We prove that the algebra $\mathbb{O}(\alpha, \beta, \gamma)$ with $\alpha, \beta, \gamma \in \mathbb{R} \setminus \{0\}$ is isomorphic with algebra $\mathbb{O}(-1, -1, -1)$ or $\mathbb{O}(1, 1, -1)$ and indicate the formulae to pass from one basis to another basis. Thus, if $\alpha, \beta, \gamma < 0$ then the real octonion algebra $\mathbb{O}(\alpha, \beta, \gamma)$ is isomorphic with algebra $\mathbb{O}(sign\alpha, sign\beta, sign\gamma)$ and this isomorphism is given by the relations:

$$\begin{aligned} A_k: \quad & f_1 \mapsto \widetilde{f}_1\sqrt{(sign\alpha)\alpha}, \quad f_2 \mapsto \widetilde{f}_2\sqrt{(sign\beta)\beta}, \quad f_3 \mapsto \widetilde{f}_3\sqrt{\alpha\beta}, \\ & f_4 \mapsto \widetilde{f}_4\sqrt{(sign\gamma)\gamma}, \quad f_5 \mapsto \widetilde{f}_5\sqrt{\alpha\gamma}, \quad f_6 \mapsto \widetilde{f}_6\sqrt{\beta\gamma}, \quad f_7 \mapsto \widetilde{f}_7\sqrt{M\alpha\beta\gamma}, \end{aligned}$$

where $M = (sign\alpha)(sign\beta)(sign\gamma)$.

We obtain 8 operators. It is easy to prove that the operators $A_k,\ k = \overline{1,8}$ is additive and multiplicative. The following statement can be proved completely analogous as Proposition 3.5.1.

Proposition 3.5.9. *The operators $A_k,\ k = \overline{1,8}$ are continuous and have norm* 1.□

Let $x = x_0 + \sum_{k=1}^{7} x_k f_k \in \mathbb{O}(\alpha, \beta, \gamma)$ and let $g : \mathbb{O}(\alpha, \beta, \gamma) \to \mathbb{O}(\alpha, \beta, \gamma)$ be a continuous function of the form $g(x) = g_0(x_0, \ldots, x_7) + \sum_{k=1}^{7} g_k(x_0, \ldots, x_7) f_k$. Let L be one of the operators $A_k,\ k = \overline{1,8}$, depending on the signs of α, β and γ. We define the operator $\mathfrak{L}$ by the rule:

$$\mathfrak{L}g := f_0 + \sum_{k=1}^{7} g_k\, L(f_k).$$

The operator $\mathfrak{L}$ for any continuous function g, taking values in $\mathbb{O}(\alpha,\beta,\gamma)$, maps it in the continuous function $\mathfrak{L}g$, taking values in $\mathbb{O}(-1,-1,-1)$ or $\mathbb{O}(1,1,-1)$,

The following statement can be analogously proved as in Theorem 3.5.2.

Theorem 3.5.10. *Let $x^0 \in \mathbb{O}(\alpha,\beta,\gamma)$, be a root of the equation $g(x) = 0$ in $\mathbb{O}(\alpha,\beta,\gamma)$. Then $L(x^0)$ is a root of the equation $\mathfrak{L}g\big(L(x)\big) = 0$ in $\mathbb{O}(-1,-1,-1)$ or $\mathbb{O}(1,1,-1)$, depending on the signs of α,β, and γ. The converse is also true.* □

Thus, the study of algebraic equations in an arbitrary algebra $\mathbb{O}(\alpha,\beta,\gamma)$ with $\alpha,\beta,\gamma \in \mathbb{R}\backslash\{0\}$ was reduced to study of the corresponding algebraic equation in one of the following two algebras: division octonion algebra $\mathbb{O}(-1,-1,-1)$ or algebra $\mathbb{O}(1,1,-1)$.

Using the above notations, we can prove the following theorem.

Theorem 3.5.11. *Equation $x^n = a$, where $a \in \mathbb{O}(\alpha,\beta,\gamma) \setminus \mathbb{R}, \alpha,\beta,\gamma < 0$, has n roots.*

Proof. The octonion $b = \frac{a}{\sqrt{\mathbf{n}(a)}}$ is in $\mathcal{S}_G^3$, then there are $w \in \mathcal{S}_G^2$, $w = A_1^{-1}(\widetilde{w}), \widetilde{w} \in \mathcal{S}^2$ and $\lambda \in \mathbb{R}$ such that $b = \cos\lambda + \widetilde{w}\sin\lambda$. From Proposition 3.5.2, we have that the solutions of the above equation are $x_r = A_1^{-1}(\widetilde{x}_r) = \sqrt[2n]{\mathbf{n}(a)}\left(\cos\frac{\lambda+2r\pi}{n} + \widetilde{w}\sin\frac{\lambda+2r\pi}{n}\right)$, where $r \in \{0,1,\ldots,n-1\}$ and $\widetilde{x}_r$ is a solution of the equation $\widetilde{x}^n = \widetilde{a}$ in $\mathbb{O}(-1,-1,-1)$.□

Remark 3.5.12. Using the operator A_1^{-1}, the rotation of the octonion $x \in \mathbb{O}(\alpha,\beta,\gamma)$ on the angle λ around the unit vector $w \in \mathcal{S}_G^2$ is defined by the formula

$$x^r = \overline{u}xu,$$

where $u \in \mathcal{S}_G^3, w \in \mathcal{S}_G^2$, $u = \cos\frac{\lambda}{2} + w\sin\frac{\lambda}{2}$ and $\overline{u} = \cos\frac{\lambda}{2} - w\sin\frac{\lambda}{2}$.

By straightforward calculations, it results that the rotation does not transform the octonion-scalar part, but the octonion-vector part $\overrightarrow{x}$ is rotated on the angle λ around w.

Example 3.5.13. 1) Let $a \in \mathcal{S}^3$,
$a = \frac{\sqrt{2}}{2} + \frac{1}{\sqrt{14}}\widetilde{f}_1 + \frac{1}{\sqrt{14}}\widetilde{f}_2 + \frac{1}{\sqrt{14}}\widetilde{f}_3 + \frac{1}{\sqrt{14}}\widetilde{f}_4 + \frac{1}{\sqrt{14}}\widetilde{f}_5 + \frac{1}{\sqrt{14}}\widetilde{f}_6 + \frac{1}{\sqrt{14}}\widetilde{f}_7$, we have $\cos\lambda = \frac{\sqrt{2}}{2}, \sin\lambda = \frac{\sqrt{2}}{2}$. It results that $a = \cos\frac{\pi}{4} + v\sin\frac{\pi}{4}$, where $v =$

$\frac{1}{\sqrt{7}}(\widetilde{f}_1+\widetilde{f}_2+\widetilde{f}_3+\widetilde{f}_4+\widetilde{f}_5+\widetilde{f}_6+\widetilde{f}_7)$. The vector a corresponds to the rotation of the space $\mathbb{R}^8$on the angle $\frac{\pi}{2}$ around the vector $v=\left(\frac{1}{\sqrt{7}},\frac{1}{\sqrt{7}},\ldots,\frac{1}{\sqrt{7}}\right)\in\mathbb{R}^7$ written in the canonical basis.

2) In the algebra $\mathbb{O}(2,4,7)$, for the above element $a\in\mathcal{S}^3$, we have $b{=}A^{-1}(a){=}\frac{\sqrt{2}}{2}+\frac{1}{2\sqrt{7}}f_1+\frac{1}{2\sqrt{14}}f_2+\frac{1}{7\sqrt{2}}f_3+\frac{1}{4\sqrt{7}}f_4+\frac{1}{14}f_5+\frac{1}{14\sqrt{2}}f_6+\frac{1}{28}f_7\in\mathcal{S}_G^3$ and corresponds to the rotation of the space $\mathbb{R}^8$on the angle $\frac{\pi}{2}$ around the vector $v=\left(\frac{1}{2\sqrt{7}},\frac{1}{2\sqrt{14}},\frac{1}{7\sqrt{2}},\frac{1}{4\sqrt{7}},\frac{1}{14},\frac{1}{14\sqrt{2}},\frac{1}{28}\right)\in\mathbb{R}^7$written in the basis $\{f_1,\ldots,f_7\}$.

In this case when $\alpha=\beta=1,\gamma=-1$, the octonion algebra $\mathbb{O}(1,1,-1)$ is not a division algebra (it is a split algebra). The norm of an octonion $a\in\mathbb{O}(1,1,-1)$, $a=a_0+a_1f_1+a_2f_2+a_3f_3+a_4f_4+a_5f_5+a_6f_6+a_7f_7$, in this situation, can be positive, zero or negative. In the following, we used definitions and propositions obtained for the split quaternions as in [Oz; 09] to generalized them to similar results for the split octonions. A split octonion is called *spacelike, timelike or lightlike* if $n(a)<0, n(a)>0$ or $n(a)=0$. If $n(a)=1$, then a is called *the unit split octonion.*

Spacelike octonions

Let $a\in\mathbb{O}(1,1,-1)$ such that $\mathbf{n}(a)=-1$, be a so called spacelike octonion. For the octonion $w=\frac{a_1f_1+a_2f_2+a_3f_3+a_4f_4+a_5f_5+a_6f_6+a_7f_7}{\sqrt{1+a_0^2}}$, we have $\mathbf{n}(w)=-1$ and $t(w)=0$, therefore $w^2=1$. Denoting $\sinh\lambda=a_0$ and $\cosh\lambda=\sqrt{1+a_0^2},\lambda\in\mathbb{R}$, it results:

$$a=e^{\lambda w}=\sinh\lambda+w\cosh\lambda.$$

If $a\in\mathbb{O}(1,1,-1)$ with $n(a)<0$, we have $a=\sqrt{|n(a)|}(\sinh\lambda+w\cosh\lambda)$.

Proposition 3.5.14. *We have that* $a^n=(\sqrt{|\mathbf{n}(a)|})^n(\sinh\lambda+w\cosh\lambda)$ *for* n *odd and* $a^n=(\sqrt{|\mathbf{n}(a)|})^n(\cosh\lambda+w\sinh\lambda)$ *for* n *even.* □

Timelike octonions

Let $a\in\mathbb{O}(1,1,-1)$ such that $\mathbf{n}(a)=1$, be a so called timelike octonion. If $1-a_0^2>0$, for the octonion $w=\frac{a_1f_1+a_2f_2+a_3f_3+a_4f_4+a_5f_5+a_6f_6+a_7f_7}{\sqrt{1-a_0^2}}$, we have $\mathbf{n}(w)=1$ and $t(w)=0$, therefore $w^2=-1$ Denoting $\cos\lambda=a_0$ and $\sin\lambda=\sqrt{1-a_0^2},\lambda\in\mathbb{R}$, it results:

Proposition 3.5.15. *With the above notations, we have the Euler's formula:*

$$a=e^{\lambda w}=\cos\lambda+w\sin\lambda.$$

Proof. Indeed, $e^{\lambda w}=\sum\limits_{i=1}^{\infty}\frac{(\lambda w)^n}{n!}=\sum\limits_{i=1}^{\infty}\frac{(-1)^n\lambda^{2n}}{(2n)!}+w\sum\limits_{i=1}^{\infty}\frac{(-1)^{n-1}\lambda^{2n-1}}{(2n-1)!}=\cos\lambda+w\sin\lambda$.□

If $a\in\mathbb{O}(1,1,-1)$ with $\mathbf{n}(a)>0$, it results $a=\sqrt{\mathbf{n}(a)}(\cos\lambda+w\sin\lambda)$.□

Proposition 3.5.16. *We have that* $a^n=(\sqrt{\mathbf{n}(a)})^n(\cos n\lambda+w\sin n\lambda)$.□

Proposition 3.5.17.

1)If $a\in\mathbb{O}(1,1,-1)$, *it results* $a^n=(\sqrt{\mathbf{n}(a)})^n(\cos n\lambda+w\sin n\lambda)$.

2) The equation $x^n=a$ *has* n *roots:* $\sqrt[2n]{|\mathbf{n}(a)|}\left(\cosh\frac{\lambda}{n}+w\sinh\frac{\lambda}{n}\right)$.□

If $1-a_0^2<0$, we have $w=\frac{a_1f_1+a_2f_2+a_3f_3+a_4f_4+a_5f_5+a_6f_6+a_7f_7}{\sqrt{a_0^2-1}}$, with $\mathbf{n}(w)=-1$ and $t(w)=0$, therefore $w^2=1$. Denoting $\cosh\lambda=a_0$ and $\sinh\lambda=\sqrt{a_0^2-1}$, $\lambda\in\mathbb{R}$, we have the following result:

Proposition 3.5.18. *With the above notations, we have Euler's formula:*

$$a=e^{\lambda w}=\cosh\lambda+w\sinh\lambda.$$

Proof. Indeed, $e^{\lambda w}=\sum\limits_{n=0}^{\infty}\frac{(\lambda w)^n}{n!}=\sum\limits_{n=0}^{\infty}\frac{\lambda^{2n}}{(2n)!}+w\sum\limits_{n=0}^{\infty}\frac{\lambda^{2n+1}}{(2n+1)!}=\cosh\lambda+w\sinh\lambda$.□

If $a\in a\in\mathbb{O}(1,1,-1)$ with $\mathbf{n}(a)<0$, it results $a=\sqrt{|\mathbf{n}(a)|}(\cosh\lambda+w\sinh\lambda)$.□

Proposition 3.5.19.

1) If $a\in\mathbb{O}(1,1,-1)$, *then* $a^n=(\sqrt{|\mathbf{n}(a)|})^n(\cosh n\lambda+w\sinh n\lambda)$.

2) The equation $x^n=a$ *has only one root:* $\sqrt[2n]{|\mathbf{n}(a)|}\left(\cosh\frac{\lambda}{n}+w\sinh\frac{\lambda}{n}\right)$.□

Remark 3.5.20. Using the above technique, De Moivre's formula and Euler's formula can be easy proved for the octonion algebra $\mathbb{O}(\alpha,\beta,\gamma)$, with $\alpha,\beta,\gamma\in\mathbb{R}\setminus\{0\}$ such that $\mathbb{O}(\alpha,\beta,\gamma)$ is split. Thus, the study of algebraic equations in an arbitrary algebra $\mathbb{O}(\alpha,\beta,\gamma)$ with $\alpha,\beta,\gamma\in\mathbb{R}\setminus\{0\}$ was reduced to study of the corresponding algebraic equation in one of the following two algebras: division octonion algebra $\mathbb{O}(-1,-1,-1)$ or algebra $\mathbb{O}(1,1,-1)$.

3.6. Fibonacci elements in Quaternion and Octonion algebras

The results presented in this section were obtained especially in the papers [Fl, Sh; 13] and [Fl, Sa; 15]. The Fibonacci numbers was introduced by *Leonardo of Pisa (1170-1240)* in his book *Liber abbaci*, book published in 1202 AD (see [Kos; 01], p. 1, 3). These numbers was used as a model for investigate the growth of rabbit populations (see [Dr, Gi, Gr, Wa; 03]). The nth term of these numbers is given by the formula:

$$f_n = f_{n-1} + f_{n-2},\ n \geq 2,$$

where $f_0 = 0, f_1 = 1$.

The following sequence

$$l_0 = 2; f_1 = 1; l_n = l_{n-1} + l_{n-2},\ n \geq 2$$

is called the Lucas number. Some properties of these numbers are known.

Proposition 3.6.1. *Let $(f_n)_{n\geq 0}$ be the Fibonacci sequence and let $(l_n)_{n\geq 0}$ be the Lucas sequence. Therefore the following properties hold:*
i) $f_n^2 + f_{n+1}^2 = f_{2n+1}, \forall\ n \in \mathbb{N}$;
ii) $f_{n+1}^2 - f_{n-1}^2 = f_{2n}, \forall\ n \in \mathbb{N}^*$;
ix) $f_m l_{m+p} = f_{2m+p} + (-1)^{m+1} f_p, \forall\ m, p \in \mathbb{N}$;
x) $f_{m+p} l_m = f_{2m+p} + (-1)^m f_p, \forall\ m, p \in \mathbb{N}$;
xi) $f_m f_{m+p} = \frac{1}{5}\left(l_{2m+p} + (-1)^{m+1} l_p\right), \forall\ m, p \in \mathbb{N}$;
xii) $l_m l_p + 5 f_m f_p = 2 l_{m+p}, \forall\ m, p \in \mathbb{N}$.□

Let $\mathbb{H}(\beta_1, \beta_2)$ be the generalized real quaternion algebra.

We denote by $\boldsymbol{t}(a)$ and $\boldsymbol{n}(a)$ the trace and the norm of a real quaternion a.

In [Ho; 61], the author generalized Fibonacci numbers and gave many properties of them: $h_n = h_{n-1} + h_{n-2},\ \ n \geq 2$, where $h_0 = p, h_1 = q$, with p, q being arbitrary integers. In the same paper [Ho; 61], relation (7), the following relation between Fibonacci numbers and generalized Fibonacci numbers was obtained:

$$h_{n+1} = p f_n + q f_{n+1}. \tag{3.6.1.}$$

The same author, in [Ho; 63], defined and studied Fibonacci quaternions and generalized Fibonacci quaternions in the real division quaternion algebra and found a lot of properties of them. For the generalized real quaternion algebra,

the Fibonacci quaternions and generalized Fibonacci quaternions are defined in the same way:

$$F_n = f_n 1 + f_{n+1} e_2 + f_{n+2} e_3 + f_{n+3} e_4,$$

for the nth Fibonacci quaternions, and

$$H_n = h_n 1 + h_{n+1} e_2 + h_{n+2} e_3 + h_{n+3} e_4,$$

for the nth generalized Fibonacci quaternions.

In the same paper, we find the norm formula for the nth Fibonacci quaternions:

$$\boldsymbol{n}(F_n) = F_n \overline{F}_n = 3 f_{2n+3}, \tag{1.2}$$

where $\overline{F}_n = f_n \cdot 1 - f_{n+1} e_2 - f_{n+2} e_3 - f_{n+3} e_4$ is the conjugate of the F_n in the algebra $\mathbb{H}$. After that, many authors studied Fibonacci and generalized Fibonacci quaternions in the real division quaternion algebra giving more and surprising new properties (for example, see [Sw; 73], [Sa-Mu; 82] and [Ha; 12]).

M. N. S. Swamy, in [Sw; 73], formula (17), obtained the norm formula for the nth generalized Fibonacci quaternions:

$$\begin{aligned} \boldsymbol{n}(H_n) &= H_n \overline{H}_n = \\ &= 3(2pq - p^2) f_{2n+2} + (p^2 + q^2) f_{2n+3}, \end{aligned}$$

where $\overline{H}_n = h_n \cdot 1 - h_{n+1} e_2 - h_{n+2} e_3 - h_{n+3} e_4$ is the conjugate of the H_n in the algebra $\mathbb{H}$.

Similar to A. F. Horadam, we define the Fibonacci-Narayana quaternions as

$$U_n = u_n 1 + u_{n+1} e_2 + u_{n+2} e_3 + u_{n+3} e_4,$$

where u_n are the nth Fibonacci-Narayana number.

As in the case of Fibonacci numbers, numerous results between Fibonacci generalized numbers can be deduced. In the following, we will study some properties of the generalized Fibonacci quaternions in the generalized real quaternion algebra $\mathbb{H}(\beta_1, \beta_2)$. Let $F_n = f_n 1 + f_{n+1} e_2 + f_{n+2} e_3 + f_{n+3} e_4$ be the nth Fibonacci quaternion and $H_n = h_n 1 + h_{n+1} e_2 + h_{n+2} e_3 + h_{n+3} e_4$ be the nth generalized Fibonacci quaternion. A first question which can arise

is what algebraic structure have these elements? The answer will be found in the below theorem, denoting first a nth generalized Fibonacci number and a nth generalized Fibonacci element with $h_n^{p,q}$, respectively $H_n^{p,q}$. In this way, we emphasis the starting integers p and q.

Theorem 3.6.2. *The set* $\mathcal{H}_n = \{H_n^{p,q} \ / \ p,q \in \mathbb{Z}\} \cup \{0\}$ *is a* $\mathbb{Z}-$*module.*

Proof. Indeed, $aH_n^{p,q} + bH_n^{p',q'} = H_n^{ap+bp',aq+bq'} \in \mathcal{H}_n$, where $a,b,p,q,p',q' \in \mathbb{Z}$.□

Proposition 3.6.3. *i) For the Fibonacci quaternion elements, we have* $\sum_{m=1}^{n} (-1)^{m+1} F_m = (-1)^{n+1} F_{n-1} + 1 + e_3 + e_4$.
ii) For the generalized Fibonacci quaternion elements, the following relation is true
$\sum_{m=1}^{n} (-1)^{m+1} H_m^{p,q} = (-1)^{n+1} H_{n-1}^{p,q} - p+q+pe_2+qe_3+pe_4+qe_4$.□

From the above proposition, we can remark that all identities valid for the Fibonacci quaternions can be easy adapted in an approximative similar expression for the generalized Fibonacci quaternions.

In the following, we will compute the norm of a Fibonacci quaternion and of a generalized Fibonacci quaternion in the algebra $\mathbb{H}(\beta_1, \beta_2)$.

Let $F_n = f_n 1 + f_{n+1}e_2 + f_{n+2}e_3 + f_{n+3}e_4$ be the nth Fibonacci quaternion, then its norm is

$$\boldsymbol{n}(F_n) = f_n^2 - \beta_1 f_{n+1}^2 - \beta_2 f_{n+2}^2 + \beta_1\beta_2 f_{n+3}^2.$$

Using recurrence of Fibonacci numbers, we have

Proposition 3.6.4. *The norm of the* nth *Fibonacci quaternion* F_n *in a generalized quaternion algebra is*

$$\boldsymbol{n}(F_n) = h_{2n+2}^{1-2\beta_2,-3\beta_2} + (-\beta_1 - 1) h_{2n+3}^{1-2\beta_2,-\beta_2} - 2(-\beta_1 - 1)(1-\beta_2) f_n f_{n+1}. \qquad (3.6.2.)$$

□

Let $H_n = h_n 1 + h_{n+1}e_2 + h_{n+2}e_3 + h_{n+3}e_4$ be the nth generalized Fibonacci quaternion. The norm is given in the following

Proposition 3.6.5. *The norm of the* nth *generalized Fibonacci quaternion* $H_n^{p,q}$ *in a generalized quaternion algebra is*

$$\boldsymbol{n}\left(H_n^{p,q}\right)=p^2h_{2n}^{1-2\beta_2,-3\beta_2}+p^2(-\beta_1\text{-}1)h_{2n+1}^{1-2\beta_2,-\beta_2}+q^2h_{2n+2}^{1-2\beta_2,-3\beta_2}+q^2(-\beta_1\text{-}1)h_{2n+3}^{1-2\beta_2,-\beta_2}\text{-}$$

$$-2p\left(-\beta_1-1\right)\left(-p\beta_2+p+q\right)f_{n-1}f_n-2q^2(-\beta_1-1)\left(1\text{-}\beta_2\right)f_nf_{n+1}+$$

$$+h_{2n+1}^{-2pq\beta_1,2pq\beta_1\beta_2}+2pq\beta_1\beta_2(f_{2n}+f_{2n+3})-2pq\beta_2\left(1+\beta_1\right)f_{n+1}f_{n+2}. \quad (3.6.3.)$$

□

It is known that the expression for the nth term of a Fibonacci element is

$$f_n=\frac{1}{\sqrt{5}}[\alpha^n-\beta^n]=\frac{\alpha^n}{\sqrt{5}}[1-\frac{\beta^n}{\alpha^n}], \quad (3.6.4.)$$

where $\alpha=\frac{1+\sqrt{5}}{2}$ and $\beta=\frac{1-\sqrt{5}}{2}$.

From the above, we can compute the following

$$\lim_{n\to\infty}\boldsymbol{n}\left(F_n\right)=\lim_{n\to\infty}(f_n^2-\beta_1f_{n+1}^2-\beta_2f_{n+2}^2+\beta_1\beta_2f_{n+3}^2)=$$

$$=\lim_{n\to\infty}(\frac{\alpha^{2n}}{5}\text{-}\beta_1\frac{\alpha^{2n+2}}{5}\text{-}\beta_2\frac{\alpha^{2n+4}}{5}+\beta_1\beta_2\frac{\alpha^{2n+6}}{5})=$$

$$=sgnE(\beta_1,\beta_2)\cdot\infty$$

where
$E(\beta_1,\beta_2)=(\frac{1}{5}-\frac{\beta_1}{5}\alpha^2-\frac{\beta_2}{5}\alpha^4+\frac{\beta_1\beta_2}{5}\alpha^6)=$
$=\frac{1}{5}\left(1-\beta_1\left(\alpha+1\right)-\beta_2\left(3\alpha+2\right)+\beta_1\beta_2\left(8\alpha+5\right)\right)=$
$=\frac{1}{5}[1-\beta_1-2\beta_2+5\beta_1\beta_2+\alpha\left(-\beta_1-3\beta_2+8\beta_1\beta_2\right)]$, since $\alpha^2=\alpha+1$.

If $E(\beta_1,\beta_2)>0$, there exist a number $n_1\in\mathbb{N}$ such that for all $n\geq n_1$ we have

$$h_{2n+2}^{1-2\beta_2,-3\beta_2}+(-\beta_1-1)h_{2n+3}^{1-2\beta_2,-\beta_2}-2(-\beta_1-1)\left(1-\beta_2\right)f_nf_{n+1}>0.$$

In the same way, if $E(\beta_1,\beta_2)<0$, there exist a number $n_2\in\mathbb{N}$ such that for all $n\geq n_2$ we have

$$h_{2n+2}^{1-2\beta_2,-3\beta_2}+(-\beta_1-1)h_{2n+3}^{1-2\beta_2,-\beta_2}-2(-\beta_1-1)\left(1-\beta_2\right)f_nf_{n+1}<0.$$

Therefore for all $\beta_1, \beta_2 \in \mathbb{R}$ with $E(\beta_1, \beta_2) \neq 0$, in the algebra $\mathbb{H}(\beta_1, \beta_2)$ there is a natural number $n_0 = \max\{n_1, n_2\}$ such that $\boldsymbol{n}(F_n) \neq 0$, hence F_n is an invertible element for all $n \geq n_0$. Using the same arguments, we can compute

$$\lim_{n\to\infty}\left(\boldsymbol{n}\left(H_n^{p,q}\right)\right) = \lim_{n\to\infty}\left(h_n^2 - \beta_1 h_{n+1}^2 - \beta_2 h_{n+2}^2 + \beta_1\beta_2 h_{n+3}^2\right) =$$

$$= \lim_{n\to\infty}[\left(pf_{n-1}+qf_n\right)^2 - \beta_1\left(pf_n+qf_{n+1}\right)^2 - \beta_2\left(pf_{n+1}+qf_{n+2}\right)^2 +$$

$$+\beta_1\beta_2\left(pf_{n+2}+qf_{n+3}\right)^2] =$$

$$= sgnE'(\beta_1, \beta_2)\cdot\infty$$

where
$E'(\beta_1, \beta_2) = \frac{1}{5}[(p+\alpha q)^2 - \beta_1\left(p\alpha + \alpha^2 q\right)^2 - \beta_2\left(p\alpha^2 + \alpha^3 q\right)^2 +$
$+\beta_1\beta_2\left(p\alpha^3 + \alpha^4 q\right)^2] =$
$= \frac{1}{5}(p+\alpha q)^2[1 - \beta_1\alpha^2 - \beta_2\alpha^4 + \beta_1\beta_2\alpha^6] =$
$= \frac{1}{5}(p+\alpha q)^2 E(\beta_1, \beta_2).$

Therefore for all $\beta_1, \beta_2 \in \mathbb{R}$ with $E'(\beta_1, \beta_2) \neq 0$ in the algebra $\mathbb{H}(\beta_1, \beta_2)$ there exist a natural number n_0' such that $\boldsymbol{n}\left(H_n^{p,q}\right) \neq 0$, hence $H_n^{p,q}$ is an invertible element for all $n \geq n_0'$.

Now, we proved

Proposition 3.6.6. *For all $\beta_1, \beta_2 \in \mathbb{R}$ with $E'(\beta_1, \beta_2) \neq 0$, there exist a natural number n' such that for all $n \geq n'$ Fibonacci elements F_n and generalized Fibonacci elements $H_n^{p,q}$ are invertible elements in the algebra $\mathbb{H}(\beta_1, \beta_2)$.*$\square$

Remark 3.6.7. Algebra $\mathbb{H}(\beta_1, \beta_2)$ is not always a division algebra, and sometimes can be difficult to find an example of invertible element. Above Theorem provides us infinite sets of invertible elements in this algebra, namely Fibonacci elements and generalized Fibonacci elements.

Let n be an arbitrary positive integer and p, q be two arbitrary integers. The sequence g_n $(n \geq 1)$, where

$$g_{n+1} = pf_n + ql_{n+1},\ n \geq 0$$

is called *the generalized Fibonacci-Lucas numbers.*
To emphasize the integer p and q, in the following, we will use the notation $g_n^{p,q}$ instead of g_n.

Let $\mathbb{H}_{\mathbb{Q}}(\alpha, \beta)$ be the generalized quaternion algebra over the rational field. We define the *n-th generalized Fibonacci-Lucas quaternion* to be the element of the form

$$G_n^{p,q} = g_n^{p,q} 1 + g_{n+1}^{p,q} i + g_{n+2}^{p,q} j + g_{n+3}^{p,q} k,$$

where $i^2 = \alpha, j^2 = \beta$, $k = ij = -ji$.

In the following proposition, for $\alpha = -1$ and $\beta = p$, we compute the norm for the n-th generalized Fibonacci-Lucas quaternions.

Let A be a Noetherian integral domain with the field of the fractions K and let $\mathbb{H}_K(\alpha, \beta)$ be the generalized quaternion algebra. We recall that $\mathcal{O}$ is an order in $\mathbb{H}_K(\alpha, \beta)$ if $\mathcal{O} \subseteq \mathbb{H}_K(\alpha, \beta)$ and it is a finitely generated $A-$ submodule of $\mathbb{H}_K(\alpha, \beta)$ which is also a subring of $\mathbb{H}_K(\alpha, \beta)$ (see [Vo; 14]).
In the following, we will built an order of a quaternion algebras using the generalized Fibonacci-Lucas quaternions. Also we will prove that Fibonacci-Lucas quaternions can have an algebra structure over $\mathbb{Q}$. For this, we make the following remarks.

Remark 3.6.8. [Fl, Sa; 15] *Let n be an arbitrary positive integer and p, q be two arbitrary integers. Let $(g_n^{p,q})_{n\geq 1}$ be the generalized Fibonacci-Lucas numbers. Then*

$$pf_{n+1} + ql_n = g_n^{p,q} + g_{n+1}^{p,0}, \forall\ n \in \mathbb{N}^*.$$

Proof.

$$pf_{n+1} + ql_n = pf_{n-1} + ql_n + pf_n = g_n^{p,q} + pf_n = g_n^{p,q} + g_{n+1}^{p,o}.$$

□

Remark 3.6.9. [Fl, Sa; 15] *Let n be an arbitrary positive integer and p, q be two arbitrary integers. Let $(g_n^{p,q})_{n\geq 1}$ be the generalized Fibonacci-Lucas numbers and $(G_n^{p,q})_{n\geq 1}$ be the generalized Fibonacci-Lucas quaternion elements. Then:*

$$G_n^{p,q} = 0 \text{ if and only if } p = q = 0.$$

Proof. " $\Leftarrow$" It is trivial.
" $\Rightarrow$" If $G_n^{p,q} = 0$, since $\{1, i, j, k\}$ is a basis in $\mathbb{H}_{\mathbb{Q}}(\alpha, \beta)$, we obtain that $g_n^{p,q} = g_{n+1}^{p,q} = g_{n+2}^{p,q} = g_{n+3}^{p,q} = 0$. It results $g_{n-1}^{p,q} = g_{n+1}^{p,q} - g_n^{p,q} = 0$, ..., $g_2^{p,q} = 0$, $g_1^{p,q} = 0$. But $g_1^{p,q} = pf_0 + ql_1 = 2q$, therefore $q = 0$. From $g_2^{p,q} = 0$, we obtain $p = 0$.□

Theorem 3.6.10. [Fl, Sa; 15] *Let M be the set*

$$M = \left\{ \sum_{i=1}^{n} 5G_{n_i}^{p_i,q_i} | n \in \mathbb{N}^*, p_i, q_i \in \mathbb{Z}, (\forall) i = \overline{1,n} \right\} \cup \{1\}.$$

1) The set M has a ring structure with quaternions addition and multiplication.
2) The set M is an order of the quaternion algebra $\mathbb{H}_{\mathbb{Q}}(\alpha, \beta)$.
3) The set $M' = \left\{ \sum_{i=1}^{n} 5G_{n_i}^{p_i',q_i'} | n \in \mathbb{N}^*, p_i', q_i' \in \mathbb{Q}, (\forall) i = \overline{1,n} \right\} \cup \{1\}$ is a $\mathbb{Q}-$algebra.

Proof. 2) First, we remark that $0 \in M$.
Now we prove that M *is a* $\mathbb{Z}-$ submodule of $\mathbb{H}_{\mathbb{Q}}(\alpha, \beta)$.
Let $n, m \in \mathbb{N}^*$, $a, b, p, q, p', q' \in \mathbb{Z}$. It is easy to prove that

$$ag_n^{p,q} + bg_m^{p',q'} = g_n^{ap,aq} + g_m^{bp',bq'}.$$

This implies that

$$aG_n^{p,q} + bG_m^{p',q'} = G_n^{ap,aq} + G_m^{bp',bq'}.$$

From here, we get immediately that M *is a* $\mathbb{Z}-$ submodule of the quaternion algebra $\mathbb{H}_{\mathbb{Q}}(\alpha, \beta)$. Since $\{1, i, j, k\}$ is a basis for this submodule, it results that M is a free $\mathbb{Z}-$ module of rank 4.
Now, we prove that M is a subring of $\mathbb{H}_{\mathbb{Q}}(\alpha, \beta)$. It is enough to show that $5G_n^{p,q} \cdot 5G_m^{p',q'} \in M$. For this, if $m < n$, we calculate

$$5g_n^{p,q} \cdot 5g_m^{p',q'} = 5(pf_{n-1} + ql_n) \cdot 5\left(p'f_{m-1} + q'l_m\right) =$$

$$= 25pp'f_{n-1}f_{m-1} + 25pq'f_{n-1}l_m + 25p'qf_{m-1}l_n + 25qq'l_nl_m \qquad (3.2).$$

Using some previous results and above equality, we obtain:

$$5g_n^{p,q} \cdot 5g_m^{p',q'} = 5pp'\left[l_{m+n-2} + (-1)^m \cdot l_{n-m}\right] + 25pq'\left[f_{m+n-1} + (-1)^m \cdot f_{n-m-1}\right] +$$

$$+25p^{'}q\left[f_{m+n-1}+(-1)^{m}\cdot f_{n-m+1}\right]+25qq^{'}\left[l_{m+n}+(-1)^{m}\cdot l_{n-m}\right]=$$

$$=5\left(pp^{'}l_{m+n-2}+5p^{'}qf_{m+n-1}\right)+5\left[5p^{'}q\,(-1)^{m}\cdot f_{n-m+1}+pp^{'}\,(-1)^{m}\cdot l_{n-m}\right]+$$

$$+25\left(pq^{'}f_{m+n-1}+qq^{'}l_{m+n}\right)+25\left[pq^{'}\cdot(-1)^{m}\cdot f_{n-m-1}+qq^{'}\cdot(-1)^{m}\cdot l_{n-m}\right]=$$

$$=5g_{m+n-2}^{5p^{'}q,pp^{'}}+5g_{m+n-1}^{5p^{'}q,0}+5g_{n-m}^{5p^{'}q\cdot(-1)^{m},pp^{'}\cdot(-1)^{m}}+5g_{n-m+1}^{5p^{'}q\cdot(-1)^{m},0}+$$

$$+5g_{m+n}^{5pq^{'},5qq^{'}}+5g_{n-m}^{5pq^{'}\cdot(-1)^{m},5qq^{'}\cdot(-1)^{m}}.$$

Therefore, it results that $5G_{n}^{p,q}\cdot 5G_{m}^{p^{'},q^{'}}\in M$.
From here, we get that M is an order of the quaternion algebra $\mathbb{H}_{\mathbb{Q}}(\alpha,\beta)$.

1) and 3) are obviously.□

Remark 3.6.11. For $\alpha=\beta=-1$, we have that M is included in the set of Hurwitz quaternions,

$$\mathcal{H}=\{q=a_1+a_2i+a_3j+a_4k\in\mathbb{H}_{\mathbb{Q}}(-1,-1),a_1,a_2,a_3,a_4\in\mathbb{Z}\text{ or }\mathbb{Z}+\frac{1}{2}\},$$

which is a maximal order in $\mathbb{H}_{\mathbb{Q}}(-1,-1)$.

3.7. Real matrix representations for the complex quaternions

The results presented in this section, were obtained especially in the paper [Fl, Sh; 13(2)]. It is know that each finite dimensional associative algebra A over an arbitrary field K is isomorphic with a subalgebra of the algebra $\mathcal{M}_n(K)$, with $n=\dim_K A$. Therefore, we can find a faithful representation of the algebra A in the algebra $\mathcal{M}_n(K)$. For example, the real quaternion division algebra is algebraically isomorphic to a 4×4 real matrix algebra. Starting from some results obtained by Y. Tian in [Ti; 00] and in [Ti; 00(1)], in the we will show that the complex quaternion algebra is algebraically isomorphic to a 8×8 real matrix algebra and will investigate the properties of the obtained left and right real matrix representations for the complex quaternions.

We also provide some examples in the special case of the complex Fibonacci quaternions.

Let K be the field $\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R}\}$. The map

$$\varphi : \mathbb{C} \to K, \varphi(a+bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

where $i^2 = -1$ is a fields morphism and $\varphi(z) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ is called the matrix representation of the element $z = a + bi \in \mathbb{C}$.

Let $\mathbb{H} = \mathbb{H}(-1,-1)$ be the real division quaternion algebra.

A complex quaternion is an element of the form $Q = c_0 + c_1 e_1 + c_2 e_2 + c_3 e_3$, where $c_n \in \mathbb{C}, n \in \{0,1,2,3\}$,

$$e_n^2 = -1, \ \ n \in \{1,2,3\}$$

and

$$e_m e_n = -e_n e_m = \beta_{mn} e_t, \ \beta_{mn} \in \{-1,1\}, m \neq n, m, n \in \{1,2,3\},$$

β_{mn} and e_t being uniquely determined by e_m and e_n. We denote by $\mathbb{H}_C$ the algebra of the complex quaternions, called *the complex quaternion algebra*. This algebra is an algebra over the field $\mathbb{C}$. Let $\{1, e_1, e_2, e_3\}$ be a basis in $\mathbb{H}_C$.

The map $\gamma : \mathbb{R} \to \mathbb{C}, \gamma(a) = a$ is the inclusion morphism between $\mathbb{R}$-algebras $\mathbb{R}$ and $\mathbb{C}$. We denote by $\mathbb{F}$ the $\mathbb{C}$-subalgebra of the algebra $\mathbb{H}_C$,

$$\mathbb{F} = \{Q \in \mathbb{H}_C \ \mid \ Q = c_0 + c_1 e_1 + c_2 e_2 + c_3 e_3, c_n \in \mathbb{R}, n \in \{0,1,2,3\}\}.$$

By the scalar restriction, $\mathbb{F}$ became an algebra over $\mathbb{R}$, with the multiplication " $\cdot$ "

$$a \cdot Q = \gamma(a) Q = aQ, a \in \mathbb{R}, Q \in \mathbb{F}.$$

We denote this algebra by $\mathbb{H}_R$. The map

$$\delta : \mathbb{H} \to \mathbb{H}_R, \delta(1) = 1, \delta(i) = e_1, \delta(j) = e_2, \delta(k) = e_3$$

and

$$\delta(a_0 + a_1 i + a_2 j + a_3 k) = a_0 + a_1 e_1 + a_2 e_2 + a_3 e_3,$$

where $a_m \in \mathbb{R}, m \in \{0,1,2,3\}$ is an algebra isomorphism between the algebras $\mathbb{H}$ and $\mathbb{H}_R$.The algebra $\mathbb{H}_R$ has the same basis $\{1, e_1, e_2, e_3\}$ as the algebra $\mathbb{H}_C$. From now one, we will identify the quaternion $a_0 + a_1 i + a_2 j + a_3 k$ with the "complex" quaternion $a_0 + a_1 e_1 + a_2 e_2 + a_3 e_3$, $a_m \in \mathbb{R}, m \in \{0,1,2,3\}$ and instead of $\mathbb{H}_R$ we will use $\mathbb{H}$.

It results that the element $Q \in \mathbb{H}_C$, $Q = c_0 + c_1 e_1 + c_2 e_2 + c_3 e_3, c_m \in \mathbb{C}, m \in \{0,1,2,3\}$, can be written as $Q = (a_0 + ib_0) + (a_1 + ib_1)e_1 + (a_2 + ib_2)e_2 + (a_3 + ib_3)e_3$, where $a_m, b_m \in \mathbb{R}, m \in \{0,1,2,3\}$ and $i^2 = -1$.

Therefore, we can write a complex quaternion under the form

$$Q = a + ib,$$

with $a, b \in \mathbb{H}$, $a = a_0 + a_1 e_1 + a_2 e_2 + a_3 e_3, b = b_0 + b_1 e_1 + b_2 e_2 + b_3 e_3$.

The conjugate of the complex quaternion Q is the element $\overline{Q} = c_0 - c_1 e_1 - c_2 e_2 - c_3 e_3$. It results that

$$\overline{Q} = \overline{a} + i\overline{b}. \tag{3.7.1.}$$

For the quaternion $a = a_0 + a_1 e_1 + a_2 e_2 + a_3 e_3 \in \mathbb{H}$, we define the element

$$a^* = a_0 + a_1 e_1 - a_2 e_2 - a_3 e_3. \tag{3.7.2.}$$

We remark that

$$(a^*)^* = a \tag{3.7.3.}$$

and

$$(a+b)^* = a^* + b^*, \tag{3.7.4.}$$

for all $a, b \in \mathbb{H}$.

For the quaternion algebra $\mathbb{H}$, in [Ti; 00], was defined the map

$$\lambda : \mathbb{H} \to \mathcal{M}_4(\mathbb{R}), \lambda(a) = \begin{pmatrix} a_0 & -a_1 & -a_2 & -a_3 \\ a_1 & a_0 & -a_3 & a_2 \\ a_2 & a_3 & a_0 & -a_1 \\ a_3 & -a_2 & a_1 & a_0 \end{pmatrix},$$

where $a = a_0 + a_1 e_1 + a_2 e_2 + a_3 e_3 \in \mathbb{H}$, is an isomorphism between $\mathbb{H}$ and the algebra of the matrices:

$$\left\{ \begin{pmatrix} a_0 & -a_1 & -a_2 & -a_3 \\ a_1 & a_0 & -a_3 & a_2 \\ a_2 & a_3 & a_0 & -a_1 \\ a_3 & -a_2 & a_1 & a_0 \end{pmatrix}, a_0, a_1, a_2, a_3 \in \mathbb{R} \right\}.$$

We remark that the matrix $\lambda(a) \in \mathcal{M}_4(\mathbb{R})$ has as columns the coefficients in $\mathbb{R}$ of the basis $\{1, e_1, e_2, e_3\}$ for the elements $\{a, ae_1, ae_2, ae_3\}$.

The matrix $\lambda(a)$ is called *the left matrix representation* of the element $a \in \mathbb{H}$.

Analogously with the left matrix representation, for the element $a \in \mathbb{H}$, in [Ti; 00], was defined *the right matrix representation*:

$$\rho : \mathbb{H} \to \mathcal{M}_4(\mathbb{R}), \quad \rho(a) = \begin{pmatrix} a_0 & -a_1 & -a_2 & -a_3 \\ a_1 & a_0 & a_3 & -a_2 \\ a_2 & -a_3 & a_0 & a_1 \\ a_3 & a_2 & -a_1 & a_0 \end{pmatrix},$$

where $a = a_0 + a_1e_1 + a_2e_2 + a_3e_3 \in \mathbb{H}$.

We remark that the matrix $\rho(a) \in \mathcal{M}_4(\mathbb{R})$ has as columns the coefficients in $\mathbb{R}$ of the basis $\{1, e_1, e_2, e_3\}$ for the elements $\{a, e_1a, e_2a, e_3a\}$.

Proposition 3.7.1. [Ti; 00] *For $x, y \in \mathbb{H}$ and $r \in K$ we have:*
i) $\lambda(x+y) = \lambda(x) + \lambda(y)$, $\lambda(xy) = \lambda(x)\lambda(y)$, $\lambda(rx) = r\lambda(x)$, $\lambda(1) = I_4$, $r \in K$.
ii) $\rho(x+y) = \rho(x) + \rho(y), \rho(xy) = \rho(y)\rho(x), \rho(rx) = r\rho(x)$, $\rho(1) = I_4$, $r \in K$.
iii) $\lambda\left(x^{-1}\right) = (\lambda(x))^{-1}, \rho\left(x^{-1}\right) = (\rho(x))^{-1}$, *for* $x \neq 0$.□

Proposition 3.7.2. [Ti; 00] *For $x \in \mathbb{H}$, let $\overrightarrow{x} = (a_0, a_1, a_2, a_3)^t \in \mathcal{M}_{1\times 4}(K)$, be the vector representation of the element x. Therefore for all $a, b, x \in \mathbb{H}$ the following relations are fulfilled:*
i) $\overrightarrow{ax} = \lambda(a)\overrightarrow{x}$.
ii) $\overrightarrow{xb} = \rho(b)\overrightarrow{x}$.
iii) $\overrightarrow{axb} = \lambda(a)\rho(b)\overrightarrow{x} = \rho(b)\lambda(a)\overrightarrow{x}$.
iv) $\rho(b)\lambda(a) = \lambda(a)\rho(b)$.
v) $\det(\lambda(x)) = \det(\rho(x)) = (n(x))^2$.□

For details about the matrix representations of the real quaternions, the reader is referred to [Ti; 00].

Let θ be the matrix $\theta = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \lambda(e_1) = \lambda(i)$. The matrix

$$\Gamma(Q) = \begin{pmatrix} \lambda(a) & -\lambda(b^*) \\ \lambda(b) & \lambda(a^*) \end{pmatrix},$$

where $Q = a + ib$ is a complex quaternion, with $a = a_0 + a_1e_1 + a_2e_2 + a_3e_3 \in \mathbb{H}, b = b_0 + b_1e_1 + b_2e_2 + b_3e_3 \in \mathbb{H}$ and $i^2 = -1$, is called *the left real matrix representation for the complex quaternion* Q. The *right real matrix representation* for the complex quaternion Q is the matrix:

$$\Theta(Q) = \begin{pmatrix} \rho(a) & -\rho(b) \\ \rho(b^*) & \rho(a^*) \end{pmatrix}.$$

We remark that $\Gamma(Q), \Theta(Q) \in \mathcal{M}_8(\mathbb{R})$.

Now, let M be the matrix

$$M = (1, -e_1, -e_2, -e_3)^t.$$

Proposition 3.7.3. *If* $a = a_0 + a_1e_1 + a_2e_2 + a_3e_3 \in \mathbb{H}$, *we have:*
i) $\lambda(a)M = Ma$.
ii) $\theta M = Me_1$.
iii) $\lambda(ia) = \theta\lambda(a)$ *and* $\lambda(ai) = \lambda(a)\theta$.

Proof. By straightforward calculations. □

Proposition 3.7.4. *Let* $a, x \in \mathbb{H}$ *be two quaternions, then the following relations are true:*
i) $a^*i = ia$, *where* $i^2 = -1$.
ii) $ai = ia^*$, *where* $i^2 = -1$.
iii) $-a^* = iai$, *where* $i^2 = -1$.
iv) $(xa)^* = x^*a^*$.
v) For $X, A \in \mathbb{H}_C, X = x + iy, A = a + ib$, *we have*

$$XA = xa - y^*b + i(x^*b + ya).$$

Proof. Relations from i), ii), iii) are obviously.

iv) From ii), it results $(xa)^{*}=-i\,(xa)\,i=-ixai=(ixi)(iai)=x^{*}a^{*}$.

v) We obtain

$XA=(x+iy)\,(a+ib)=xa+xib+iya+iyib=$

$=xa-y^{*}b+i\,(x^{*}b+ya)\,.\square$

Proposition 3.7.5. *For* $X,A\in\mathbb{H}_{C},X=x+iy,A=a+ib$, *we have* $\Gamma\,(XA)=\Gamma\,(X)\,\Gamma\,(A)\,.$

Proof. It results that

$$\Gamma\,(X)\,\Gamma\,(A)=\begin{pmatrix}\lambda\,(x) & -\lambda\,(y^{*})\\ \lambda\,(y) & \lambda\,(x^{*})\end{pmatrix}\begin{pmatrix}\lambda\,(a) & -\lambda\,(b^{*})\\ \lambda\,(b) & \lambda\,(a^{*})\end{pmatrix}=$$

$$=\begin{pmatrix}\lambda\,(x)\,\lambda\,(a)-\lambda\,(y^{*})\,\lambda\,(b) & -\lambda\,(x)\,\lambda\,(b^{*})-\lambda\,(y^{*})\,\lambda\,(a^{*})\\ \lambda\,(y)\,\lambda\,(a)+\lambda\,(x^{*})\,\lambda\,(b) & -\lambda\,(y)\,\lambda\,(b^{*})+\lambda\,(x^{*})\,\lambda\,(a^{*})\end{pmatrix}=$$

$$=\begin{pmatrix}\lambda(xa-y^{*}b) & -\lambda(xb^{*}+y^{*}a^{*})\\ \lambda(ya+x^{*}b) & \lambda(-yb^{*}+x^{*}a^{*})\end{pmatrix}.$$

$$\Gamma\,(XA)=\begin{pmatrix}\lambda(xa-y^{*}b) & -\lambda((x^{*}b+ya)^{*})\\ \lambda(x^{*}b+ya) & \lambda((xa-y^{*}b)^{*})\end{pmatrix}=$$

$$=\begin{pmatrix}\lambda(xa-y^{*}b) & -\lambda(xb^{*}+y^{*}a^{*})\\ \lambda(ya+x^{*}b) & \lambda(x^{*}a^{*}-yb^{*})\end{pmatrix}.\ \square$$

Definition 3.7.6. For $X\in\mathbb{H}_{C},X=x+iy$, we denote by

$$\overrightarrow{X}=(\overrightarrow{x},\overrightarrow{y})^{t}\in\mathcal{M}_{8\times1}\,(\mathbb{R})$$

the vector representation of the element X, where

$x=x_0+x_1e_1+x_2e_2+x_3e_3\in\mathbb{H},y=y_0+y_1e_1+y_2e_2+y_3e_3\in\mathbb{H}$ and

$\overrightarrow{x}=(x_0,x_1,x_2,x_3)^{t}\in\mathcal{M}_{4\times1}\,(\mathbb{R})\,,$

$\overrightarrow{y}=(y_0,y_1,y_2,y_3)^{t}\in\mathcal{M}_{4\times1}\,(\mathbb{R})$ are the vector representations for the quaternions x and y, as was defined above.

Proposition 3.7.7. *Let* $X\in\mathbb{H}_{C},X=x+iy,x,y\in\mathbb{H}$, *then:*

i) $\overrightarrow{X}=\Gamma\,(X)\begin{pmatrix}1\\0\end{pmatrix}$, *where* $1=I_4\in\mathcal{M}_4\,(\mathbb{R})$ *is the identity matrix and* $0=O_4\in\mathcal{M}_4\,(\mathbb{R})$ *is the zero matrix.*

ii) $\overrightarrow{AX} = \Gamma(A)\overrightarrow{X}$.

iii) $\alpha\overrightarrow{y^*} = \overrightarrow{y}$, *where* $\alpha = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \in \mathcal{M}_4(\mathbb{R})$.

iv) $\alpha^2 = I_4$.

Proof. i) $\Gamma(X)\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \lambda(x) & -\lambda(y^*) \\ \lambda(y) & \lambda(x^*) \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \lambda(x) \\ \lambda(y) \end{pmatrix} =$

$= \begin{pmatrix} \lambda(1 \cdot x) \\ \lambda(1 \cdot y) \end{pmatrix} = \begin{pmatrix} \lambda(1)\overrightarrow{x} \\ \lambda(1)\overrightarrow{y} \end{pmatrix} = \begin{pmatrix} \overrightarrow{x} \\ \overrightarrow{y} \end{pmatrix}$.

ii) From i), we obtain that

$\overrightarrow{AX} = \Gamma(AX)\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \Gamma(A)\Gamma(X)\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \Gamma(A)\overrightarrow{X}$.

iii) $\alpha\overrightarrow{y^*} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}\begin{pmatrix} y_0 \\ y_1 \\ -y_2 \\ -y_3 \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{pmatrix} = \overrightarrow{y}$.□

Proposition 3.7.8. *Let* M_8 *be the matrix* $M_8 = \begin{pmatrix} \theta M \\ -M \end{pmatrix}$, *therefore we have* $-\frac{1}{4}M_8^t M_8 = 1$.

Proof. By straightforward calculations.□

Theorem 3.7.9. *Let* $Q \in \mathbb{H}_C$ *be a complex quaternion. With the above notations, the following relations are fulfilled:*

i) $\Gamma^t(Q^*)M_8 = M_8 Q$, *where* $Q = x + iy, Q^* = x^* + iy, x, y \in \mathbb{H}$.

ii) $Q = -\frac{1}{4}M_8^t \Gamma(Q^*)M_8$.

Proof. i) Let Q be a complex quaternion. We obtain

$\Gamma^t(Q^*)M_8 = \begin{pmatrix} \lambda(x^*) & \lambda(y) \\ -\lambda(y^*) & \lambda(x) \end{pmatrix}\begin{pmatrix} \theta M \\ -M \end{pmatrix} =$

$= \begin{pmatrix} \lambda(x^*)\theta M - \lambda(y)M \\ -\lambda(y^*)\theta M - \lambda(x)M \end{pmatrix} = \begin{pmatrix} \lambda(x^* i - y)M \\ -\lambda(y^* i + x)M \end{pmatrix} =$

$$=\begin{pmatrix} \lambda(ix+iiy)M \\ -\lambda(iy+x)M \end{pmatrix}=\begin{pmatrix} \lambda(i(x+iy))M \\ -M(x+iy) \end{pmatrix}=$$

$$=\begin{pmatrix} \theta\lambda(x+iy)M \\ -M(x+iy) \end{pmatrix}=\begin{pmatrix} \theta M(x+iy) \\ -M(x+iy) \end{pmatrix}\begin{pmatrix} \theta M \\ -M \end{pmatrix}(x+iy)=M_8Q.$$

ii) If we multiply the relation $\Gamma^t(Q^*)M_8=M_8Q$ to the left side with $-\frac{1}{4}M_8^t$, we obtain $Q=-\frac{1}{4}M_8^t\Gamma^t(Q^*)M_8$.□

Proposition 3.7.10. *For $X,A\in\mathbb{H}_C, X=x+iy, A=a+ib$, we have*

$$\Theta(XA)=\Theta(A)\Theta(X).$$

Proof. It results that

$$\Theta(XA)=\begin{pmatrix} \rho(xa\text{-}y^*b) & \text{-}\rho(x^*b+ya) \\ \rho\left((x^*b+ya)^*\right) & \rho\left((xa\text{-}y^*b)^*\right) \end{pmatrix}=$$

$$=\begin{pmatrix} \rho(xa\text{-}y^*b) & \text{-}\rho(x^*b+ya) \\ \rho\left((x^*b+ya)^*\right) & \rho\left((xa\text{-}y^*b)^*\right) \end{pmatrix}=$$

$$=\begin{pmatrix} \rho(xa\text{-}y^*b) & \text{-}\rho(x^*b+ya) \\ \rho(xb^*+y^*a^*) & \rho(x^*a^*\text{-}yb^*) \end{pmatrix}.$$

$$\Theta(A)\Theta(X)=\begin{pmatrix} \rho(a) & \text{-}\rho(b) \\ \rho(b^*) & \rho(a^*) \end{pmatrix}\begin{pmatrix} \rho(x) & \text{-}\rho(y) \\ \rho(y^*) & \rho(x^*) \end{pmatrix}=$$

$$=\begin{pmatrix} \rho(a)\rho(x)\text{-}\rho(b)\rho(y^*) & \text{-}\rho(a)\rho(y)\text{-}\rho(b)\rho(x^*) \\ \rho(b^*)\rho(x)+\rho(a^*)\rho(y^*) & \text{-}\rho(b^*)\rho(y)+\rho(a^*)\rho(x^*) \end{pmatrix}=$$

$$=\begin{pmatrix} \rho(xa-y^*b) & -\rho(x^*b+ya) \\ \rho(xb^*+y^*a^*) & \rho(x^*a^*-yb^*) \end{pmatrix}.\square$$

Proposition 3.7.11. *Let $X\in\mathbb{H}_C, X=x+iy, x,y\in\mathbb{H}$, then:*

i) $\overrightarrow{X}=\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\Theta(X)\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, where $1=I_4\in\mathcal{M}_4(\mathbb{R})$ is the identity matrix, $0=O_4\in\mathcal{M}_4(\mathbb{R})$ is the zero matrix and $\alpha\in\mathcal{M}_4(\mathbb{R})$ as in Proposition 2.5 iii).

ii) $\overrightarrow{XA}=\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\Theta(A)\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\overrightarrow{X}$.

iii) $\Gamma(A)\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\Theta(B)\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}=$

$=\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\Theta(B)\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\Gamma(A)$, *for all* $A,B\in\mathbb{H}_C$.

Proof. i) We have $\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\Theta(X)\begin{pmatrix} 1 \\ 0 \end{pmatrix}=$

$=\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\begin{pmatrix} \rho(x) & -\rho(y) \\ \rho(y^*) & \rho(x^*) \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}=$

$=\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\begin{pmatrix} \rho(x) \\ \rho(y^*) \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\begin{pmatrix} \overrightarrow{x} \\ \overrightarrow{y^+} \end{pmatrix}=$

$=\begin{pmatrix} \overrightarrow{x} \\ \alpha\overrightarrow{y^+} \end{pmatrix}=\begin{pmatrix} \overrightarrow{x} \\ \overrightarrow{y} \end{pmatrix}$.

ii) $\overrightarrow{XA}=\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\Theta(XA)\begin{pmatrix} 1 \\ 0 \end{pmatrix}=$

$=\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\Theta(A)\Theta(X)\begin{pmatrix} 1 \\ 0 \end{pmatrix}=$

$=\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\Theta(A)\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\Theta(X)\begin{pmatrix} 1 \\ 0 \end{pmatrix}=$

$=\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\Theta(A)\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\overrightarrow{X}$.

iii) We obtain $\overrightarrow{AXB}=\overrightarrow{A(XB)}=\Gamma(A)\overrightarrow{XB}=$

$=\Gamma(A)\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\Theta(B)\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\overrightarrow{X}$.

Since $\overrightarrow{AXB}=\overrightarrow{A(XB)}=\overrightarrow{(AX)B}$, it results that

$\overrightarrow{(AX)B}=\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\Theta(B)\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\overrightarrow{AX}=$

$=\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix} \Theta(B) \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix} \Gamma(A) \overrightarrow{X}$, therefore we obtain the asked relation.
□

Theorem 3.7.12. *With the above notations, the following relation is true:*

$$\Gamma^t(X) = M_1 \Theta(X) M_2,$$

where

$M_1=\begin{pmatrix} -A_1 & 0 \\ 0 & A_1 \end{pmatrix} \in \mathcal{M}_8(\mathbb{R})$,

$M_2=\begin{pmatrix} -A_2 & 0 \\ 0 & A_2 \end{pmatrix} \in \mathcal{M}_8(\mathbb{R})$ *and*

$$A_1=\begin{pmatrix} 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix} \in \mathcal{M}_4(\mathbb{R}),$$

$$A_2=\begin{pmatrix} 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \in \mathcal{M}_4(\mathbb{R}).$$

Proof. First, we remark that $A_1 \rho(a) A_2 = \lambda^t(a)$.

We have

$M_1 \Theta\left(\overline{X}\right) M_2 =$

$$= \begin{pmatrix} -A_1 & 0 \\ 0 & A_1 \end{pmatrix} \begin{pmatrix} \rho(x) & -\rho(y) \\ \rho(y^*) & \rho(x^*) \end{pmatrix} \begin{pmatrix} -A_2 & 0 \\ 0 & A_2 \end{pmatrix} =$$

$$= \begin{pmatrix} -A_1\rho(x) & A_1\rho(y) \\ A_1\rho(y^*) & A_1\rho(x^*) \end{pmatrix} \begin{pmatrix} -A_2 & 0 \\ 0 & A_2 \end{pmatrix} =$$

$$= \begin{pmatrix} A_1\rho(x)A_2 & A_1\rho(y)A_2 \\ -A_1\rho(y^*)A_2 & A_1\rho(x^*)A_2 \end{pmatrix} = \begin{pmatrix} \lambda(x) & \lambda(y) \\ -\lambda(y^*) & \lambda(x^*) \end{pmatrix} =$$

$$= \begin{pmatrix} \lambda(x) & -\lambda(y^*) \\ \lambda(y) & \lambda(x^*) \end{pmatrix}^t = \Gamma^t(x). \square$$

Remark 3.7.13. From the above results, it results that

$$Q = -\frac{1}{4} N_1 \Theta^t (X^*) N_2,$$

where $Q \in \mathbb{H}_C$ is a complex quaternion, $N_1 = M_8^t M_2^t$ and $N_2 = M_1^t M_8$.

Proposition 3.7.14. *For $Q \in \mathbb{H}_C, Q = a + ib$, we have:*

$$\det \Gamma (Q) = \det \Theta (Q) = n (aa^* + b^* b)^2 = n (a^* a + b^* b)^2 .$$

Proof.

We obtain: $\det \Gamma (Q) = \det \begin{pmatrix} \lambda (a) & -\lambda (b^*) \\ \lambda (b) & \lambda (a^*) \end{pmatrix} =$

$= \det (\lambda (a) \lambda (a^*) + \lambda (b^*) \lambda (b)) =$

$= \det (\lambda (aa^* + b^* b)) = n (aa^* + b^* b)^2 .$

For the second, we have: $\det \Theta (Q) = \det \begin{pmatrix} \rho (a) & -\rho (b) \\ \rho (b^*) & \rho (a^*) \end{pmatrix} =$

$= \det (\rho (a) \rho (a^*) + \rho (b) \rho (b^*)) =$

$= \det (\rho (a^* a + b^* b)) = n (a^* a + b^* b)^2 .$

Chapter 4

Some applications in Coding Theory

4.1. Preliminaries

Coding Theory is a mathematical domain with many applications in Information Theory. Various type of codes and their parameters have been intensively studied.(see [Li, Xi; 04]) As one of the important parameters of a code, the distance associated (such as Hamming, Lee, Mannheim, etc.) was also studied for many types of codes and formulae for the minimum values or the maximum values for such distances were found (see [Ne, In, Fa, Pa; 01]). Some of these codes, which have undergone significant development over the last years, are Integer Codes. Integer Codes are codes defined over finite rings of integers modulo $m, m \in \mathbb{Z}$ and have some advantages over the traditional block codes. One of these advantages is that integer codes are capable of correcting a limited number of error patterns which occur most frequently, while the conventional codes intend to correct all possible error patterns, without completely succeeding. Integer Codes have a low encoding and decoding complexity and are suitable for application in real communication systems (see [Ko, Mo, Ii, Ha, Ma; 10]). There are some other codes similar to the Integer Codes, such as for example codes over Gaussian integers ([Hu; 94], [Gh, Fr; 10], [Ne, In, Fa, Pa; 01], [Ri; 95]), codes over Eisenstein–Jacobi integers, [Ne, In, Fa, Pa; 01], a class of error correcting codes based on a generalized Lee distance, [Ni, Hi; 08], codes over Hurwitz integers, [Gu; 13], etc, which have been intensively studied in recent years.

QAM, that is quadrature amplitude modulation, is used in many digital data radio communications and data communication applications. The most

common errors which appear in many digital data radio communications and data communication applications are those which change a point into its nearest neighbor. The Hamming distance and the Lee distance are not able to correct these errors in a QAM signal. To improve this situation, in [Hu; 94], Huber constructed codes over Gaussian integers with a new distance, called Mannheim distance. He proved that these codes can correct Mannheim error of weight 1 and used this new distance to find the properties of these codes (see [Mo, Ha, Ko; 04] for further details). Nevertheless, in [Ni, Hi; 08] the authors introduced a new distance which generalized the Lee distance and constructed codes capable of correcting errors of generalized Lee weight one or two.

In [Gu; 13], the author generalized some results from [Ne, In, Fa, Pa; 01] constructing codes over Hurwitz integers.

The results presented below, were obtained, by the author, especially in the papers [Fl; 15(1)], [Fl; 16].

In information theory and coding theory the error correction are considered a technique used for sending a message, in a redundant way, helping the sender to control errors in data transmission over unreliable or noisy communication channels. In coding theory, a block code is an error-correcting code which encode data in blocks. A block code acts on a block of k bits of input data to produce n bits of output data. We denote this with (n, k). When a very long data stream is transmitted using a block code, the stream is broken into pieces of some fixed size. Each such piece is encoded into a codeword, using the block codes, also called block, and it is transmitted to the receiver for decoding them.

Let $A \neq \varnothing$ be a finite set called *alphabet*. A block code is an injective map

$$\mathcal{C} : A^k \to A^n,$$

where $k, n \in \mathbb{N}$ and $A^k = \underbrace{A \times A \times ... \times A}_{k-times}$.The cardinal q of the set A is called the size of the alphabet. When $q = 2$, the block code is called binary block

code and we can identify the alphabet A with the field $\mathbb{Z}_2$. A message is an element $m \in A^k$ and k is called the length of the message and represents the number of symbols from the message m.The number n represents the length of the block and represents the number of symbols in a block. The rate of a block code is

$$R = \frac{k}{n}$$

and measures the transmission speed.

The *Hamming distance* between two code-words $x = (x_1...x_n) \in \mathcal{C}$ and $y = (y_1...y_n) \in \mathcal{C}$ is the number of positions where x and y differ

$$d_H(x,y) = |\{i \ / \ x_i \neq y_i, i \in \{1,2,...,n\}\}|.$$

The Hamming weight is

$$w_H(x) = |\{i \ / \ x_i \neq 0, x \in \mathcal{C} \ \}|.$$

The minimum distance of a block code is

$$d_{\min} = \min\{d_H(x,y), x \neq y, x, y \in \mathcal{C}\}.$$

Let $x \in A^n$ and $e \in \mathbb{N}$. We define the sphere $S(x,e)$ of radius e and center x to be the set

$$S(x,e) = \{y \in A^n \ / \ d_H(x,y) \leq e \ \}.$$

We have

$$|S(x,e)| = \sum_{i=0}^{e} \mathtt{C}_n^i (q-1)^i,$$

see [Va; 75].

Definition 4.1.1, [Va; 75]. 1) A code $\mathcal{C}$ is called *e-error-correcting code* if and only if for all $x, y \in \mathcal{C}, x \neq y$, we have $d_H(x,y) \geq 2e+1$.From here, for all $x, y \in \mathcal{C}, x \neq y$, it results that $S(x,e) \cap S(y,e) \neq \varnothing$.

2) If $A^n = \underset{x \in \mathcal{C}}{\cup} S(x,e)$ then the code $\mathcal{C}$ is called *perfect*. It result that for each $y \in A^n$, there is an element $x \in \mathcal{C}$, unique determined, such that $d_H(x,y) \leq e$.

Proposition 4.1.2. *A code $\mathcal{C}$ with minimum Hamming distance $d = d_{\min}$ can detected $d-1$ errors and can correct $[\frac{d-1}{2}]$ errors.*

Definition 4.1.3. Let $\mathbb{F}_{p^n}$ be a finite field with p a prime number. Using its vector space structure over $\mathbb{Z}_p$, let $\{\overline{a}_1, ...\overline{a}_s\}$ be a generating system for $\mathbb{F}_{p^n}$. Therefore, each $\overline{x} \in \mathbb{F}_{p^n}$ has the form $\overline{x} = \sum\limits_{i=1}^{s} \overline{x}_i \overline{a}_i, x_i \in \mathbb{Z}$. The $s-$*Lee weight* of $\overline{x}$ is

$$w_L(\overline{x}) = \sum_{i=1}^{s} |x_i|$$

and *Lee distance* between $\overline{x}, \overline{y} \in \mathbb{F}_{p^n}$ is

$$d_L(\overline{x}, \overline{y}) = w_L(\overline{x} - \overline{y}).$$

Definition 4.1.4. 1) A *linear code* of length n over the alphabet $\mathbb{Z}_q$ is a linear subspace of the vector space $\mathbb{Z}_q^n$. If $k = \dim_{\mathbb{Z}_q} \mathcal{C}$ and d is the minimum Hamming distance, therefore the information rate of the code is $R = \frac{k}{n}$ and $\mathcal{C}$ is a code of the type $[n, k, d]_q$.

2) Let $\mathcal{C}$ be a code of the type $[n, k]$. A matrix G whose lines are a basis in $\mathcal{C}$ over $\mathbb{Z}_q$ is called *a generating matrix* for the code $\mathcal{C}$.

3) A *parity check matrix,* H, of a linear code $\mathcal{C}$ is a generator matrix of the dual code, $\mathcal{C}^{\perp} = \{y \in \mathbb{Z}_q^n \ / \ < y, x >= 0, x \in \mathcal{C}\}$. Therefore, we have that $c \in \mathcal{C}$ if and only if $cH^t = 0$.

4) With the above notations, for each $x \in \mathbb{Z}_q^n$, *the syndrome* of the vector x is $s(x) = Hx^t \in \mathbb{Z}_q^{n-k}$.

How we can use the syndrome in the decoding process? We define the vector space modulo $\mathcal{C}$, $\mathbb{Z}_q^n/\mathcal{C}$. We remark that two vectors $x, y \in \mathbb{Z}_q^n$ belong to the same equivalence class $c + \mathcal{C}$ if and only if $s(x) = s(y)$. Indeed, if $x, y \in c + \mathcal{C}$, we have $x - y \in \mathcal{C}$, therefore $H(x - y)^t = 0$. It results that $Hx^t = Hy^t$. Therefore, for decoding using the syndrome, we must follow the below algorithm:

-We compute the syndrome of the received vector x, $s(x)$;

-We search a representative e such that $s(e) = s(x)$;

-We will decode x by $c = x - e$.

Definition 4.1.5. A code $\mathcal{C} \subset \mathbb{Z}_q^n$ is called *a cyclic code* if and only if $\mathcal{C}$ is a linear code and if for each $c \in \mathcal{C}$, $c = (c_0, ..., c_{n-1})$, we have $(c_{n-1}, c_0, ..., c_{n-2}) \in \mathcal{C}$.

Remark 4.1.6. To each codeword $c \in \mathcal{C}$, $c = (c_0, ..., c_{n-1})$, we associate the polynomial code $c(x) = c_0 + c_1 x + ... + c_{n-1}x^{n-1}$. We have $x\left(c_0 + c_1 x + ... + c_{n-1}x^{n-1}\right) = c_{n-1}(x^n - 1) + c_{n-1} + c_0 x + ... + c_{n-2}x^{n-1}$. It results that $\mathcal{C}$ is an ideal in the ring $\mathbb{Z}_q[x] \,/\, (x^n - 1)$, therefore a principal ideal since $\mathbb{Z}_q[x] \,/\, (x^n - 1)$ is a principal ring. This ideal is generated by the unique monic element in $\mathcal{C}$ of minimum degree, called *the generator polynomial* and denoted with g. The polynomial g is a divisor of the polynomial $x^n - 1$.

4.2. Integer Codes

Integer Codes are codes defined over finite rings of integers modulo $m, m \in \mathbb{Z}$. These codes have a low encoding and and decoding complexity and are suitable for application in communication systems. Thus they became increasingly popular over the last years (see [Ko, Mo, Ii, Ha, Ma; 10]).

These codes were defined first in [Vi, Mo; 98]. Let $\mathbb{Z}_p$ be a ring of integer modulo p, where p is an arbitrary integer. Let $H \in \mathcal{M}_{m,n}(\mathbb{Z}_p)$ be a matrix. An integer code of length n and parity check matrix H is the set

$$\mathcal{C}(H, f) = \{c \in \mathbb{Z}_p^n \;/\; cH^T = f \;\; mod \; p\},$$

where $f \in \mathbb{Z}_p^m$. The matrix H is called *the parity check* matrix for the code $\mathcal{C}(H, f)$ (see [Ko, Mo, Ii, Ha, Ma;10]). Therefore, if $c = (c_1, ..., c_n) \in \mathcal{C}(H, f)$, we have

$$\sum_{i=1}^{n} c_i h_{ji} = f_j, f_j \in \mathbb{Z}_p, j \in \{1, 2, ..., m\} \qquad (4.2.1.)$$

When $f = 0$, the code are linear. In the following, we will consider only linear codes. Supposing that a codeword c is sent through a noisy channel, we can receive a vector under the form $w = c + e$, where $e = (e_1, ...e_n)$ is an error vector. If t of the entries of e are nonzero, we say that t errors occurred in c. Integer codes have many applications in various domains as for example information theory, computer science, graph theory, etc. In coding theory these codes are a useful tool in a single–error–correction codes. It results that the integer codes over the block codes can correct errors of a given type. Therefore, for a given channel we can choose the type of the most common

errors and after that we construct integer code capable of correcting those errors. (see [Ko, Ma, Mo; 10])

Definition 4.2.1. [Ko, Ma, Mo; 10] The code $\mathcal{C}(H, f)$ is called $t-multiple$ $(\pm e_1, ..., \pm e_r)$ errors correctable if this code can correct up to t errors with values in the set $E = \{\pm e_1, ..., \pm e_r\}$, called *the error set.*

In [Ta; 08], the author described the construction of the linear perfect Integer Codes. We shortly present this construction from the above mentioned paper. Let p be a prime integer and $\mathbb{Z}_p$ the residue group modulo p. Let $\mathbb{Z}_p^* = (\mathbb{Z}_p - \{0\}, \cdot)$ the multiplicative cyclic group. We denote with $\mathfrak{H} = \{h_j = (h_{j1}, ...h_{jn}),\ j \in \{1, 2, ..., m\}\}$, the integers modulo p defined in (4.2.1). We consider the errors set $E = \{\pm e_1, ..., \pm e_r\}$, as was defined in Definition 4.2.1, supposing that $1 \in E$. We consider g a generator of $\mathbb{Z}_p^*$, therefore $g^{\frac{p-1}{2}} = -1$. If we take $\mathbb{Z}_p^*/\{-1, 1\}$, we have that $\widehat{g}$ is also a generator in $\mathbb{Z}_p^*/\{-1, 1\}$. The idea of this construction is to organize E as a subgroup isomorphic with a subgroup $\mathcal{G}$ of $\mathbb{Z}_p^*/\{-1, 1\}$. The group $\mathbb{Z}_p^*/\{-1, 1\}$ is generated by $\widehat{g}$ and $\mathcal{G}$ must be generated by an element of the form $\widehat{g}^t, t \ / \ \frac{p-1}{2}$ since the order of the group $\mathcal{G}$ is a divisor of $\frac{p-1}{2}$, the order of the group $\mathbb{Z}_p^*/\{-1, 1\}$. Therefore, we have that $x \in \mathcal{G}$ if and only if it is on the form

$$x = g^{jt}, j \in \{0, ..., \frac{p-1}{2t}\}.$$

Algorithm for Perfect Integer Codes.(see [Ta; 08])

1. We find a generator g for the group $\mathbb{Z}_p^*/\{-1, 1\}$;
2. All elements $e_i \in E$ will be write on the form $e_i = \widehat{g}^{\alpha_i}$ in $\mathbb{Z}_p^*/\{-1, 1\}$.
3. We consider D the set of all divisors of $\frac{p-1}{2t}$. For all $s \in D$, let $\alpha_i = s\beta_i$. If the set $\{\beta_0 \ mod \ t, ..., \beta_{t-1} mod \ t\}$ is equal with the set $\{0, 1, ..., t-1\}$, therefore we obtain the subgroup $\mathcal{G} = \{(\widehat{g}^s)^{jt},\ j \in \{0, ..., \frac{p-1}{2t}\}\}$.

Let $\mathbb{Z}[i] = \{z = a + bi \ / \ a, b \in \mathbb{Z}\}$, $p \in \mathbb{Z}$ be a prime number of the form $4k+1$, such that $p^2 = a^2 + b^2 = \pi\overline{\pi} = \mathbf{n}(\pi)$, where $\pi \in \mathbb{Z}[i]$, $\pi = a + bi$ and $\mathbf{n}(\pi)$ is the norm of the Gaussian integer π.The Gaussian integer π is called a prime integer in $\mathbb{Z}[i]$. We consider $\mathbb{Z}[i]_\pi$ the residue class modulo π.How we can obtain $\mathbb{Z}[i]_\pi$? The procedure is presented in [Hu; 94], Appendix E and [Da,Sa,Va; 03], Proposition 2.1.2, which we briefly describe it in the following.

Let $z \in \mathbb{C}, z = a+bi$. We define $[z] = [a] + [b]\, i$, where $[a]$ is the integer part of the real number a. Let $u, w \in \mathbb{Z}[i],\ w \neq 0$. We can find $\alpha, \beta \in \mathbb{Z}[i]$ such that $u = \alpha w + \beta$, where $\alpha = \left[\frac{u\overline{w}}{\mathbf{n}(w)}\right]$, $\beta = u - \alpha w$ and $\mathbf{n}(\beta) < \mathbf{n}(w)$. Indeed, let $\frac{u}{w} = x + iy, x, y \in \mathbb{R}$ and let $a, b \in \mathbb{Z}$ such that $\mathbf{n}(x-a) \leq \frac{1}{2}$ and $\mathbf{n}(y-b) \leq \frac{1}{2}$. We take $\alpha = a + bi \in \mathbb{Z}[i]$ and $\beta = w\left[(x-a) + i\,(y-b)\right]$. We remark that $\beta = u - \alpha w$ with $\alpha = \left[\frac{u\overline{w}}{\mathbf{n}(w)}\right]$. It results $\mathbf{n}(\frac{\beta}{w}) = (x-a)^2 + (y-b)^2 \leq \frac{1}{2}$, therefore $\mathbf{n}(\beta) < \mathbf{n}(w)$.

Now we can consider the modulo function $f : \mathbb{Z}_p \to \mathbb{Z}[i]_\pi$,

$$f(\mathbf{u}) = u \ mod \pi = u - \left[\frac{u\overline{\pi}}{\mathbf{n}(\pi)}\right]\pi = \beta, \qquad (4.2.2.)$$

with $\mathbf{n}(\beta) < \mathbf{n}(\pi)$. We remark that the representation of $\mathbb{Z}[i]_\pi$ as points in the complex plane is called *signal constellation.* (see [Hu; 94])

Proposition 4.2.2 . ([Da,Sa,Va; 03], Proposition 2.1.4.) *For each $u, w \in \mathbb{Z}[i]$, there is the greater common divisor $(u, w) \in \mathbb{Z}[i]$ and the following relation holds*

$$(u, w) = au + bw, a, b \in \mathbb{Z}[i].$$

Proof. The set $I = \{au + bw \ / \ a, b \in \mathbb{Z}[i]\}$ is an ideal in $\mathbb{Z}[i]$. We consider the element $\theta = \sigma u + \tau v \in I$ such that it is not zero element and its norm is minimum. From the above, we can find α and β such that $u = c\theta + r$, with $n(r) < n(\theta)$, which is false. Therefore $r = 0$ and $\theta \mid u$.□

We have that $(\pi, \overline{\pi}) = 1$, therefore $1 = v_1\pi + v_2\overline{\pi}$. Using (4.2.2) and the above proposition, we can find $g : \mathbb{Z}[i]_\pi \to \mathbb{Z}_p$,

$$g(\beta) = f^{-1}(\beta) = \beta(v_2\overline{\pi}) + \overline{\beta}(v_1\pi) \ \ mod\ p$$

the inverse of the map f. Indeed, we have that $f(g(\beta)) = f\left(\beta(v_2\overline{\pi}) + \overline{\beta}(v_1\pi)\right) =$
$\beta(v_2\overline{\pi}) + \overline{\beta}(v_1\pi) \ mod\ \pi =$
$= \beta(1 - v_1\pi) + \overline{\beta}(v_1\pi) = \beta.$

Remark 4.2.3. From the above, it results that $\mathbb{Z}[i]_\pi$ is isomorphic with $\mathbb{Z}_p$, therefore the field $\mathbb{Z}_p$ is isomorphic with the residue class of $\mathbb{Z}[i]$ modulo π, where $\mathbf{n}(\pi) = p$. The idea which arise from here is to try to find a subset S of an algebra obtained by the Cayley-Dickson process and an equivalence

relation ρ such that S/ρ is isomorphic with the field $\mathbb{Z}_p$. In papers [Fl; 15], [Fl; 16], was found such a construction.

Over $\mathbb{Z}[i]_\pi$, in [Hu; 94], in the similar way as in [Vi, Mo; 98], were defined binary block codes. A block codes over the Gaussian integer $\mathbb{Z}[i]_\pi$ is a set of codewords of length n of the form $c = (c_1, ..., c_n)$, where $c_i \in \mathbb{Z}[i]_\pi$.

In the following, we briefly present the construction of such a codes with the minimum Mannheim distance $d_M \geq 3$, as was designed in [Hu; 94]. This is necessary to understand how these codes were generalized to Hurwitz Integers in [Gu; 13] and more generally to subsets S of algebras obtained by the Cayley-Dickson process with the property that S is isomorphic with $\mathbb{Z}_p, p$ a prime number. This isomorphism allows us a more flexibility since for a given p, we can find different sets S being in different algebras A_t, obtained by the Cayley-Dickson process.

For $c_1, c_2 \in \mathbb{Z}[i]_\pi$,and $c = (c_1 - c_2) \bmod \pi$, we define the Mannheim weight of c

$$w_M(c) = |\mathrm{Re}c| + |\mathrm{Im}c|$$

and the Mannheim distance between c_1 and c_2

$$d_M(c_1, c_2) = w_M(c).$$

If $v = (v_0, ..., v_{n-1}) \in (\mathbb{Z}[i]_\pi)^n$, we have $w_M(v) = \sum_{i \in \{0,...,n-1\}} w_M(v_i)$.

Let $p = 4n + 1$ be a prime number. We will define codes of length n which can correct one Mannheim error of weight 1. Such errors of weight one can take only values from the set $\{-1, 1 - i, i\}$ and are situated in positions $j \in \{0, 1, ..., n - 1\}$. For an element $\sigma \in \mathbb{Z}[i]_\pi$ of order $p - 1$, a One Mannheim Errors Correction code (OMEC) $\mathcal{C}$ is given by the parity-check matrix

$$H = \left(\sigma^0, \sigma^1, ..., \sigma^{\frac{p-1}{4}-1}\right). \tag{4.2.3.}$$

We know that a codeword c belong to $\mathcal{C}$ if and only if $Hc^t = 0$. It is clear that in this case the generating matrix is

$$G = \begin{pmatrix} -\sigma^1 & 1 & 0 & ... & 0 \\ -\sigma^2 & 0 & 1 & ... & 0 \\ ... & ... & ... & ... & ... \\ -\sigma^{\frac{p-1}{4}-1} & 0 & 0 & ... & 1 \end{pmatrix}.$$

Decoding is easy using the syndrome. We remark that $\sigma^n, \sigma^{2n}, \sigma^{3n}.\sigma^{4n} \in \{-1, 1-i, i\}$. If we receive a vector $r = c + e$, with e an error of $w_M(e) = 1$ resulted at position q, computing the syndrome, we obtain the location q from the relation $s = \sigma^q mod\ n$, with s the syndrome. If we reduce q modulo n, we obtain t, the location of the error, and from here we obtain σ^{q-t}, the value of the error.

The above codes can be generalized to codes of length $n = \frac{p^r-1}{4}$ and the parity check matrix

$$H = \left(\sigma^0, \sigma^1, ..., \sigma^{\frac{p^r-1}{4}-1}\right), \tag{4.2.4.}$$

with $\sigma \in \mathbb{Z}[i]_{\pi^r}$ an element of order $p^r - 1$.In this way, in [Hu; 94], were defined, OMEC block codes over $\mathbb{Z}[i]_\pi$ of the form $[n, k, d_M]$, determined by the matrix H from (4.2.4) of length $\frac{p^r-1}{4}$, of dimension k and minimum Mannheim distance d_M.

To obtain Mannheim Errors Correction codes which can correct errors of Mannheim weight greater than one, in the same paper, was considered a code $\mathcal{C}$ defined by the parity check matrix

$$H = \begin{pmatrix} \sigma^0 & \sigma^1 & \sigma^2 & ... & \sigma^{n-1} \\ \sigma^0 & \sigma^5 & \sigma^{10} & ... & \sigma^{5(n-1)} \\ ... & ... & ... & ... & ... \\ \sigma^0 & \sigma^{4t+1} & \sigma^{2(4t+1)} & ... & \sigma^{(n-1)(4t+1)} \end{pmatrix}, \tag{4.2.5.}$$

where $\sigma \in \mathbb{Z}[i]_{\pi^r}$ is an element of order $4n$ and $\sigma^n = i$. If $c \in \mathcal{C}$, $c = (c_0, ..., c_{n-1})$ is a codeword, if we write it as a polynomial $c = c(x) = \sum_{i=0}^{n-1} c_i x^i$ and since $Hc^t = 0$, we obtain $c\left(\sigma^{4k+1}\right) = 0, k \in \{0, 1, ..., t\}$. If $g(x)$ is the generator polynomial, we have that $g \ / \ c$ and $c/(x^n - i)$. Such a code is called *icyclic*. From here, it results that from $c(x) \in \mathcal{C}$, with $c = (c_0, ..., c_{n-1})$, we obtain $xc(x) - c_{n-1}(x^n - i) = (ic_{n-1}, c_0, ..., c_{n-2}) \in \mathcal{C}$.

To design codes which can correct Mannheim errors of weight two, in the same paper, was considered the case $t = 2$, therefore the parity check matrix

$$H = \begin{pmatrix} \sigma^0 & \sigma^1 & \sigma^2 & ... & \sigma^{n-1} \\ \sigma^0 & \sigma^5 & \sigma^{10} & ... & \sigma^{5(n-1)} \end{pmatrix}.$$

For a received vector $r = e + c$, we compute the syndrome $s = \begin{pmatrix} s_1 \\ s_5 \end{pmatrix} =$

Hr^t. If in position q_1, q_2, we have errors of weight one, namely $\sigma^{L_1-q_1}, \sigma^{L_2-q_2} \in \{-1, 1, -i, i\}$, the error determinator polynomial can be computed $f(z) = \left(z - \sigma^{L_1}\right)\left(z - \sigma^{L_2}\right) = z^2 - s_1 z + P, P = \sigma^{L_1}\sigma^{L_2}$. This polynomial can help us to find the errors, if we can determine the solutions.

Using these ideas, the above results were generalized to Hurwitz Integers, in [Gu; 13], to Octonion integers and to some subsets of algebras obtained by the Cayley-Dickson process in [Fl; 15] and [Fl; 16].

4.3. Codes constructed over Hurwitz Integers

In [Gu; 13], the author described codes over Hurwitz Integers. He played with primes p of the form $6n + 1$ and worked on the quaternion real division algebra $\mathbb{H}$. He considered the set $\mathbb{H}(\mathbb{Z}) = \{q = a_0 + a_1 i + a_2 j + a_3 k \ / \ a_0, a_1, a_2, a_3 \in \mathbb{Z}\}$ and the set of Hurwitz integers $\mathcal{H} = \mathbb{H}(\mathbb{Z}) \cup \mathbb{H}\left(\mathbb{Z} + \frac{1}{2}\right)$.

For $w = \frac{1}{2}(1 + i + j + k)$, he defined the set $\mathcal{R} = \{a + bw \ / \ a, b \in \mathbb{Z}\}$. For $\pi \in \mathcal{R}, \pi$ a prime element, with $\mathbf{n}(\pi) = p, p$ a prime integer, $q_1, q_2 \in \mathcal{R}$, we have $q_1 \equiv q_2 \bmod \pi$ if and only if there is an element $\alpha \in \mathcal{R}$ such that $q_1 - q_2 = \alpha\pi$.Was obtained the set $\mathcal{R}_\pi = \{q \bmod \pi \ / \ q \in \mathcal{R}\}$. We have that $\mathcal{R}_\pi$ and $\mathbb{Z}_p$ are isomorphic. In this way, the field $\mathbb{Z}_p$ is isomorphic with a set which was built using a subset of quaternion, extended the construction of Huber, in which $\mathbb{Z}_p$ is isomorphic with a set which was built using a subset of complex numbers.

Definition 4.3.1. Let $\pi \in \mathbb{H}(\mathbb{Z})$ a prime element and $q_1, q_2 \in \mathcal{H}$ such that there is $\alpha \in \mathbb{H}(\mathbb{Z})$ with property $q_1 - q_2 = \alpha\pi$. We call q_1, q_2 *right congruent modulo* π, denoted $\equiv_r$.

The quotient ring of the Hurwitz integers modulo the above equivalence relation is denoted $\mathcal{H}_\pi = \{q \bmod \pi \ / \ q \in \mathcal{H}\}$.

Definition 4.3.2. [Gu; 13] For $\alpha, \beta \in \mathcal{H}_\pi$, let $\gamma = \alpha - \beta \equiv_r a_0 + a_1\widehat{e}_1 + a_2\widehat{e}_2 + a_3\widehat{e}_3 \bmod \pi$. The *Hurwitz weight* of γ is

$$w_H(\gamma) = |a_0| + |a_1| + |a_2| + |a_3|,$$

with $|a_0|+|a_1|+|a_2|+|a_3|$ minimum.

The *Hurwitz distance* between α, β is defined as

$$d_H(\alpha,\beta) = w_H(\gamma).$$

We have that $d_H(\alpha,\beta)$ is a metric.

For a prime $\pi \in \mathcal{R}$, was considered $\sigma \in \mathcal{R}_\pi$ such that $\sigma^{\frac{p-1}{6}} = w$ or $\sigma^{\frac{p-1}{6}} = -w$. Was defined a code $\mathcal{C}$ given by the following parity check matrix

$$H = \begin{pmatrix} \sigma^0 & \sigma^1 & \sigma^2 & ... & \sigma^{n-1} \\ \sigma^0 & \sigma^7 & \sigma^{14} & ... & \sigma^{7(n-1)} \\ ... & ... & ... & ... & ... \\ \sigma^0 & \sigma^{6t+1} & \sigma^{2(6t+1)} & ... & \sigma^{(n-1)(6t+1)} \end{pmatrix}, t < n.$$

We have that $c \in \mathcal{R}_\pi^n$ is a codeword in $\mathcal{C}$ if and only if $Hc^t = 0$. For the associated code polynomial $c(x) = \sum_{i\in\{0,...,n-1\}} c_i x^i$, we have $c\left(\sigma^{6k+1}\right) = 0, k \in \{0,...,t\}$ and therefore the code generator polynomial
$g(x) = (x-\sigma)\left(x-\sigma^7\right)...\left(x-\sigma^{6t+1}\right)$ is a divisor for $c(x)$ and for the polynomial $x^n - w$ or $x^n + w$. It results that $\mathcal{C}$ is a principal ideal of the ring $\mathcal{R}_\pi[x]/(x^n - w)$ or $\mathcal{R}_\pi[x]/(x^n + w)$. In [Gu; 13], in Theorem 4, Theorem 5, Theorem 6, Theorem 7, were proved the following results.

Proposition 4.3.3. 1) *A code $\mathcal{C}$ defined by the parity check matrix*

$$H = \left(\sigma^0, \sigma^1, ..., \sigma^{n-1}\right)$$

can correct any errors of the form $e(x) = e_i x^i, i \in \{0,1,...,n-1\}$, with $w_H(e_i) = 1$ and any errors of the form $e(x) = w^2 x^i$ or $e(x) = -w^2 x^i, i \in \{0,1,...,n-1\}$, with $w_H\left(-w^2\right) = w_H\left(w^2\right) = 2$. Therefore, $\mathcal{C}$ can correct error vectors of Hurwitz weight 1 with one nonzero component which can take values in the set $\{-1,1,w,-w\}$. The code $\mathcal{C}$ can also correct some of error vectors of Hurwitz weight 2 with one nonzero component which can take value in the set $\{w^2,-w^2\}$.

2) *A code $\mathcal{C}$ given by the parity check matrix*

$$H = \begin{pmatrix} \sigma^0 & \sigma^1 & \sigma^2 & ... & \sigma^{n-1} \\ \sigma^0 & \sigma^7 & \sigma^{14} & ... & \sigma^{7(n-1)} \end{pmatrix}$$

can correct any errors of the form $e(x) = e_i x^i, i \in \{0, 1, ..., n-1\}$, *with* $1 \leq w_H(e_i) \leq d_{\max}$.

3) *A code* $\mathcal{C}$ *given by the parity check matrix*

$$H = \begin{pmatrix} \sigma^0 & \sigma^1 & \sigma^2 & ... & \sigma^{n-1} \\ \sigma^0 & \sigma^7 & \sigma^{14} & ... & \sigma^{7(n-1)} \\ \sigma^0 & \sigma^{13} & \sigma^{26} & ... & \sigma^{13(n-1)} \end{pmatrix}$$

can correct any errors of the form $e_i x^i + e_j x^j$, *with* $w_H(e_i), w_H(e_j) \in \{0, 1\}, i.j \in \{0, 1, ..., n-1\}$.

4) *A code* $\mathcal{C}$ *defined by the parity check matrix*

$$H = \begin{pmatrix} \sigma^0 & \sigma^1 & \sigma^2 & ... & \sigma^{n-1} \\ \sigma^0 & \sigma^7 & \sigma^{14} & ... & \sigma^{7(n-1)} \\ \sigma^0 & \sigma^{13} & \sigma^{26} & ... & \sigma^{13(n-1)} \\ \sigma^0 & \sigma^{19} & \sigma^{38} & ... & \sigma^{19(n-1)} \end{pmatrix}$$

can correct any errors of the form $e_i x^i + e_j x^j$, *with* $w_H(e_i), w_H(e_j) \in [0, d_{\max}], i.j \in \{0, 1, ..., n-1\}$.

The above results were generalized for subsets of Octonion Integers, as we can see in the following section.

4.4. Codes over a subset of Octonion Integers

Due to the structure of the real Octonion algebra, a nonassociative and a noncommutative algebra, in the following, we generalize the above results to a special subset of Octonion integers, comparing them with some results obtained until now. We prove that, under certain circumstances, these codes can correct up to two errors for a transmitted vector and the code rate of the codes is greater than the code rate of the codes defined on the Quaternion integers.

As we can see in the former chapters, the octonion division algebra over $\mathbb{R}$, denoted by $\mathbb{O}(\mathbb{R})$, is a nonassociative unital algebra. This algebra is *power-associative* and *flexible* The algebra $\mathbb{O}(\mathbb{R})$ has the basis $\{1, e_2, e_3, e_4, e_5, e_6, e_7, e_8\}$

and 1 is the unity in $\mathbb{O}(\mathbb{R})$. The basis's elements satisfy the following properties: $e_2^2 = e_3^2 = e_4^2 = e_5^2 = e_6^2 = e_7^2 = e_8^2 = -1$ and $e_i e_j = -e_j e_i = e_k, i \neq j, i, j \in \{2, ..., 8\}$, where $k = i \otimes j$, where $\otimes$ is "x-or" for i, j written in the decimal basis (see [Ba; 09]).

If $x = x_1 + x_2e_2 + x_3e_3 + x_4e_4 + x_5e_5 + x_6e_6 + x_7e_7 + x_8e_8 \in \mathbb{O}(\mathbb{R})$, then its *conjugate* is the octonion $\overline{x} = x_1 - (x_2e_2 + x_3e_3 + x_4e_4 + x_5e_5 + x_6e_6 + x_7e_7 + x_8e_8)$ and the *norm* of the octonion x is $\mathbf{n}(x) = x\overline{x} = \overline{x}x = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 + x_8^2$. The octonionic norm $\mathbf{n}$ is multiplicative.. The *real part* of the octonion x is x_1 and its *vector part* is $x_2e_2 + x_3e_3 + x_4e_4 + x_5e_5 + x_6e_6 + x_7e_7 + x_8e_8 \in \mathbb{O}(\mathbb{R})$.

In [Co, Sm; 03] pp. 55, the authors described *Hurwitz integers* or *Hurwitz Integral Quaternions*, denoted by $\mathcal{H}$, as elements of the form $q = x_1 + x_2e_2 + x_3e_3 + x_4e_4$ where x_1, x_2, x_3, x_4 are in $\mathbb{Z}$ or in $\mathbb{Z} + \frac{1}{2}$. In the same book, pp. 99-105, *Octavian Integers* or *Octonion Integers* were defined as the set of elements spanned by $i_{1587}, i_{2457}, i_{2685}, i_{2378}$ over $\mathbb{O}(\mathbb{Z})$, where

$$i_{abcd} = \frac{1}{2}(e_a + e_b + e_c + e_d).$$

We will denote this ring with $\mathcal{O}$. $\mathbb{O}(\mathbb{Z})$ is also called the set of *Gravesian Octonion integers*, the octonions with all coordinates in $\mathbb{Z}$.

Let $w = \frac{1}{2}\left(1 + \sum_{i=2}^{8} e_i\right) \in \mathcal{O}$, be an octonion integer and let $\mathbb{V} = \{a + bw \ / \ a, b \in \mathbb{Z}\}$. We note that $\mathbf{n}(w) = 2$ and $w^2 - w + 2 = 0$. Since octonion algebra is a power associative algebra, it results that $\mathbb{V}$ is an associative and a commutative ring and $\mathbb{V} \subset \mathcal{O}$.

Remark 4.4.1. For $x \in \mathbb{V}$, the following properties are equivalent:
i) x is invertible in the algebra $\mathbb{V}$.
ii) $\mathbf{n}(x) = 1$.
iii) $x \in \{\pm 1\}$.

Definition 4.4.2. The octonion $x \in \mathbb{V}$ is *prime* in $\mathbb{V}$ if x is not an invertible element in $\mathbb{V}$ and if $x = ab$, then a or b is an invertible element in $\mathbb{V}$.

Proposition 4.4.3. *If $x, y \in \mathbb{V}$, $y \neq 0$, then there are $z, v \in \mathbb{V}$ such that $x = zy + v$, with $\mathbf{n}(v) < \mathbf{n}(y)$.*

Proof. In this proof, we will use some ideas given in [Da, Sa, Va; 03], Proposition 2.1.2. Since $y \neq 0$, we have that $\frac{x}{y} = a + bw, a, b \in \mathbb{R}$. Let $m, n \in \mathbb{Z}$ such that $|a - m| \leq \frac{1}{2}$ and $|b - n| \leq \frac{1}{2}$. Let $z = m + nw \in \mathbb{V}$ and $v = y\left[(a - m) + (b - n)w\right]$. It results that $\frac{x}{y} = z + \frac{v}{y}$, therefore $x = zy + v$ and $v = x - zy$. From here, we have that $v \in \mathbb{V}$. If $|a - m| = \frac{1}{2}$ and $|b - n| = \frac{1}{2}$, we have $v = y\frac{1}{2}(1 + w)$. Therefore $x = (z + 1)y + v', v' = v - y$ and $v' = y\frac{1}{2}(-1 + w)$. We have $\mathbf{n}(v') = \frac{1}{4}\mathbf{n}(y)\left(\frac{1}{4} + 7\frac{1}{4}\right) = \frac{1}{2}\mathbf{n}(y) < \mathbf{n}(y)$. It results that $x = (z + 1)y + v'$. Then, we suppose that or $|a - m| < \frac{1}{2}$ or $|b - n| < \frac{1}{2}$ or both.We obtain that
$\mathbf{n}(y)\left[\left[(a - m) + \frac{1}{2}(b - n)\right]^2 + \frac{7}{4}(b - n)^2\right] < \frac{16}{16}\mathbf{n}(y) = \mathbf{n}(y)$.□

Remark 4.4.3. Let $x = a + bw \in \mathbb{V}$. We have that
$\mathbf{n}(x) = x\overline{x} = (a + bw)(a + b\overline{w}) = a^2 + ab + 2b^2 = \left(a + \frac{b}{2}\right)^2 + 7\frac{b^2}{4} = A^2 + 7B^2$.

Proposition 4.4.5. ([Co; 89]) *Let $p \in \mathbb{N}$ be a prime number. There are integers a, b such that $p = a^2 + ab + 2b^2$ if $p = 7k + 1, k \in \mathbb{Z}$.*□

Definition 4.4.6. With the above notations, let $\pi = x + yw$ be a prime integer in $\mathbb{V}$ and v_1, v_2 be two elements in $\mathbb{V}$. If there is $v \in \mathbb{V}$ such that $v_1 - v_2 = v\pi$, then v_1, v_2 are called *congruent modulo* π and it is denoted $v_1 \equiv v_2 \ mod\ \pi$.

Proposition 4.4.7.

i) The above relation is an equivalence relation on $\mathbb{V}$. The set of equivalence classes is denoted by $\mathbb{V}_\pi$ and is called the residue classes field of $\mathbb{V}$ modulo π.

ii) $\mathbb{V}_\pi$ is a field isomorphic to $\mathbb{Z}/p\mathbb{Z}$, $p = \mathbf{n}(\pi), p$ a prime number.

Proof. i) We will denote the elements from $\mathbb{V}_\pi$ in bold. If $v_1 \equiv v_2 \ mod\ \pi$ and $v_2 \equiv v_3 \ mod\ \pi$ then there are $v, v' \in \mathbb{V}$ such that $v_1 - v_2 = v\pi$ and $v_2 - v_3 = v'\pi$. It results that $v_1 - v_3 = (v + v')\pi$, therefore the transitivity holds.

ii) For $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{V}_\pi$, we define $\mathbf{v}_1 + \mathbf{v}_2 = (v_1 + v_2) mod\ \pi$ and $\mathbf{v}_1 \cdot \mathbf{v}_2 = (v_1 v_2) mod\ \pi$. These multiplications are well defined. Indeed, if $v_1 \equiv v_1' \ mod\ \pi$ and $v_2 \equiv v_2' \ mod\ \pi$, it results that $v_1 - v_1' = u\pi, v_2 - v_2' = u'\pi, u, u' \in \mathbb{V}$, therefore $(v_1 + v_2) - (v_1' + v_2') = (u + u')\pi$. From Proposition 4.4.3 and since $v_1 = v_1' + u\pi$, $v_2 = v_2' + u'\pi$, it results that $v_1 v_2 = v_1' v_2' + M_\pi$, with M_π a multiple of π.

Denoting in bold the equivalence classes from $\mathbb{Z}_p$, let f be the map

$$f : \mathbb{Z}_p \to \mathbb{V}_\pi,\ f(\mathbf{m}) = (m+\pi)\ mod\ \pi,\ \text{where } m \in \mathbf{m}. \qquad (4.4.1.)$$

Map f is well defined, since if $m \equiv m'\ mod\ p$ we have $(m+\pi)-(m'+\pi) = m-m' = pq = \pi\overline{\pi}q, q \in \mathbb{Z}$, therefore $(m+\pi) \equiv (m'+\pi)\ mod\ \pi$.

Since $1 = v_1\pi + v_2\overline{\pi}$, (see [Da, Sa,Va; 03], Proposition 2.1.4 and Proposition 2.1.5.) if $f(\mathbf{m}) = v, v = (m+\pi)\ mod\ \pi \in \mathbb{V}_\pi$, we define $f^{-1}(v) = \overline{m}(v_1\pi) + m(v_2\overline{\pi})$ and $\overline{m}(v_1\pi) + m(v_2\overline{\pi}) = \overline{m}(v_1\pi) + m(1-v_1\pi) = m$.

Map f is a ring morphism. Indeed, $f(\mathbf{m}) + f(\mathbf{m}') = (m+\pi)mod\pi + (m'+\pi)mod\ \pi = (m+m'+\pi)mod\ \pi = f(\mathbf{m}+\mathbf{m}')$ and
$f(\mathbf{m})\, f(\mathbf{m}') = (m+\pi)(m'+\pi)mod\pi =$
$=\left(mm' + (m+m')\pi + \pi^2\right)mod\ \pi = (mm'+\pi)mod\ \pi$. We obtain that $\mathbb{V}_\pi$ is isomorphic to $\mathbb{Z}_p$.□

Remark 4.4.8. The field $\mathbb{V}_\pi$ has the property that if $x, y \in \mathbb{V}_\pi$, then there are $z, v \in \mathbb{V}_\pi$ such that $x = zy + v$, with $\mathbf{n}(v) < \mathbf{n}(y)$.

Remark 4.4.9.

1) $\mathbb{O}(\mathbb{Z})_\pi$ has $\mathbf{n}(\pi)^4$ elements (see [Ma,Be, Ga; 09], Theorem 25).

2) From Proposition 4.4.7 and from Remark 4.4.8, we have that for $v_i, v_j \in \mathbb{V}_\pi, i, j \in \{1, 2, ..., p-1\}$, $v_i + v_j = v_k$ if and only if $k = i + j\ mod\ p$ and $v_i \cdot v_j = v_k$ if and only if $k = i \cdot j\ mod\ p$. From here, with the above notations, we have the following labelling procedure:

i) Let $\pi \in \mathbb{V}$ be a prime, with $\mathbf{n}(\pi) = p, p$ a prime number, $\pi = a + bw, a, b \in \mathbb{Z}$.

ii) Let $s \in \mathbb{Z}$ be the only solution to the equation $a + bx = 0\ mod p,\ x \in \{0, 1, 2, ..., p-1\}$.

iii) For $k \in \mathbb{Z}$, let $\mathbf{k} \in \mathbb{Z}_p$ be its equivalence class. The element $\mathbf{k} \in \mathbb{Z}_p$ is the label of the element $v = m + nw \in \mathbb{V}_p$ if $m + ns = k\ mod\ p$ and $\mathbf{n}(v)$ is minimum.

The above Remark generalizes and adapts Theorem 1 and the Labeling procedure from [Ne, In, Fa, Pa; 01] to octonions**.**

3) This labelling procedure is nothing else than the map $\alpha + \beta w \longmapsto \alpha - \frac{a}{b}\beta\ mod\ p$ which is immediately induced by the reduction map of the integer ring of

$\mathbb{Q}\left(\sqrt{-7}\right)$ reduced modulo a prime ideal $\mathcal{P} = (a + bw, p)$ (see [Ni, Hi; 08]). We will use this algorithm in the next section to provide words having minimum Cayley-Dickson weight.

Using the above labelling procedure, we will provide an algorithm to see how we can find the representative of the class containing a given element of $\mathbb{V}$, therefore how we can find the elements the field $\mathbb{V}_\pi$.

The Algorithm.

1. Let $\pi \in \mathbb{V}$ be a prime, $\pi = a + bw, a, b \in \mathbb{Z}$, with $\mathbf{n}(\pi) = p, p$ a prime positive number.

2. Let $s \in \mathbb{Z}$ be the only solution to the equation $a + bx = 0 \ mod \ p, \ x \in \{0, 1, 2, ..., p-1\}$.

3. Let $q = \left[\frac{p-1}{2}\right] \in \mathbb{N}$, where [] denotes the integer part.

4. Let $k \in \mathbb{Z}$ and $\mathbf{k} \in \mathbb{Z}_p$ be its equivalence class modulo p.

5. For all integers $\alpha, \beta \in \{-q-1, ..., q\}$, let $c = (\alpha + s\beta) \ mod \ p$ and $d = (\alpha + \frac{\beta}{2})^2 + \frac{7}{4}\beta^2$. We will compute c and d.

6. If $d < p$ and $c = k$, then we find the pairs (α, β) such that $\mathbf{k}$ is the label of the element $\alpha + \beta w \in \mathbb{V}_\pi$, that means $\alpha + \beta s = k \ mod \ p$ and $\mathbf{n}(\alpha + \beta w)$ is minimum. If there are more than two pairs satisfying the last condition, then we will choose that pair such that $|\alpha| + |\beta| \leq |a| + |b|$. If there are more than two pairs satisfying the last inequality, then we will randomly choose one of them.

Even though these calculation results do not depend on the chosen software, we will use MAPLE to give an example for the above algorithm.

Example 4.4.10. Let $p = 29$ and $\pi = -1 + 4w$, with $\mathbf{n}(\pi) = 29$, therefore $a = -1, b = 4, q = 14$. With MAPLE, we find first that $s = 22$.We provide a representative system of $\mathbb{V}_\pi$, with the below small MAPLE procedure. For $k = 3$, we get:

```
for i from -15 to 14 do
for j from -15 to 14 do
c := (22*j+i)mod 29; d :=(7/4)*j^2+(i+(1/2)*j)^2;
if d < 29 and c = 3 then print(i, j);fi;od;od;
```

```
                                    -5, 3
```

```
-4, -1
 3, 0
```

In this case, we have three solutions: $-4-w, -5+3w$ and 3. Since $\mathbf{n}(-4-w)=23, \mathbf{n}(-5+3w)=28$ and $\mathbf{n}(3)=9$, we choose $c=3$, with the label $\mathbf{k}=\mathbf{3}$. For $k=4$, we get:

```
for a from -15 to 14 do
for b from -15 to 14 do
c := (22*b+a)mod 29; d := (7/4)*b^2+(a+(1/2)*b)^2;
if d < 29 and c = 4 then print(a, b);fi;od;od;
                                    -4, 3
                                    -3, -1
                                     4, 0
```

Since $\mathbf{n}(-4+3w)=22$ and $\mathbf{n}(-3-w)=\mathbf{n}(4)=16$, the last two solutions are good. We will chose $c=-3-w$, with the label $\mathbf{k}=\mathbf{4}$. For $k=6$, we get:

```
for a from -15 to 14 do
for b from -15 to 14 do
c := (22*b+a)mod 29; d := (7/4)*b^2+(a+(1/2)*b)^2;
if d < 29 and c = 6 then print(a, b);fi;od;od;
                                    -2, 3
                                    -1, -1
```

We obtain $c=-2+3w$ and $c=-1-w$. Since $\mathbf{n}(-2+3w)=16$ and $\mathbf{n}(-1-w)=2$, we will choose $c=-1-w$ with the label $\mathbf{k}=\mathbf{6}$.

It results:
$\mathbb{V}_\pi=\{0,1,2,3,-3-w,-2-w,-1-w,-w,1-w,2-w,$
$3-w,4-w,-2w-2,2w-2,-2w,-2w+1,-2w+2,$
$2+2w,w-4,w-3,w-2,w-1,w,1+w,2+w,3+w,-3,-2,-1\}$, with labels $\{\mathbf{0},\mathbf{1},\mathbf{2},...,\mathbf{27},\mathbf{28}\}$, in this order.

Codes over $\mathbb{V}_\pi$

Using ideas from the above definitions and generalizing the Hurwitz weight from [Gu; 13], we define the *Cayley-Dickson weight*, denoted d_C. Let π be a prime in $\mathbb{V}$, $\pi = a+bw$. Let $x \in \mathbb{V}$, $x = a_0+b_0w$. The *Cayley-Dickson weight* of x is defined as $w_C(x) = |a_0|+|b_0|$, where $x = a_0+b_0w \ mod\ \pi$, with $|a_0|+|b_0|$ minimum.

The *Cayley-Dickson distance* between $x, y \in \mathbb{V}_\pi$ is defined as

$$d_C(x,y) = w_C(x-y).$$

We will prove that d_C is a metric. Indeed, for $x, y, z \in \mathbb{V}_\pi$, we have $d_C(x,y) = w_C(\alpha_1) = |a_1|+|b_1|$, where $\alpha_1 = x-y = a_1+b_1 \ mod\ \pi$ is an element in $\mathbb{V}_\pi$ and $|a_1|+|b_1|$ is minimum.
$d_C(y,z) = w_C(\alpha_2) = |a_2|+|b_2|$, where $\alpha_2 = y-z = a_2+b_2 \ mod\ \pi$ is an element in $\mathbb{V}_\pi$ and $|a_2|+|b_2|$ is minimum.
$d_C(x,z) = w_C(\alpha_3) = |a_3|+|b_3|$, where $\alpha_3 = x-z = a_3+b_3 \ mod\ \pi$ is an element in $\mathbb{V}_\pi$ and $|a_3|+|b_3|$ is minimum.
We have $x-y = \alpha_2+\alpha_3 \ mod\ \pi$. It results that $w_C(\alpha_2+\alpha_3) \geq w_C(\alpha_1)$ since $w_C(\alpha_1) = |a_1|+|b_1|$ is minimum.

Remark 4.4.11. The maximum Cayley-Dickson distance $d_{C_{\max}}$ has the property that $d_{C_{\max}} \leq |a|+|b|$, with $\pi = a+bw$.

Remark 4.4.12. i) Since the Octonion algebra is alternative, due to Artin's Theorem (see [Sc; 66]), each two nonzero different elements generate an associative algebra. From here, for $x, y \in \mathbb{O}(\mathbb{R})$, we have that $x^m(x^n y) = x^{m+n}y$, for all $m, n \in \mathbb{Z}$.

ii) Hereafter, we assume that π is a prime in $\mathbb{V}$ and $\mathbf{n}(\pi) \equiv 1 \ mod\ 7$ such that there are α_1, α_2 two primitive elements (of order $p-1$) in $\mathbb{V}_\pi$, with the properties $\alpha_1^{\frac{p-1}{7}} = w$ or $\alpha_2^{\frac{p-1}{7}} = -w$. Let $\alpha \in \{\alpha_1, \alpha_2\}$. We will consider codes of length $n = \frac{p-1}{7}$.

Let $\mathcal{C}$ be the code given by the parity-check matrix H,

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & ... & \alpha^{n-1} \\ 1 & \alpha^8 & \alpha^{16} & ... & \alpha^{8(n-1)} \\ ... & ... & ... & ... & ... \\ 1 & \alpha^{7k+1} & \alpha^{2(7k+1)} & ... & \alpha^{(7k+1)(n-1)} \end{pmatrix}, \tag{4.4.2.}$$

with $k < n$. We know that c is a codeword in $\mathcal{C}$ if and only if $Hc^t = 0$. From here, if we consider the associate code polynomial $c(x) = \sum_{i=0}^{n-1} c_i x^i$, we have that $c\left(\alpha^{7l+1}\right) = 0, l \in \{0, 1, ..., k\}$. We consider the polynomial $g(x) = (x-\alpha)\left(x-\alpha^8\right)...\left(x-\alpha^{7k+1}\right)$. Since the elements $\alpha, \alpha^8, ..., \alpha^{7k+1}$ are distinct, from [Li, Xi; 04], Lemma 8.1.6, we have that $c(x)$ is divisible by the generator polynomial $g(x)$. Since $g(x) \ / \ (x^n \pm w)$, $g(x)$ is the generator polynomial of the code $\mathcal{C}$, it results that $\mathcal{C}$ is a principal ideal in the ring $\mathbb{V}_\pi \ / \ (x^n \pm w)$.

Supposing that a codeword polynomial $c(x)$ is sent over the channel and the error $e(x)$ occurs, it results that the received polynomial is $r(x) = c(x) + e(x)$. The vector corresponding to the polynomial $r(x) = c(x) + e(x)$ is $r = c + e$ and *the syndrome* of r is $S = Hr^t$, where H is the above parity-check matrix.

Theorem 4.4.13. *We consider $\mathcal{C}$ a code defined on $\mathbb{V}_\pi$ by the parity check matrix*

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & ... & \alpha^{n-1} \end{pmatrix}. \tag{4.4.3.}$$

Code $\mathcal{C}$ is able to correct all errors of the form $e(x) = e_t x^t$, with $0 \leq w_C(e_t) \leq 1$ and any errors of the form $e(x) = e_t x^t$, with $w_C(e_t) = 3, e_t = \pm w^2$.

Proof. Let $r(x) = c(x) + e(x)$ be the received polynomial, with $c(x)$ the codeword polynomial and $e(x) = e_t x^t$ denoting the error polynomial with $0 \leq w_C(e_t) \leq 1$. Using Remark 4.4.12 ii), since $\alpha^n = w$, or $\alpha^n = -w$ and $w^2 = w - 2, w_C\left(w^2\right) = 3$, it results that $e_t = \alpha^{nl}$. We have the syndrome $S = \alpha^{t+nl} = \alpha^L$, with $t, L \in \mathbb{Z}, 0 \leq t, L \leq n-1$. If we reduce L modulo n, we obtain t, the location of the error, and from here, $l = \frac{L-t}{n}$ and α^{nl}, the value of the error. □

Example 4.4.14. With the above notation, let $\pi = 7 + 2w, p = 71, n =$

$10, w = \alpha^{10}$ and the parity check matrix

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 \end{pmatrix}.$$

Supposing that the received vector is $r = (w, 1, w-1, 1, 1, 0, 0, 0, 1, 1)$, we compute the syndrome. We easily find that $s = 32$ is the label for the element w.

From the below MAPLE procedures and The Algorithm from the above, we obtain the syndrome.

```
print(‘pi=7+2w‘);A:=(-7*2^(-1))mod 71;
for a to 71 do b :=a^10 mod 71; if b = 32 then print(a);fi;od;
(9^10+9+9^22+9^2+9^3+9^4+9^8+9^9)mod 71;9^14 mod 71;
 pi=7+2w, 32 9 11 12 16 26 45 55 59 60 62 5 5

for a from -36 to 35 do for b from -36 to 35 do
c :=(32*b+a)mod 71; d := (7/4)*b^2+(a+(1/2)*b)^2;
if d < 71 and c = 5 then print(a, b);fi;od;fi;od;
                      -2  -2
                       5  0
```

We get $\alpha = -2-2w$ with the label 9. It results that $S = Hr^t = -2-2w = \alpha^{14}$ *mod* π. We get $L = 14$, therefore the location of the error is $t = L$ *mod* $10 = 4$ *mod* 10. The value is $w = \alpha^{14-4} = \alpha^{10}$ *mod* π, therefore the corrected vector is
$c{=}r - (0, 0, 0, 0, w, 0, 0, 0, 0, 0){=}(w, 1, w-1, 1, 1-w, 0, 0, 0, 1, 1)$ *mod* π.

Theorem 4.4.15. *We consider* $\mathcal{C}$ *a code given by the parity-check matrix*

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & ... & \alpha^{n-1} \\ 1 & \alpha^8 & \alpha^{16} & ... & \alpha^{8(n-1)} \end{pmatrix}. \tag{4.4.4.}$$

Then $\mathcal{C}$ *can correct any errors of the form* $e(x) = e_i x^i$, $0 \leq i \leq n-1$, *with* $e_i \in \mathbb{V}_\pi$.

Proof. Let $r(x) = c(x) + e(x)$ be the received polynomial, with $c(x)$ the codeword polynomial and $e(x) = e_i x^i$ denoting the error polynomial with $e_i \in \mathbb{V}_\pi$. Then, the corresponding vector of the polynomial $r(x)$ is $r = c + e$

and we will compute the syndrome S of r. We have $e_i = \alpha^q, 0 \leq q \leq 7n-1$. Therefore the syndrome is

$$S{=}Hr^t{=}\begin{pmatrix} s_1 = \alpha^{i+q} = \alpha^{M_1} \\ s_8 = \alpha^{8i+q} = \alpha^{M_2} \end{pmatrix}.$$

We obtain $a^{i+q-M_1} = 1$, with $i+q = M_1 \ mod(p-1)$ and $\alpha^{8i+q-M_2} = 1$, with $8i+q = M_2 \ mod(p-1)$. We get $7i = (M_2 - M_1) \ mod(p-1)$, then the unique solution of the system is $i = \frac{M_2-M_1}{7} \ mod \ n$ and $q = (M_1 - i) \ mod(p-1)$. In this way, we can find the location and the value of the error.□

Example 4.4.16. Let $\pi = -1+4w, p = 29, n = 4, \alpha = 1-w, -w = \alpha^4$ *mod* π, and the parity check matrix

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & \alpha^8 & \alpha^{16} & \alpha^{24} \end{pmatrix}.$$

Supposing that the received vector is $r = \left(\alpha, \alpha^2, 1, \alpha^3\right) = (1-w, -1-w, 1, -3+w)$ and using MAPLE software, we compute the syndrome. It results that

$$S = Hr^t = \begin{pmatrix} s_1 = \alpha^7 \\ s_8 = \alpha^7 \end{pmatrix}.$$

The location of the error is $i = \frac{7-7}{7} = 0 \ mod \ 4$ and the value of the error is $\alpha^{7-0} = \alpha^7 = 17 = (2+2w) \ mod \ \pi$. Therefore the corrected vector is
$c = r - (2+2w, 0, 0, 0) = (-1-3w, -1-w, 1, -3+w) mod \ \pi =$
$= (-2+w, -1-w, 1, -3+w)$.

Theorem 4.4.17. *We consider* $\mathcal{C}$ *a code defined by the parity-check matrix*

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & ... & \alpha^{n-1} \\ 1 & \alpha^8 & \alpha^{16} & ... & \alpha^{8(n-1)} \\ 1 & \alpha^{15} & \alpha^{30} & ... & \alpha^{15(n-1)} \end{pmatrix}. \qquad (4.4.5.)$$

Then $\mathcal{C}$ *can find the location and can correct errors of the form* $e(x) = e_i x^i$, $0 \leq i \leq n-1$, *with* $e_i \in \mathbb{V}_\pi$, *or can only correct errors of the above mentioned form.*

Proof. Using notations from the above Theorem, we have $e_i = \alpha^q, 0 \leq q \leq 7n-1$. Therefore the syndrome is

$$S{=}Hr^t{=}\begin{pmatrix} s_1 = \alpha^{i+q} = \alpha^{M_1} \\ s_8 = \alpha^{8i+q} = \alpha^{M_2} \\ s_{15} = \alpha^{15i+q} = \alpha^{M_3} \end{pmatrix}.$$

Since the rank of the matrix (4.4.5) is 3, then this system always has a solution. We obtain $a^{i+q-M_1} = 1$, with $i+q = M_1 \ mod(p-1)$, $\alpha^{8i+q-M_2} = 1$, with $8i+q = M_2 \ mod(p-1)$, $\alpha^{15i+q-M_3} = 1$, with $15i+q = M_3 \ mod(p-1)$. We can find the location of the error if $7i = (M_2 - M_1) \ mod(p-1)$ and $7i = (M_3 - M_2) \ mod(p-1)$ or, equivalently, $i = \frac{M_2-M_1}{7} \ mod \ n = \frac{M_3-M_2}{7}$ $mod \ n$ and the value of the error e_i if
$(M_1 - i) \ mod(p-1) = (M_2 - 8i) \ mod(p-1) = (M_3 - 15i) \ mod(p-1)(= q)$. □

Example 4.4.18.

1) Let $\pi = -1 + 4w, p = 29, n = 4, \alpha = 1 - w, -w = \alpha^4 \ mod \ \pi$, and the parity check matrix

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & \alpha^8 & \alpha^{16} & \alpha^{24} \\ 1 & \alpha^{15} & \alpha^{30} & \alpha^{45} \end{pmatrix}.$$

We suppose that the received vector is $r = (1-w, -1-w, 1, -3+w) =$
$= \left(\alpha, \alpha^2, 1, \alpha^3\right)$. Using MAPLE software, we compute the syndrome. It results that

$$S = Hr^t = \begin{pmatrix} s_1 = \alpha^7 = \alpha^{i+q} \\ s_8 = \alpha^7 = \alpha^{8i+q} \\ s_{15} = \alpha^{27} = \alpha^{15i+q} \end{pmatrix}.$$

The location of the error is $i = \frac{7-7}{7} = \frac{27-7}{7} = 0 \ mod \ 4$. We can not find the value of the error since $\alpha^{7-0} = \alpha^7 = 17 = (2+2w) \ mod \ \pi$ is different from $\alpha^{27-0} = \alpha^{27} = 11 = (4-w) \ mod \ \pi$.

2) In the same conditions, supposing that the received vector is
$r = \left(1, \alpha^3, 1, \alpha^2\right) = (1, -3+w, 1, -1-w)$ and using MAPLE, the syndrome is

$$S = Hr^t = \begin{pmatrix} s_1 = \alpha^{21} = \alpha^{i+q} \\ s_8 = \alpha^{11} = \alpha^{8i+q} \\ s_{15} = \alpha^{19} = \alpha^{15i+q} \end{pmatrix}.$$

We can't find the location and the value of the error, since $2 = \frac{11-21}{7} \ mod \ 4 \neq \frac{19-11}{7} \ mod \ 4 = 0$.

3) If we suppose that the received vector is $r = (5,0,0,0) = (-2-w,0,0,0) = \left(\alpha^{26},0,0,0\right)$, the syndrome is

$$S = Hr^t = \begin{pmatrix} s_1 = \alpha^{26} \\ s_8 = \alpha^{26} \\ s_{15} = \alpha^{26} \end{pmatrix}.$$

The location of the error is 0 and the value of the error is 5. Therefore the corrected vector is $(0,0,0,0)$.

Theorem 4.4.19. *We consider $\mathcal{C}$ a code defined by the parity-check matrix*

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & ... & \alpha^{n-1} \\ 1 & \alpha^8 & \alpha^{16} & ... & \alpha^{8(n-1)} \\ 1 & \alpha^{15} & \alpha^{30} & ... & \alpha^{15(n-1)} \\ 1 & \alpha^{22} & \alpha^{44} & ... & \alpha^{22(n-1)} \end{pmatrix}. \qquad (4.4.6.)$$

Then $\mathcal{C}$ can correct errors of the form $e(x) = e_i x^i + e_j x^j$, $0 \leq i,j \leq n-1$, with $e_i, e_j \in \mathbb{V}_\pi$.

Proof. We will prove this in the general case, when we have two errors. We have $e_i = \alpha^q \neq 0$ and $e_j = \alpha^t \neq 0, q, t \in \mathbb{Z}$. We obtain the syndrome:

$$S{=}Hr^t{=}\begin{pmatrix} s_1 = \alpha^{i+q} + \alpha^{j+t} \\ s_8 = \alpha^{8i+q} + \alpha^{8j+t} \\ s_{15} = \alpha^{15i+q} + \alpha^{15j+t} \\ s_{22} = \alpha^{22i+q} + \alpha^{22j+t} \end{pmatrix}.$$

Denoting $\alpha^{i+q} = A$ and $\alpha^{j+t} = B$, it results that

$$S{=}Hr^t{=}\begin{pmatrix} s_1 = A + B \\ s_8 = \alpha^{7i}A + \alpha^{7j}B \\ s_{15} = \alpha^{14i}A + \alpha^{14j}B \\ s_{22} = \alpha^{21i}A + \alpha^{21j}B \end{pmatrix}. \qquad (4.4.7.)$$

If the system (4.4.7) admits only one solution, then the code $\mathcal{C}$ can correct two errors. First, we will prove the following Lemma.

Lemma. *With the above notations, if we have two errors, we obtain* $\alpha^{7i} \neq \alpha^{7j}, 0 \leq i, j \leq n-1$ *and* $s_1 s_{15} \neq s_8^2$.

Proof. If $\alpha^{7i} = \alpha^{7j}$, then $\alpha^{7(i-j)} = 1$ and $7n \ / \ 7(i-j)$, which is false. Supposing that $s_1 s_{15} - s_8^2 = 0$, we have $s_1 s_{15} = s_8^2$. For $x = \alpha^{i+q}$, it results that $\alpha^{14i} s_1 x + \alpha^{14j} s_1^2 - \alpha^{14j} s_1 x = \left(\alpha^{7i} - \alpha^{7j}\right)^2 x^2 + \alpha^{14j} s_1^2 + 2\alpha^{7j}\left(\alpha^{7i} - \alpha^{7j}\right) s_1 x$. We get $\left(\alpha^{7i} - \alpha^{7j}\right)^2 x^2 + 2\alpha^{7i+7j} s_1 x - \alpha^{14i} s_1 x - \alpha^{14j} s_1 x = 0$. From here, $x = 0$ or $x = \frac{-2\alpha^{7i+7j} s_1 + \alpha^{14i} s_1 + \alpha^{14j} s_1}{(\alpha^{7i} - \alpha^{7j})^2} = s_1$. If we have $x = \alpha^{i+q} = s_1$, this implies $\alpha^{j+t} = 0$, which is false.

We now return to the proof of the Theorem and we are under conditions $\alpha^{7i} \neq \alpha^{7j}, 0 \leq i, j \leq n-1$ and $s_1 s_{15} \neq s_8^2$. For $B = s_1 - A$, it results that

$A\left(\alpha^{7i} - \alpha^{7j}\right) = s_8 - s_1 \alpha^{7j}$
$A\left(\alpha^{14i} - \alpha^{14j}\right) = s_{15} - s_1 \alpha^{14j}$
$A\left(\alpha^{21i} - \alpha^{21j}\right) = s_{22} - s_1 \alpha^{21j}$. We obtain

$$s_{15} - s_1 \alpha^{14j} = \left(s_8 - s_1 \alpha^{7j}\right)\left(\alpha^{7i} + \alpha^{7j}\right)$$

and

$$s_{22} - s_1 \alpha^{21j} = \left(s_8 - s_1 \alpha^{7j}\right)\left(\alpha^{14i} + \alpha^{7i}\alpha^{7j} + \alpha^{14j}\right).$$

Denoting $\alpha^{7i} + \alpha^{7j} = s_7$ and $\alpha^{7i}\alpha^{7j} = p_7$, we have

$$s_{15} - s_8 s_7 + p_7 s_1 = 0$$

and

$$\left(s_8 - s_1 \alpha^{7j}\right)\left(s_7^2 - p_7\right) = s_{22} - s_1 \alpha^{21j}.$$

It results that

$$p_7 = \frac{s_8 s_7 - s_{15}}{s_1}$$

and

$$s_7(s_1 s_{15} - s_8^2) = s_1 s_{22} - s_8 s_{15}.$$

We obtain

$$s_7 = \frac{s_1 s_{22} - s_8 s_{15}}{s_1 s_{15} - s_8^2}$$

and for p_7 we get

$$p_7 = \frac{s_8 s_{22} - s_{15}^2}{s_1 s_{15} - s_8^2}.$$

From here, by solving the equation $x^2 - s_7 x + p_7 = 0$, we find the locations and the values of the errors. □

Example 4.4.20.

1) Let $\pi = -1 + 4w, p = 29, n = 4, \alpha = 1 - w, -w = \alpha^4 \ mod\ \pi$, and the parity check matrix

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & \alpha^8 & \alpha^{16} & \alpha^{24} \\ 1 & \alpha^{15} & \alpha^{30} & \alpha^{45} \\ 1 & \alpha^{22} & \alpha^{44} & \alpha^{66} \end{pmatrix}.$$

Supposing that the received vector is
$r = \left(1, \alpha^3, 1, \alpha^2\right) = (1, -3 + w, 1, -1 - w)$ and using once again MAPLE, the syndrome is

$$S{=}Hr^t{=} \begin{pmatrix} s_1 = \alpha^{21} \\ s_8 = \alpha^{11} \\ s_{15} = \alpha^{19} \\ s_{22} = \alpha^{20} \end{pmatrix}.$$

We obtain

$$s_7 = \frac{s_1 s_{22} - s_8 s_{15}}{s_1 s_{15} - s_8^2} = (2 + w)\ mod\ \pi$$

and

$$p_7 = \frac{s_8 s_{22} - s_{15}^2}{s_1 s_{15} - s_8^2} = \ 1\ mod\ \pi\ .$$

Equation $x^2 - (2 + w)x + 1 = 0$ has no roots in $\mathbb{V}_\pi$, therefore we can not find the locations and the values of the errors.

2) If the received vector is $r = (5, 0, 1, 0) = (-2 - w, 0, 1, 0) = \left(\alpha^{26}, 0, 1, 0\right)$, the syndrome is

$$S{=}Hr^t{=} \begin{pmatrix} s_1 = \alpha^{27} = 11 \\ s_8 = \alpha^{14} = 28 \\ s_{15} = \alpha^{27} = 11 \\ s_{22} = \alpha^{14} = 28 \end{pmatrix}.$$

We get $s_7 = 0$ and $p_7 = -1$ and $\alpha^{7i} = 1, \alpha^{7j} = 28 \bmod \pi$. It results that $\alpha^i = 1, \alpha^j = 4 = \alpha^{10}$, then $i = 0$ and $j = 10 \bmod 4 = 2$. The errors are in positions 0 and 2. The corrected vector is $c = (4, 0-3, 0) = (-3-w, 0, -3, 0)$.

Remark 4.4.21. The above Theorems adapted and generalized Theorems 7,8,9,10,11,13,14,15 from [Ne, In, Fa, Pa; 01] and Theorems 4,5,6,7 from [Gu; 13] to octonions.

Remark 4.4.22. In this situation, when $p = 7k+1, k = 6l, l \in \mathbb{Z}$, and when the considered alphabets have the same cardinality, we note that the code rate of the codes defined on $\mathbb{V}_\pi$ can be better than in the case of the codes defined in [Gu; 13] on $\mathcal{R}_\pi$, but smaller than the codes defined on $\mathcal{H}_\pi$. Here $\mathcal{H}$ is the set of all Hurwitz integers, $\mathcal{R} = \{a + bw : a, b \in \mathbb{Z}\}, w = \frac{1}{2}(1 + i + j + k)$, with $\{1, i, j, k\}$ a basis in the Quaternion algebra and $\mathcal{R}_\pi$, $\mathcal{H}_\pi$ are the quotient rings modulo π, with π a prime quaternion. If $\mathcal{C}_1$ is a code over $\mathcal{R}_\pi$ of length $n_1 = \frac{p-1}{6}$, $\mathcal{C}_2$ a code over $\mathbb{V}_\pi$ of length $n_2 = \frac{p-1}{7}$, with $\mathbf{n}(\pi) = p$ and if $\mathcal{C}_1, \mathcal{C}_2$ have the same dimension k, we obtain that the rate $R_{\mathcal{C}_2}$ of the code $\mathcal{C}_2$ is always greater than the rate $R_{\mathcal{C}_1}$ of the code $\mathcal{C}_1$. Indeed, $R_{\mathcal{C}_2} = \frac{7k}{p-1}$ and $R_{\mathcal{C}1} = \frac{6k}{p-1}$. This difference appears more clearly in the case of very long codes.

In this section we have defined block codes over subsets of the Octonion integers and we have given decoding algorithms for these codes. Specifically, the alphabets considered are quotients of the subset of Octonion integers. Once the metric space has been stated, we present two code constructions: the first for one error correcting block codes and the second for double error correcting codes. Even if these constructions are standard, following the same techniques as the ones presented in [Ne, In, Fa, Pa; 01], by comparing these codes with some of the codes defined on Hurwitz integers as in [Gu; 13], we note that the code rate in the Octonions case can be better than in the Hurwitz case.

The above observation can be a good motivation to use the Octonion integers instead of Hurwitz integers for constructing such error correcting codes and can be considered as a first step in the study of codes over Octonions, which will lead readers to a new field.

4.5. Codes over subsets of algebras obtained by the Cayley-

Dickson process

In the following, we will extend the study of Integer Codes to codes over subsets of real algebras obtained by the Cayley-Dickson process. The results presented below, were obtained, by the author, in the paper [Fl; 16].This idea comes in a natural way, starting from same ideas developed by Huber in [Hu; 94], in which he regarded a finite field as a residue field of the Gaussian integer ring modulo a Gaussian prime, ideas extended to Hurwitz integers in [Gu; 13] and to a subset of the Octonions integers in [Fl; 15]. In this way, we can regard a finite field as a residue field modulo a prime element from $\mathbb{V}$, where $\mathbb{V}$ is a subset of an algebra $\mathbb{A}_t(\mathbb{R})$, where $\mathbb{A}_t(\mathbb{R})$ is a real algebra obtained by the Cayley-Dickson process and $\mathbb{V}$ has a commutative and associative ring structure. We obtain an algorithm, called the Main Algorithm, which allows us to find codes with a good rate. This algorithm offers more flexibility than other methods known until now. Keeping the proportions, the Main Algorithm is similar to the Lenstra's algorithm on elliptic curves compared with $p-1$ Pollard's algorithm. It is well known that for a prime p, the Lenstra's algorithm replaces the group $\mathbb{Z}_p^*$ with the group of the rational points of an elliptic curve $\mathcal{C}_1$ over $\mathbb{Z}_p$ and, if this algorithm failed, the curve will be replaced with another curve $\mathcal{C}_2$ over $\mathbb{Z}_p$ and we can retake the algorithm (see [Si, Ta; 92]).

In the case of the Main Algorithm, the algebra $\mathbb{A}_t(\mathbb{R})$ and w offer this kind of flexibility since, for the same prime p, these can be changed and the algorithm can be retaken.

In the following, we will consider $A_t = \left(\frac{\alpha_1,...,\alpha_t}{K}\right)$ the algebra obtained by the Cayley-Dickson process and for $\gamma_1 = ... = \gamma_t = -1$, we will denote it with $\mathbb{A}_t(\mathbb{R})$.

Let $B = \{1, e_2, ..., e_{2^t}\}$ be the a basis in $\mathbb{A}_t(\mathbb{R})$, where 1 is the unit. If $x = x_1 + \sum_{i=2}^{2^t} x_i e_i \in \mathbb{A}_t(\mathbb{R})$, then its *conjugate* is the element $\overline{x} = x_1 - \sum_{i=2}^{2^t} x_i e_i$ and

the *norm* of the element x is $\mathbf{n}(x) = x\overline{x} = \overline{x}x = \sum_{i=1}^{2^t} x_i^2$. The norm $\mathbf{n}$, in general, is not multiplicative, i.e. for $x, y \in \mathbb{A}_t(\mathbb{R})$, we have $\mathbf{n}(xy) \neq \mathbf{n}(x)\mathbf{n}(y)$. We remark that the norm is multiplicative if and only if the algebra has dimension less or equal to 8. (See [Sc; 66]). The *real part* of the element x is x_1 and its *vector part* is $\sum_{i=2}^{2^t} x_i e_i \in \mathbb{A}_t(\mathbb{R})$.

For example, if $t = 2$ and $\gamma_1 = \gamma_2 = -1$, we obtain the Quaternion division algebra, denoted by $\mathbb{Q}(\mathbb{R})$, for $t = 3$ and $\gamma_1 = \gamma_2 = \gamma_3 = -1$, we obtain the Octonion division algebra, denoted by $\mathbb{O}(\mathbb{R})$, and for $t = 4$ and $\gamma_1 = \gamma_2 = \gamma_3 = \gamma_4 = -1$, we obtain the Sedenion algebra, denoted by $\mathbb{S}(\mathbb{R})$. Due to the Hurwitz's Theorem, for $t \geq 4$, all obtained algebras are not division algebras (i.e. we can find $a, b \in \mathbb{A}_t(\mathbb{R})$, $a \neq 0, b \neq 0$, such that $ab = 0$).

Let $w = \alpha(1 + \sum_{i=2}^{2^t} e_i) \in \mathbb{A}_t(\mathbb{R}), \alpha \in \mathbb{R}$, and let $\mathbb{V} = \{a + bw \mid a, b \in \mathbb{Z}\}$ and $\mathbb{V}' = \{a + bw \mid a, b \in \mathbb{R}\}$. We note that $\mathbf{t}(x) = 2\alpha$, $\mathbf{n}(x) = 2^t\alpha^2$ and $w^2 - 2\alpha w + 2^t\alpha^2 = 0$. Since the algebra $\mathbb{A}_t(\mathbb{R})$ is a power associative algebra, it results that $\mathbb{V}$ and $\mathbb{V}'$ are associative and commutative rings. (See [Sc; 66]).

Remark 4.5.1. For $x \in \mathbb{V}$, we know that the following properties are equivalent:

i) x is an invertible element in the algebra $\mathbb{V}$.

ii) $\mathbf{n}(x) = 1$.

iii) $x \in \{\pm 1\}$.

An element $x \in \mathbb{V}$ is a *prime* element in $\mathbb{V}$ if x is not an invertible element in $\mathbb{V}$ and if $x = ab$, it results that a or b is an invertible element in $\mathbb{V}$.

Proposition 4.5.2. i) *For* $x, y \in \mathbb{V}'$, *we have* $\mathbf{n}(xy) = \mathbf{n}(x)\mathbf{n}(y)$.

ii) *The ring* $\mathbb{V}'$ *is a division ring.*

Proof. i) Denoting with $q = 2^t - 1$, let $x = a + bw$ and $y = c + dw$. We obtain

$\mathbf{n}(x)\mathbf{n}(y) = \left[(a + b\alpha)^2 + b^2\alpha^2 q\right]\left[(c + d\alpha)^2 + d^2\alpha^2 q\right] =$

$= \left(2ab\alpha + a^2 + b^2\alpha^2 + b^2 q\alpha^2\right)\left(2cd\alpha + c^2 + d^2\alpha^2 + d^2 q\alpha^2\right) = 2abc^2\alpha + 2a^2cd\alpha +$
$4abcd\alpha^2 + a^2c^2 + 2abd^2\alpha^3 + 2b^2cd\alpha^3 + 2abd^2q\alpha^3 + 2b^2cdq\alpha^3 + a^2d^2\alpha^2 + b^2c^2\alpha^2 +$
$b^2d^2\alpha^4 + a^2d^2q\alpha^2 + b^2c^2q\alpha^2 + 2b^2d^2q\alpha^4 + b^2d^2q^2\alpha^4.$

Computing $\mathbf{n}(xy)$, we get

$\mathbf{n}(xy) = \left[ac + (ad + bc)\alpha - \alpha^2 bd(q+1) + 2\alpha^2 bd\right]^2 + q\alpha^2 \left[ad + bc + 2\alpha bd\right]^2 =$
$2abc^2\alpha + 2a^2cd\alpha + 4abcd\alpha^2 + a^2c^2 + 2abd^2\alpha^3 + 2b^2cd\alpha^3 + 2abd^2q\alpha^3 + 2b^2cdq\alpha^3 +$
$a^2d^2\alpha^2 + b^2c^2\alpha^2 + b^2d^2\alpha^4 + a^2d^2q\alpha^2 + b^2c^2q\alpha^2 + 2b^2d^2q\alpha^4 + b^2d^2q^2\alpha^4.$

Therefore $\mathbf{n}(xy) = \mathbf{n}(x)\,\mathbf{n}(y)$.

ii) It results from i).

Remark 4.5.3. The above result is also true for all elements from the set $\mathbb{V}$.

In the following, we will consider $\alpha = \frac{1}{2^r}, r \geq t-1, t \geq 2$.

Proposition 4.5.4. *If $x, y \in \mathbb{V}$, $y \neq 0$, with $t \geq 2$, then there are $z, v \in \mathbb{V}$ such that $x = zy + v$ and $\mathbf{n}(v) < \mathbf{n}(y)$.*

Proof. Since $y \neq 0$, we have that y is an invertible element in $\mathbb{A}_t(\mathbb{R})$, therefore $\frac{x}{y} = a + bw, a, b \in \mathbb{R}$. Let $m, n \in \mathbb{Z}$ such that $|a - m| \leq \frac{1}{2}$ and $|b - n| \leq \frac{1}{2}$. For $z = m + nw \in \mathbb{V}$ and $v = y\left[(a-m) + (b-n)w\right]$, it results that $\frac{x}{y} = z + \frac{v}{y}$, therefore $x = zy + v$ and $v = x - zy$. From here, we have that $v \in \mathbb{V}$. Since $2^t \leq 2^{r+1}$, we have

$\mathbf{n}(v) = \mathbf{n}(y)\,\mathbf{n}((a-m) + (b-n)w) =$
$= \mathbf{n}(y)\left[\left[(a-m) + \frac{1}{2^r}(b-n)\right]^2 + \frac{2^t-1}{2^{2r}}(b-n)^2\right] \leq (\frac{(2^r+1)^2}{2^{2r+2}} + \frac{2^{r+1}-1}{2^{2r+2}})\mathbf{n}(y) =$
$= \frac{2^{2r}+2^{r+2}}{2^{2r+2}}\mathbf{n}(y) = \frac{2^r+2^2}{2^{r+2}}\mathbf{n}(y) < \mathbf{n}(y)$. □

Definition 4.5.6. With the above notations, let $\pi = x + yw$ be a prime integer in $\mathbb{V}$ and v_1, v_2 be two elements in $\mathbb{V}$. If there is $v \in \mathbb{V}$ such that $v_1 - v_2 = v\pi$, then v_1, v_2 are called *congruent modulo* π and we denote this by $v_1 \equiv v_2 \ mod\ \pi$.

Proposition 4.5.7. *The above relation is an equivalence relation on $\mathbb{V}$. The set of equivalence classes mod π is denoted by $\mathbb{V}_\pi$ and is called the residue classes of $\mathbb{V}$ modulo π.*

Proof. Denoting the elements from $\mathbb{V}_\pi$ in bold, if $v_1 \equiv v_2 \ mod\ \pi$ and $v_2 \equiv v_3 \ mod\ \pi$, then there are $v, v' \in \mathbb{V}$ such that $v_1 - v_2 = v\pi$ and $v_2 - v_3 = v'\pi$. It results that $v_1 - v_3 = (v + v')\pi$, therefore the transitivity holds. □

Proposition 4.5.8. *For each $x, y \in \mathbb{V}$, there is $\delta = (x, y)$, the greatest common divisor of x and y. We also have that there are γ and $\tau \in \mathbb{V}$, such that $\delta = \gamma x + \tau y$.*(**the Bézout's Theorem**).

Proof. We denote by $J = \{\gamma x + \tau y \mid \gamma, \tau \in \mathbb{V}\}$.We remark that if $z = \gamma' x + \tau' y \in J$ and $w \in \mathbb{V}$, we have $wz = (w\gamma')x + (w\tau')y \in J$. We consider $\delta_1 = \gamma_1 x + \tau_1 y \in J$, such that δ_1 has the norm $\mathbf{n}(\delta_1)$ minimum in J. We will prove that $\delta = \delta_1$.From Proposition 4.5.4, it results that $x = q_1\delta_1 + r_1$, with $\mathbf{n}(r_1) < \mathbf{n}(\delta_1), q_1, r_1 \in \mathbb{V}$ and $r_1 = x - q_1\delta_1 \in J$. Since $\mathbf{n}(r_1) < \mathbf{n}(\delta_1)$ and $\delta_1 \in J$ has minimum norm in J, we get $r_1 = 0$, therefore $\delta_1 \mid x$. In the same way, we will prove that $\delta_1 \mid y$. Since $\delta_1 = \gamma_1 x + \tau_1 y$, it results that each common divisor for x and y is a divisor for δ_1, therefore $\delta \mid \delta_1$ and finally $\delta = \delta_1$.□

The above proposition generalized to elements in $\mathbb{V}$ Proposition 2.1.4. from [Da, Sa, Va;03], with a similar proof.

Proposition 4.5.9. *$\mathbb{V}_\pi$ is a field isomorphic to $\mathbb{Z}/p\mathbb{Z}$, $p = \mathbf{n}(\pi)$, where p is a prime number.*

Proof.

For $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{V}_\pi$, we define $\mathbf{v}_1 + \mathbf{v}_2 = (v_1 + v_2) mod\ \pi$ and $\mathbf{v}_1 \cdot \mathbf{v}_2 = (v_1 v_2) mod\ \pi$. These multiplications are well defined. Indeed, if $v_1 \equiv v_1'\ mod\ \pi$ and $v_2 \equiv v_2'\ mod\ \pi$, it results that $v_1 - v_1' = u\pi, v_2 - v_2' = u'\pi, u, u' \in \mathbb{V}$, therefore $(v_1 + v_2) - (v_1' + v_2') = (u + u')\pi$. Since $v_1 = v_1' + u\pi$, $v_2 = v_2' + u'\pi$, we get $v_1 v_2 = v_1' v_2' + M_\pi$, with M_π a multiple of π.

Denoting in bold the equivalence classes from $\mathbb{Z}_p$, let f be the map

$$f : \mathbb{Z}_p \to \mathbb{V}_\pi,\ f(\mathbf{m}) = (m + \pi)\ mod\ \pi,\ \text{where } m \in \mathbf{m}. \qquad (4.5.1.)$$

The map f is well defined. Indeed, if $m \equiv m'\ mod\ p$ we have $(m + \pi) - (m' + \pi) = m - m' = pq = \pi\overline{\pi}q, q \in \mathbb{Z}$, therefore $(m + \pi) \equiv (m' + \pi)\ mod\ \pi$.

If $f(\mathbf{m}) = \mathbf{v}, \mathbf{v} = (m + \pi)\ mod\ \pi \in \mathbb{V}_\pi$, we define $f^{-1}(\mathbf{v}) = \mathbf{m}$.

The map f^{-1} is well defined. Indeed, if $\mathbf{v} = \mathbf{v}'$,it results $m \equiv m'\ mod\ \pi$, we have $m - m' = \pi v_3$ and $m - m' = \overline{\pi v_3}$, therefore $\pi \mid m - m'$ and $\overline{\pi} \mid m - m'$. We obtain $p \mid m - m'$ and $\mathbf{m} = \mathbf{m}'$.

The map f is a ring morphism. Indeed, $f(\mathbf{m}) + f(\mathbf{m}') = (m + \pi) mod\ \pi + (m' + \pi) mod\ \pi = (m + m' + \pi) mod\ \pi = f(\mathbf{m} + \mathbf{m}')$ and
$f(\mathbf{m}) f(\mathbf{m}') = (m + \pi)(m' + \pi) mod \pi =$

$=\left(mm' + (m+m')\,\pi + \pi^2\right) mod\ \pi = (mm' + \pi) mod\ \pi$. We obtain that $\mathbb{V}_\pi$ is isomorphic to $\mathbb{Z}_p$.□

Let $x = a + bw \in \mathbb{V}$, therefore we have $\mathbf{n}(x) = (a + b\alpha)^2 + q(b\alpha)^2$. For $q = 2^t - 1$ and for certain values of t, we know the form of some prime numbers, as we can see in the proposition below.

Proposition 4.5.10. ([Co; 89])
Let $p \in \mathbb{N}$ be a prime number.

1) *There are integers a, b such that $p = a^2 + 3b^2$ if and only if $p \equiv 1 (mod\ 3)$ or $p = 3$.*

2) *There are integers a, b such that $p = a^2 + 7b^2$ if and only if $p \equiv 1, 2, 4 (mod\ 7)$ or $p = 7$.*

3) *There are integers a, b such that $p = a^2 + 15b^2$ if and only if $p \equiv 1, 19, 31, 49 (mod\ 60)$.*□

The label Algorithm for $\mathbb{A}_t(\mathbb{R})$.

1. We will fix the elements t, α and therefore w.

2. We consider $\pi \in \mathbb{V}$ a prime element, $\pi = a + bw, a, b \in \mathbb{Z}$, such that $\mathbf{n}(\pi) = p = (a + b\alpha)^2 + q(b\alpha)^2$, with p a prime positive number.

3. Let $s \in \mathbb{Z}$ be the only solution to the equation $a + bx = 0\ mod\ p$, $x \in \{0, 1, 2, ..., p-1\}$.

4. Let $r = \left[\frac{p-1}{2}\right] \in \mathbb{N}$, where [ ] denotes the integer part.

5. Let $k \in \mathbb{Z}$ and $\mathbf{k} \in \mathbb{Z}_p$ be its equivalence class modulo p.

6. For all integers $\sigma, \tau \in \{-r-1, ..., r\}$, let $c = (s\tau + \sigma)\ mod\ p$ and $d = (\sigma + \tau\alpha)^2 + q(\tau\alpha)^2$.

6. If $d < p$ and $c = k$, then we find the pairs (σ, τ) such that $\mathbf{k}$ is the label of the element $\sigma + \tau w \in \mathbb{V}_\pi$. From here, we have that $\sigma + \tau s = k\ mod\ p$ and $\mathbf{n}(\sigma + \tau w)$ is minimum. If we find more than two pairs satisfying the last condition, then we will choose that pair with the following property $|\sigma| + |\tau| \leq |a| + |b|$. If there exist more than two pairs satisfying the last inequality, then we will choose one of them randomly.

Codes over $\mathbb{V}_\pi$

Using ideas from the above definitions and generalizing the Hurwitz weight from [Gu; 13] and Cayley-Dickson weight for the octonions, from [Fl; 15], in the same manner, we define the *generalized Cayley-Dickson weight*, for algebras obtained by the Cayley-Dickson process, denoted d_G. We will fix t, α, w and we will consider the elements in the algebra $\mathbb{A}_t(\mathbb{R})$. Let π be a prime in $\mathbb{V}$, $\pi = a + bw$ and let $x \in \mathbb{V}$, $x = a_0 + b_0 w$. The *generalized Cayley-Dickson weight* of x is defined as $w_G(x) = |a_0| + |b_0|$, where $x = a_0 + b_0 w \ mod \ \pi$, with $|a_0| + |b_0|$ minimum.

The *generalized Cayley-Dickson distance* between $x, y \in \mathbb{V}_\pi$ is defined as

$$d_G(x, y) = w_G(x - y)$$

and we will prove that d_G is a metric. Indeed, for $x, y, z \in \mathbb{V}_\pi$, we have $d_G(x, y) = w_G(\alpha_1) = |a_1| + |b_1|$, where $\alpha_1 = x - y = a_1 + b_1 w \ mod \ \pi$ is an element in $\mathbb{V}_\pi$ and $|a_1| + |b_1|$ is minimum.
$d_G(y, z) = w_G(\alpha_2) = |a_2| + |b_2|$, where $\alpha_2 = y - z = a_2 + b_2$ w$mod \ \pi$ is an element in $\mathbb{V}_\pi$ and $|a_2| + |b_2|$ is minimum.
$d_G(x, z) = w_G(\alpha_3) = |a_3| + |b_3|$, where $\alpha_3 = x - z = a_3 + b_3 w \ mod \ \pi$ is an element in $\mathbb{V}_\pi$ and $|a_3| + |b_3|$ is minimum.
We obtain $x - z = \alpha_1 + \alpha_2 \ mod \ \pi$ and it results that $w_G(\alpha_1 + \alpha_2) \geq w_G(\alpha_3)$, since $w_G(\alpha_3) = |a_3| + |b_3|$ is minimum, therefore $d_G(x, y) + d_G(y, z) \geq d_G(x, z)$.

In the following, we assume that π is a prime in $\mathbb{V}$ with $\mathbf{n}(\pi) = p$ a prime number of the form $\mathbf{n}(\pi) = Mn + 1$, $M, n \in \mathbb{Z}, n \geq 0$, such that there are β a primitive element (of order $p - 1$) in $\mathbb{V}_\pi$, with the properties $\beta^{\frac{p-1}{M}} = w$ or $\beta^{\frac{p-1}{M}} = -w$. We will consider codes of length $n = \frac{p-1}{M}$.

The definitions and the Theorems below have adapted and have generalized to all algebras obtained by the Cayley-Dickson process some definitions from [Gu; 13], [Ne, In, Fa, Pa; 01], [Fl; 15], the Theorems 7,8,9,10,11,13,14,15 from [Ne, In, Fa, Pa; 01], the Theorems 4,5,6,7 from [Gu; 13] and the Theorems 2.3, 2.5, 2.7, 2.9 from [Fl; 15] with similar proofs.

We consider $\mathcal{C}$ a code defined by the parity-check matrix H,

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & ... & \beta^{n-1} \\ 1 & \beta^{M+1} & \beta^{2(M+1)} & ... & \beta^{(n-1)(M+1)} \\ ... & ... & ... & ... & ... \\ 1 & \beta^{Mk+1} & \beta^{2(Mk+1)} & ... & \beta^{(n-1)(Mk+1)} \end{pmatrix}, \qquad (4.5.2.)$$

with $k < n$. We know that c is a codeword in $\mathcal{C}$ if and only if $Hc^t = 0$. If we consider the associate code polynomial $c(x) = \sum_{i=0}^{n-1} c_i x^i$, we have that $c\left(\beta^{Ml+1}\right) = 0, l \in \{0, 1, ..., k\}$. For the polynomial $g(x) = (x-\beta)\left(x-\beta^{M+1}\right)...\left(x-\beta^{(Mk+1)}\right)$, since the elements $\beta, \beta^{M+1}, ..., \beta^{Mk+1}$ are distinct, from [Li, Xi; 04], Lemma 8.1.6, we obtain that $c(x)$ is divisible by $g(x)$, where $g(x)$ is the generator polynomial of the code C. Since $g(x) \ / \ (x^n \pm w)$, it results that C is a principal ideal in the ring $\mathbb{V}_\pi \ / \ (x^n \pm w)$.

If we suppose that a codeword polynomial $c(x)$ is sent over a channel and the error pattern $e(x)$ occurs, it results that the received polynomial is $r(x) = c(x) + e(x)$. The vector corresponding to the polynomial $r(x) = c(x) + e(x)$ is $r = c + e$ and *the syndrome* of r is $S = Hr^t$, where H is the above parity-check matrix.

Theorem 4.5.11. *We consider $\mathcal{C}$ a code defined on $\mathbb{V}_\pi$ by the parity check matrix*

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & ... & \beta^{n-1} \end{pmatrix}. \qquad (4.5.3.)$$

It results that, the code $\mathcal{C}$ is able to correct all errors of the form $e(x) = e_i x^i$, with $0 \leq w_C(e_i) \leq 1$.

Proof. We consider $r(x) = c(x) + e(x)$ the received polynomial, with $c(x)$ the codeword polynomial and $e(x) = e_i x^i$ the error polynomial such that $0 \leq w_C(e_i) \leq 1$. Since $\beta^n = w$ or $\beta^n = -w$, it results that $e_i = \beta^{nl}$. If we compute the syndrome, we obtain $S = \beta^{i+nl} = \beta^L$, with $i, L \in \mathbb{Z}, 0 \leq i, L \leq n-1$. By reducing L modulo n, we obtain i, the location of the error, and from here, $l = \frac{L-i}{n}$ and β^{nl}, the value of the error. □

Theorem 4.5.12. *We consider $\mathcal{C}$ a code defined by the parity-check matrix*

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & ... & \beta^{n-1} \\ 1 & \beta^{M+1} & \beta^{2(M+1)} & ... & \beta^{(n-1)(M+1)} \end{pmatrix}. \quad (4.5.4.)$$

Then $\mathcal{C}$ can correct error patterns of the form $e(x) = e_i x^i$, with $e_i \in \mathbb{V}_\pi$, $0 \leq i \leq n-1$.

Proof. We consider the received polynomial, $r(x) = c(x) + e(x)$ with $c(x)$ the codeword polynomial and $e(x) = e_i x^i$ the error polynomial with $e_i \in \mathbb{V}_\pi$. It results that the corresponding vector of the polynomial $r(x)$ is $r = c + e$. We will compute the syndrome S of r. We have $e_i = \beta^j, 0 \leq j \leq Mn-1$ and the syndrome is

$$S = Hr^t = \begin{pmatrix} s_1 = \beta^{i+j} = \beta^{M_1} \\ s_{M+1} = \beta^{(M+1)i+j} = \beta^{M_2} \end{pmatrix}.$$

We obtain $\beta^{i+j-M_1} = 1$, with $i + j = M_1 \ mod(p-1)$ and $\beta^{(M+1)i+j-M_2} = 1$, with $(M+1)i + j = M_2 \ mod(p-1)$. We get $Mi = (M_2 - M_1) \ mod(p-1)$, if there is, then the solution to the system is $i = \frac{M_2 - M_1}{M} \ mod \ n$ and $j = (M_1 - i) \ mod(p-1)$. From here, we can find the location and the value of the error.□

Theorem 4.5.13. *We consider $\mathcal{C}$ a code defined by the parity-check matrix*

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & ... & \beta^{n-1} \\ 1 & \beta^{M+1} & \beta^{2(M+1)} & ... & \beta^{(n-1)(M+1)} \\ 1 & \beta^{2M+1} & \beta^{2(2M+1)} & ... & \beta^{(n-1)(2M+1)} \end{pmatrix}. \quad (4.5.5.)$$

Then $\mathcal{C}$ can find the location and can correct errors of the form $e(x) = e_i x^i$, $0 \leq i \leq n-1$, with $e_i \in \mathbb{V}_\pi$, or can only correct error patterns of this form.

Proof. From the above Theorem, we have $e_i = \beta^j, 0 \leq j \leq Mn-1$ and the syndrome is

$$S = Hr^t = \begin{pmatrix} s_1 = \beta^{i+q} = \beta^{M_1} \\ s_{M+1} = \beta^{(M+1)i+j} = \beta^{M_2} \\ s_{2M+1} = \beta^{(2M+1)i+j} = \beta^{M_3} \end{pmatrix}.$$

Since the matrix $\begin{pmatrix} 1 & \beta & \beta^2 \\ 1 & \beta^{M+1} & \beta^{2(M+1)} \\ 1 & \beta^{2M+1} & \beta^{2(2M+1)} \end{pmatrix}$ has its determinant equal

to $\beta^3\beta^M\left(\beta^{2M}-1\right)^3 \neq 0$, it results that the rank of the matrix (4.5.5) is 3, then this system always has a solution. We obtain $\beta^{i+j-M_1}=1$, with $i+q=M_1\ mod(p-1)$, $\beta^{(M+1)i+j-M_2}=1$, with $(M+1)\,i+j=M_2\ mod(p-1)$, $\beta^{(2M+1)i+j-M_3}=1$, with $(2M+1)\,i+j=M_3\ mod(p-1)$. We can find the location of the error if $Mi=(M_2-M_1)\ mod(p-1)$ and $Mi=(M_3-M_2)\ mod(p-1)$ or, equivalently, $i=\frac{M_2-M_1}{M}\ mod\ n=\frac{M_3-M_2}{M}\ mod\ n$ and the value of the error e_i if
$(M_1-i)\ mod(p-1)=(M_2-(M+1)\,i)\ mod(p-1)=(M_3-(2M+1)\,i)\ mod(p-1)(=j)$. □

Theorem 4.5.14. *Let $\mathcal{C}$ be a code defined by the following parity-check matrix*

$$H=\begin{pmatrix} 1 & \beta & \beta^2 & ... & \beta^{n-1} \\ 1 & \beta^{M+1} & \beta^{2(M+1)} & ... & \beta^{(n-1)(M+1)} \\ 1 & \beta^{2M+1} & \beta^{2(2M+1)} & ... & \beta^{(n-1)(2M+1)} \\ 1 & \beta^{3M+1} & \beta^{2(3M+1)} & ... & \beta^{(n-1)(3M+1)} \end{pmatrix}. \qquad (4.5.6.)$$

Then $\mathcal{C}$ can correct error patterns of the form $e(x)=e_ix^i+e_jx^j$, $0\leq i,j\leq n-1$, where $e_i,e_j\in\mathbb{V}_\pi$.

Proof. We will give a proof in the general case, when we have two errors. We have $e_i=\beta^{q'}\neq 0$ and $e_j=\beta^{t'}\neq 0, q',t'\in\mathbb{Z}$. The syndrome is:

$$S{=}Hr^t{=}\begin{pmatrix} s_1=\alpha^{i+q'}+\alpha^{j+t\prime} \\ s_{M+1}=\alpha^{(M+1)i+q'}+\alpha^{(M+1)j+t'} \\ s_{2M+1}=\alpha^{(2M+1)i+q'}+\alpha^{(2M+1)j+t\prime} \\ s_{3M+1}=\alpha^{(3M+1)i+q'}+\alpha^{(3M+1)j+t'} \end{pmatrix}.$$

We denote $\beta^{i+q'}=A$ and $\beta^{j+t'}=B$ and we get

$$S{=}Hr^t{=}\begin{pmatrix} s_1=A+B \\ s_{M+1}=\beta^{Mi}A+\beta^{Mj}B \\ s_{2M+1}=\beta^{2Mi}A+\beta^{2Mj}B \\ s_{3M+1}=\beta^{3Mi}A+\beta^{3Mj}B \end{pmatrix}. \qquad (4.5.7.)$$

In the case when the system (4.5.7) admits only one solution, the code $\mathcal{C}$ can correct two errors. To obtain this result, we will prove first the following Lemma.

Lemma. *Using the above notations, if we have two errors, we get* $\beta^{Mi} \neq \beta^{Mj}, 0 \leq i, j \leq n-1$ *and* $s_1 s_{2M+1} \neq s_{M+1}^2$.

Proof. In the case when $\beta^{Mi} = \beta^{Mj}$, then $\beta^{M(i-j)} = 1$ and $Mn \ / \ M(i-j)$, which it is false. Supposing that $s_1 s_{2M+1} - s_{M+1}^2 = 0$, it results $s_1 s_{2M+1} = s_{M+1}^2$. If $x = \beta^{i+q'}$, we obtain that $\beta^{2Mi} s_1 x + \beta^{2Mj} s_1^2 - \beta^{2Mj} s_1 x = \left(\beta^{Mi} - \beta^{Mj}\right)^2 x^2 + \beta^{2Mj} s_1^2 + 2\beta^{Mj}\left(\beta^{Mi} - \beta^{Mj}\right) s_1 x$. We get $(\beta^{Mi} - \beta^{Mj})^2 x^2 + 2\beta^{Mi+Mj} s_1 x - \beta^{2Mi} s_1 x - \beta^{2Mj} s_1 x = 0$. It results $x = 0$ or $x = \frac{-2\beta^{Mi+Mj} s_1 + \beta^{2Mi} s_1 + \beta^{2Mj} s_1}{(\beta^{Mi} - \beta^{Mj})^2} = s_1$. If we have $x = \beta^{i+q'} = s_1$, this implies $\beta^{j+t'} = 0$, which it is false.

We go back now to the proof of the Theorem and we know that the following conditions are fulfilled: $\beta^{Mi} \neq \beta^{Mj}, 0 \leq i, j \leq n-1$ and $s_1 s_{2M+1} \neq s_{M+1}^2$.

For $B = s_1 - A$, it results that
$A\left(\beta^{Mi} - \beta^{Mj}\right) = s_{M+1} - s_1 \beta^{Mj}$
$A\left(\beta^{2Mi} - \beta^{2Mj}\right) = s_{2M+1} - s_1 \beta^{2Mj}$
$A\left(\beta^{3Mi} - \beta^{3Mj}\right) = s_{3M+1} - s_1 \beta^{3Mj}$.
We obtain $s_{2M+1} - s_1 \beta^{2Mj} = \left(s_{M+1} - s_1 \beta^{Mj}\right)\left(\beta^{Mi} + \beta^{Mj}\right)$ and $s_{3M+1} - s_1 \beta^{3Mj} = \left(s_{M+1} - s_1 \beta^{Mj}\right)\left(\beta^{2Mi} + \beta^{Mi}\beta^{Mj} + \beta^{2Mj}\right)$.
If we denote by $s_M = \beta^{Mi} + \beta^{Mj}$ and $p_M = \beta^{Mi}\beta^{Mj}$, we have

$$s_{2M+1} - s_{M+1} s_M + p_M s_1 = 0$$

and

$$\left(s_{M+1} - s_1 \beta^{Mj}\right)\left(s_M^2 - p_M\right) = s_{3M+1} - s_1 \beta^{3Mj}.$$

It results that

$$p_M = \frac{s_{M+1} s_M - s_{2M+1}}{s_1}$$

and

$$s_M(s_1 s_{2M+1} - s_{M+1}^2) = s_1 s_{3M+1} - s_{M+1} s_{2M+1}.$$

Therefore, we obtain

$$s_M = \frac{s_1 s_{3M+1} - s_{M+1} s_{2M+1}}{s_1 s_{2M+1} - s_{M+1}^2}$$

$$p_M = \frac{s_{M+1} s_{3M+1} - s_{2M+1}^2}{s_1 s_{2M+1} - s_{M+1}^2}.$$

Using the above, by solving the equation $x^2 - s_M x + p_M = 0$, we find the locations and the values of the errors. $\square$

Main algorithm and some examples

The Main Algorithm

Let p be a prime number.

1. We find $a, b, t \in \mathbb{N}$ such that we can write p under the form

$$p = a^2 + \left(2^t - 1\right) b^2. \tag{4.5.8.}$$

We remark that the values for $a, b, t,$ if there exist, are not unique. Let $\{a_l, b_l, t_l\}, l \in \{1, 2, ..., u\}$ all solutions to the equation (4.5.8) .

2. Let $p = n_j M_j + 1,$ with n_j, M_j not unique such that $n_j M_j = p - 1, j \in \{1, 2, ..., v\}$.

3. For $l \in \{1, 2, ..., u\}$ and for $j \in \{1, 2, ..., v\},$ we find the algebra $\mathbb{A}_{t_l}(\mathbb{R})$, the element $w = \frac{1}{2^{r_l - 1}}(1 + \sum_{i=2}^{2^{t_l}} e_i) \in \mathbb{A}_{t_l}(\mathbb{R}), r_l \geq t_l - 1, \mathbb{V} \subset \mathbb{A}_{t_l}(\mathbb{R})$, the element $\pi \in \mathbb{V}$, such that $\mathbf{n}(\pi) = p$, we find $\mathbb{V}_\pi$ such that $\mathbb{V}_\pi$ is isomorphic to $\mathbb{Z}_p$ and we find $\beta \in \mathbb{V}_\pi$ such that $\beta^{n_j} = w$ or $\beta^{n_j} = -w$.

If the elements $\{a_l, b_l, t_l\}$ don't exist, then the algorithm stops.

If we have at least a solution for the equation (4.5.8) but we don't find for $j \in \{1, 2, ..., v\}$ the element $\beta \in \mathbb{V}_\pi$ such that $\beta^{n_j} = w$ or $\beta^{n_j} = -w$, then the algorithm stops. If we have solutions in both cases, then we go to the Step 4.

4. For each solution $\{a_l, b_l, t_l\}, l \in \{1, 2, ..., u\},$ let $\mathcal{J} \subseteq \{1, 2, ..., v\}$. For each $j \in \mathcal{J},$ we have n_j such that $\beta^{n_j} = w$ or $\beta^{n_j} = -w$. We can change w by increasing the value of r_l , if it is necessary, but working in the algebra $\mathbb{A}_{t_l}(\mathbb{R})$. For each n_j we compute M_j and the rate of the obtained code, $R_j = \frac{k_j}{n_j}$. Since we can suppose that the obtained codes have the same dimension $k = k_j$, we will chose the indices $l \in \{1, 2, ..., u\}, j \in \mathcal{J},$ the pair $\{a_l, b_l, t_l\}$ and the number n_j such that the rate R_j has the biggest value.

In the following, we will denote by Algorithm 1, the method described in [Gu; 13] and by Algorithm 2, the method described in [Fl; 15].

Remark 4.5.15. In the papers [Gu; 13] and [Fl; 15] were developed several algorithms which have built binary block codes over subsets of integers in the real quaternion division algebra and in the real octonion division algebra. The above algorithm has generalized these two algorithms to real algebras obtained by the Cayley-Dickson process. Moreover, the Main Algorithm can be generalized to almost all prime numbers, which in general the Algorithm 1 and the Algorithm 2 don't make it. That means, in general, for a prime number p, we can get the algebra $\mathbb{A}_t(\mathbb{R})$, the element $w \in \mathbb{A}_t(\mathbb{R})$, the subset $\mathbb{V} \subset \mathbb{A}_{t_l}(\mathbb{R})$, $\pi \in \mathbb{V}$, such that $\mathbf{n}(\pi) = p$, we can find $\mathbb{V}_\pi$ with $\mathbb{V}_\pi$ isomorphic to $\mathbb{Z}_p$, such that the obtained binary block code can have the highest rate.

With the Main Algorithm, we have a higher flexibility, similar to the Lenstra's algorithm for elliptic curves compared with $p-1$ Pollard algorithm. It is well known that for a prime p, Lenstra's algorithm replaces the group $\mathbb{Z}_p^*$ with the group of the rational points of an elliptic curve $\mathcal{C}_1$ over $\mathbb{Z}_p$. If this algorithm failed, the curve will be replaced with another curve $\mathcal{C}_2$ over $\mathbb{Z}_p$ and we can retake the algorithm (see [Si, Ta; 92]).

In the case of the Main Algorithm, the algebra $\mathbb{A}_t(\mathbb{R})$ and w offer this kind of flexibility since, for the same prime p, these can be changed and the algorithm can be retaken, with better chances of success.

We will explain this in the following examples.

Example 4.5.16. Let $p = 29$. We have $a = 1, b = 2$ and $t = 3$, therefore $p = 1 + 7 \cdot 4$ with unique decomposition. It results that we can use the real Octonion algebra. If we apply Algorithm 2, we have $w = \frac{1}{2}\left(1 + \sum_{i=2}^{8} e_i\right)$, $\pi = -1 + 4w, p = 29, n = 4, s = 22, \beta = 1 - w, \beta^4 = -w \ mod \ \pi$, therefore we can define codes.

If we apply the Main Algorithm for $w = \frac{1}{4}\left(1 + \sum_{i=2}^{8} e_i\right)$, we have $\pi = -1 + 8w, n = 4, s = 11$ which is the label for the element $w \in \mathbb{V}_\pi$. We remark that we can't find $\beta \in \mathbb{V}_\pi$ such that $\beta^4 = w$, as we can see from the MAPLE's procedures below.

```
for i from -15 to 14 do for j from -15 to 14 do
```

```
c := (11*j+i)mod 29; d := ((7/4)*j)^2+(i+(1/4)*j)^2;
if d < 29 and c = 11 then print(i, j);fi;od;od;
                                        0, 1
                                        4, -2

A := 8^{-1} mod 29; for a to 29 do
b := a^4 mod 29; if b = 11 then print(a);fi;od;
                                          11
```

But, if we increase α we still work on the octonions and we take $w = \frac{1}{32}\left(1+\sum_{i=2}^{8} e_i\right)$, with the label $s = 24$. We obtain $\beta = -1 - w$ with the label 4 such that $\beta^4 = w$. Therefore we can define codes. In this situation, both algorithms can be applied with success.

Example 4.5.17. Let $p = 71 = 64 + 7 \cdot 1$, with unique decomposition. Therefore $a = 8, b = 1, t = 3$. Then we work on real Octonion algebra. If we apply the Algorithm 2, we have $w = \frac{1}{2}\left(1+\sum_{i=2}^{8} e_i\right)$, $\pi = 7 + 2w, p = 71, n = 10, s = 32, \beta = 2 - 2w, \beta^{10} = w \ mod \ \pi$.(see [Fl; 15])

If we apply the Main Algorithm and if we take first time $w = \frac{1}{4}\left(1+\sum_{i=2}^{8} e_i\right)$, we have $\pi = 7 + 4w, p = 71, n = 10, s = 16$, which is the label for the element $w \in \mathbb{V}_\pi$.We remark that we can't find $\beta \in \mathbb{V}_\pi$ such that $\beta^{10} = w$ (even if we increase the value of r, as in Example 4.5.16), as we can see in the procedure below.

```
A := -7*4^{-1}mod71; for a from 1 to 71 do b := a^{10} mod 71;
if b = 16 then print(a);fi;od:
                                          16
```

Therefore, the Algorithm 2 is better than the Main Algorithm.

Example 4.5.18. For $p = 31 = 6 \cdot 5 + 1$, we have $p = 4 + 3 \cdot 9 = 16 + 15 \cdot 1$, therefore $t \in \{4, 16\}$ and we can use the real Quaternion algebra or the real

Sedenion algebra. If we apply the Main Algorithm for sedenions, we have $w = \frac{1}{8}\left(1 + \sum_{i=2}^{16} e_i\right)$. We get $\pi = 3 + 8w, p = 31$ and $s = 19$. We remark that we can't use the Main Algorithm for the sedenions since we can't find $\beta \in \mathbb{V}_\pi$ such that $\beta^5 = w$. Therefore, we will use the Main Algorithm only for Quaternion algebra, which can be applied in this case.

Example 4.5.19. Let $p = 61$. We have that $p = 4 \cdot 3 \cdot 5 + 1 = 1 + 60 = 1 + 15 \cdot 4 = 49 + 3 \cdot 4$, therefore $t \in \{4, 16\}$ and we can use the real Quaternion algebra or the real Sedenion algebra.

If we take p under the form $p = 61 = 7^2 + 3 \cdot 2^2$, we use the real Quaternion algebra. For $w = \frac{1}{2}\left(1 + \sum_{i=2}^{4} e_i\right)$, we get $\pi = 5 + 4w$. The label for w is $s = 14, n = 10 (p = 6 \cdot 10 + 1)$ and we have $\beta = -4 + w, \beta^{10} = w$, as we can see in the below procedures:

```
A := -5*4^{-1}mod 61; for a to 61 do
b := a^{10}mod 61; if b = 14 then print(a);fi;od;
   14 10 17  26 29 30 30 31 32 35 44 51
```

```
for i from -31 to 30 do for j from -31 to 30 do
c :=(14*j+i) mod 61 d := (3/4)*j^2+(i+(1/2)*j)^2;
if d < 61 and c = 10 then print(i, j)fi;od;od;
                                        -4, 1
                                        1, 5
                                        5, -4
```

In this case, the rate code is $R_1 = \frac{6k}{p-1} = \frac{k}{10}$, where k is the dimension of the code, since we can't find β such that $\beta^6 = w$ or $\beta^{M_j} = w$, for $M_j \mid p - 1, j \in \{1, 2, ..., v\}$.

If we consider p under the form $p = 1 + 15 \cdot 4$, we use the real Sedenion algebra, we get $n = 4$ and for $w = \frac{1}{8}\left(1 + \sum_{i=2}^{16} e_i\right)$, we have $\pi = -1 + 16w$. The label for w is $s = 42$ and $\beta = 2 + 2w$. In this case, the rate of the code is $R_2 = \frac{15k}{p-1} = \frac{k}{4}$ and it is greater than R_1. We remark that we can use both

algebras to define codes, but in the second case, we have chance to obtain a better rate.(The dimension k is considered the same, in both situations).

```
A :=16^{-1}mod 61; for a to 61 do b :=a^{4}mod61;
if b = 42 then print(a);fi;od;
42 25 30 31 36
```

```
for i from -31 to 30 do for j from -31 to 30 do c :=42*j+i mod 61;
 d := (15/64)*j^2+(i+(1/8)*j)^2; if d < 61 and c = 25 then print(i, j);
fi;do;do;
                                    -6, 8
                                    -5, -8
                                     -2, 5
                                    -1, -11
                                     2, 2
                                    3, -14
                                     6, -1
```

Example 4.5.20. Let $p = 151 = 4 + 3 \cdot 49 = 16 + 15 \cdot 9 = 6 \cdot 25 + 1$.

We have $t \in \{2, 4\}$ and will use the real Quaternion algebra or real Sedenion algebra. For $w = \frac{1}{2}\left(1 + \sum_{i=2}^{4} e_i\right)$, we have $\pi = -3 + 14w, n = 25$ and $s = 140$, the label for w. In this case, we can't find an element β, such that $\beta^{25} = w$, $\beta^6 = w, \beta^{15} = w$ and so on, as we can see in the procedure below.

```
A:=-3*14^{-1} mod 151; for a to 151 do b:=a^25 mod 151;
if b = 140 then print(a);fi;od:
                                    140
```

But, as we remarked, the number p can be written under the form $p = 16 + 15 \cdot 9 = 25 \cdot 6 + 1$, then if we take $t = 4$, we can use the real Sedenion algebra. We consider $w = \frac{1}{8}\left(1 + \sum_{i=2}^{16} e_i\right)$. We obtain $\pi = 1 + 24w, n = 6$

and $s = 44$, the label for w. We can find β, such that $\beta^6 = w \ mod \ \pi$ and $\beta = 3 - 3w$, with the label $s = 22$.

```
A:=-24^{-1}mod 151; for a to 151 do
b:=a^6 mod 151; if b = 44 then print(a);fi;do;
                  44 22 51 100 122 129

for i from -76 to 75 do for j from -76 to 75 do
c := 44*j+i mod 151; d:= (15/64)*j^2+(i+(1/8)*j)^2;
 if d < 151 and c = 22 then print(i, j);fi;od;od;
                                    -9, 11
                                    -4, -20
                                     -3, 4
                                     3, -3
                                     4, 21
                                    9, -10
```

Example 4.5.21. Let $p = 149 = 25 + \mathbf{31} \cdot 4 = 121 + \mathbf{7} \cdot 4$. In this situation, $t \in \{3, 5\}$ and we can use the real Octonion algebra or a real Cayley-Dickson algebra of dimension 32.

We can't use the Algorithm 2 for octonions, since we can't obtain the element β and p is not under the form $7k+1$. For $w = \frac{1}{4}\left(1 + \sum_{i=2}^{8} e_i\right)$, we have $\pi = 9 + 8w$. We consider $p = 1 + 4 \cdot 37$ and we can't find an element β, even if we take $p = 2k + 1$ or $4k + 1$ or $37k + 1$.

```
A := -9*8^{-1} mod 149; for a to 149 do
b := a^2 mod 149; if b = 92 then print(a);fi;od;
                                    92

A := -9*8^{-1}mod 149; for a to 149 do
b := a^4 mod 149; if b = 92 then print(a);fi;od;
                                    92

A := -9*8^{-1}mod 149; for a to 149 do
```

```
b := a^37 mod 149 if b = 92 then print(a);fi;od;
                                        92
```

But we can choose another α. For example, for $w = \frac{1}{8}\left(1 + \sum_{i=2}^{8} e_i\right)$, we have $\pi = 9 + 16w$, and $s_1 = 46,$ the label for w. If we consider $p = 74n + 1,\ n = 2,$ we get $\beta = -2 + 4w$, with label $s_2 = 33$. In this case, the rate of the code is $R_1 = \frac{74k}{p-1} = \frac{k}{2}$. For $p = 37n + 1$, $n = 4,$ the label of $\beta = 4w$ is $s_3 = 35$. In this case the rate of the code is $R_2 = \frac{37k}{p-1} = \frac{k}{4}$. We have $R_2 < R_1$. Therefore the code in the first case is better, since the code can have a greater rate as in the second case. For $p = 2k + 1$ or $4k + 1$, we can't find β.

```
A := -9*16^{-1} mod 149; for a to 149 do
 b := a^2 mod 149; if b = 46 then print(a);fi;od;
                                 46  33 116
```

```
for i from -75 to 74 do for j from -75 to 74 do
c := (46*j+i) mod 149); d := (31/64)*j^2+(i+(1/8)*j)^2;
if d < 149 and c = 33 then print(i, j);fi;do;do;
                                      -4, 17
                                       -2, 4
                                       0, -9
                                       9, 7
                                      11, -6
```

```
A := -9*16^{-1} mod 149; for a to 149 do
b := a^4 mod 149; if b = 46 then print(a);fi;do;
               46 35 50 99 114
```

```
for i from -75 to 74 do for j from -75 to 74 do
c :=(46*j+i) mod 149); d := (31/64)*j^2+(i+(1/8)*j)^2;
if d < 149 and c = 35 then print(i, j);fi;do;do;
                                      -11, 1
```

```
                                    -2, 17
                                     0, 4
                                     2, -9

A := -9*16^{-1} mod 149; for a to 149 do
b := a^37 mod 149; if b = 46 then print(a);fi;od;
                                       46
```

If we work on a real algebra of dimension 32, we consider $w = \frac{1}{16}\left(1 + \sum_{i=2}^{32} e_i\right)$. We have $\pi = 3 + 32w, s = 107$, the label for $w, \beta = 4$, with the label $s = 4, n = 4, p = 37 \cdot 4 + 1$, as we can see in the procedures below.

```
 A := -3*32^{-1} mod 149; for a to 149 do
 b := a^4 mod 149; if b = 107 then print(a);fi;od;
                        107 4 27 122 145


for i from -75 to 74 do for j from -75 to 74 do
c := (107*j+i) mod 149; d := (31/256)*j^2+(i+(1/16)*j)^2;
if d < 149 and c = 4 then print(i, j);fi;od;od;
                                    -8, 21
                                    -7, -18
                                    -4, 14
                                    -3, -25
                                     0, 7
                                    1, -32
                                     4, 0
                                     8, -7
                                    12, -14
```

In this case, we can work on both algebras to obtain codes with good rates.

(B-ii) The evolution and development plans for career development

Career development directions

I graduated Faculty of Mathematics of University of Bucharest in 1990. From 1991 I have worked at "Ovidius" University of Constanta. I taught various courses for Bachelor and Master degrees, as for example: Linear Algebra, Algebra (fundamental structures), Graph Algorithms , Graphs and Combinatorics, Special chapters of algebra, some of these courses can be found on http://cristinaflaut.wikispaces.com/. I participated at several national and international conferences:

1) Invited speaker and member in International Committee at *Fifth International Eurasian Conference on Mathematical Sciences and Applications* (IECMSA)-2016 which will be held in Belgrade (Serbia) in August 16-19, 2016.

2) Organizer of Conference in the honor of Professor Ravi P Agarwal with occasion of DHC ceremony, 10 July 2015.

3) Member in Scientific Committee of *MITAV 2015*, 18-19 Iunie 2015 (Mathematics, Information Technologies, and Applied Sciences (Vědy, in Czech))

4) *MAOCOS 2014*, International Conference on Mathematics and Computer Science, June 26-28 2014, Braşov, Romania, in Organizing Committee,

5) *Workshop on Algebraic and Analytic Number Theory and Their Applications*, 23-24 mai 2013, Universitatea Ovidius Constanta-Co-organizer , PN-II-ID-WE-2012-4-161.

6) Organizer of the conference *A new approach in theoretical and applied methods in algebra and analysis*, 4-6 Aprilie 2013, Universitatea Ovidius, Constanta, PN-II-ID-WE-2012-4-169, Constanta.

7) *Mathematics and Computer in Business and Economics*, the 9th WSEAS International on Mathematics and Computer in Business and Economics (MCBE' 08), Bucuresti, 24-26 June 2008, with talks. (www.wseas.org.)

8) 2007, 5-10 September- *The XVIth National School of Algebra* (Scoala nationala de algebra, editia a- XVI-a) , Constanta, participant and organizer.

9) 2007-Workshop on Combinatorics and Commutative Algebra II, 26-31 August, Thessaloniki, Greece.

10) 2006-Ring and Category of Modules, 16-18 decembrie 2007, Bressanone, Italia, with talk.

11) 2006, August- National School of Cryptography (Scoala Nationala de Criptografie), Vatra-Dornei, with talk.

Between 2002-2009, 2012-2013 I was editor and from 2013, I am the Editor in Chief of the ISI journal *Analele Stiintifice ale Universitatii Ovidius din Constanta, Seria Matematica,* 2013IF=0.333.

I obtained some grants:

1) PN-II- RU-PRECISI-2014-8-6330 for the paper A Clifford algebra associated to generalized Fibonacci quaternions, Adv. Differ. Equ.-NY, 2014:279, p.1-7,**Yellow zone**.

2) PN-II-ID-WE-2012-4-169, Cristina FLAUT, "Ovidius" University, Constanta: *A new approach in theoretical and applied methods in algebra and analysis*

3) PN-II-RU-PRECISI-2013-7-4123, for Levels and sublevels of algebras obtained by the Cayley–Dickson process, Ann. Mat. Pur. Appl., **Red zone**.

4) UNESCO-UNITWIN OCW/OER Initiative, Handong Global University, South Korea, 1 April 2012- 10 November 2012, April 2013-December 2013, January 2014-July 2014.

5) UNESCO-UNITWIN OCW/OER Initiative, Handong Global University, South Korea, 1 October 2011-20 January 2012.

6) UNESCO-UNITWIN OCW/OER Initiative, Handong Global University, South Korea, 1 September 2013- 31 March 2014.

7) UNESCO-UNITWIN OCW/OER Initiative, Handong Global University, South Korea, 1 April 2012- 10 November 2012.

8) UNESCO-UNITWIN OCW/OER Initiative, Handong Global University, South Korea, 1 October 2011-20 January 2012.

Other **4 PN-II-RU-PRECISI** grants, **1 in red zone and 3 in yellow zone**, will be obtained until the end of 2015.

I was member in the grants:

1) Proiect POSDRU/157/1.3/S/141587, Reţea de formare continuă a cadrelor didactice pentru a utiliza multimedia, instrumentaţia virtuală şi web 2.0 în aria curriculară Matematică şi ştiinţe ale naturii (ProWeb)", valoare totala 5.845.359,05 RON, professor formator al disciplinei Fundamente psihopedagogice ale utilizării TIC în formarea continuă a cadrelor didactice din aria curriculară Matematică şi ştiin21be ale naturii.

2) Sistem pentru detecţie, localizare, urmărire şi identificare a factorilor de risc la adresa obiectivelor de importanţă strategică din zone de litoral – SSSNOC",

Cod depunere PN-II-PT-PCCA 2013-4-0377, Domeniul 8 –Spaţiu şi securitate, Instituţia coordonatoare: Centrul de Cercetare Ştiinţifică pentru Forţele Navale. Parteneri: Oceanografica SRL; Unitatea Militară 02133; Eltex Echipamente Electronice Industriale S.R.L.; General Conf Grup S.R.L.; Universitatea "Ovidius". Durata proiectului: 24 luni (1 iulie 2014-30 iunie 2016).

3) Workshop on Algebraic and Analytic Number Theory and Their Applications, CNCSIS-PN-II-ID-WE-2012-4-161, 20120 ron, 23-24 mai 2013, PN-II-ID-WE-2012-4-161.

4) INTUITION Network of Excellence, co-funded by European Commission, contract number 507248, 1 September 2004- 31 October 2008.

Regarding my research activity, I published several papers in ISI and BDI journals. In this moment, the total of impact factors (regarding CNATDCU requirements) is I=7.4585 in ISI journals with IF$\geq$ 0.5 and, until now, I have 32 citations in ISI journals with IF $\geq$ 0.5. I also write several books and chapters in the books, all of these can be found in my attached list of research activities. I was invited reviewer for many ISI journals.

My didactic activity is well appreciated by the students. I organized some scientific seminaries for students:
1) Seminarul Studentesc de Structuri Matematice Fundamentale:
2) Seminarul Studentesc: Algebre ciclice cu diviziune si aplicatiile lor in teoria codurilor
3) Seminarul Studentesc: Coduri.

In the future, I intend to improve my courses, for this it is necessary to attend conferences and scientific seminaries. I will continue to guide my students

in all common activities, I will continue to organize scientific seminaries for students and I will continue my work at Anale, trying to increase its impact factor.

Scientific development directions

The study of algebras obtained by the Cayley-Dickson process constitutes an important topic in the study of nonassociative algebras.

The results presented in this work can contribute to the development of this domain of research and we will try in the next papers to extend them. Most of ideas presented below can be found at the end of almost papers written by the author (as single author or coauthor). These papers end with conclusions and remarks which can constitute starting points of some further research.

Levels and sublevels of algebras obtained by the Cayley-Dickson process

The construction of quadratic division algebras arising over rational function fields by means of the Cayley-Dickson process, presented in Chapter 2, is closely related to, but actually much more natural than, the ones presented by Brown in [Br, 67] and, more recently, by Garibaldi and Petersson in [Ga, Pe; 11]. The significance of this construction is enhanced still further by the profound connection recently established between non-associative division algebras and the theory of signal transmissions ([Ho; 08]), with important applications to smart phones and other technical devices. One of the main theorems from [Fl; 13]says that such algebras having any pre-assigned positive integer as

their level always exist. This striking result constitutes great progress when compared with what is presently known about the level of quaternion and octonion algebras. The main result obtained in Theorem 2.3.14, where was proved that for any positive integer n there is an algebra A, obtained by the Cayley-Dickson process with the norm form anisotropic over a suitable field, which has level $n \in \mathbb{N} - \{0\}$ allow us to obtain further development in this area. Since it is still unknown what exact numbers can be realised as levels and sublevels of quaternion and octonion division algebras, as further research, can be very interesting to improve the bounds for the level and sublevel of division quaternion and octonion algebras and to provide some new examples of values for the level and sublevel of division quaternion algebras or of division octonion algebras. It remains unknown whether there exist quaternion division algebras of sublevel 5, or quaternion division algebras of level 6. The result obtained in Theorem 2.3.14 seems to indicate that one of the problems in finding a given value for the level of division quaternion and octonion algebras can be the dimension of these algebras and it is easier to work with algebras obtained by the Cayley- Dickson process with higher dimension. This remark allows us to consider this problem in the reverse sense: for any positive integer n, how can the existence of an octonion division algebra of level n influence the existence of a quaternion division algebra of level n? For example, if we have an Octonion division algebra of level 6, its quaternion division subalgebra has the same level 6? Or we can built a quaternion division algebra of level 6 starting from an octonion algebra of level 6? Or, more generally, for any positive integer n, how can the existence of an algebra obtained by the Cayley-Dickson process, of dimension $2^t, t \geq 4$ and level n, influence the existence of a quaternion or an octonion division algebra of level n?

Properties of algebras obtained by the Cayley-Dickson process and some of their applications

Since the algebras obtained by the Cayley-Dickson process are poor in properties when their dimension increase, losing commutativity, associativity

and alternativity, the study of all kind of identities on these algebras is one of the direction of the study. Therefore any supplementary relation, identity or property can be very useful for the study of these algebras. For example, we are looking for other similar relation as Hall identity, to characterize some type $\mathcal{N}$ of nonassociative algebras, $\mathcal{N}$ ={alternative algebras, quadratic algebras, quaternion algebras, octonions algebras, algebras obtained by the Cayley-Dickson process, etc.}: *The property P is true on the algebra A if and only if $A \in \mathcal{N}$.* To support this idea, we can use for example the papers [Po, Ro; 10], [Fl; 14(1)]. Some identities in algebras obtained by the Cayley-Dickson process can be an useful tool to find solutions for some equations in these algebras or to solve them.

Using results obtained in the paper [Ba; 09] and obtained properties of the multiplication of the basis's elements as in [Fl, Sh; 15(1)], we can found some new and very interesting relations and properties of the elements from such an algebra. Starting from results given in [Ja, Op; 10], [Ja, Op; 13], [Mi; 11] we can try to find zeros for some quaternionic and octonionic polynomials, or we can solve some equations and systems in these algebras as in [Er, Oz; 13], [Mi, Sz; 08], [Mi; 10], [Sh; 11].

The Fibonacci-Lucas quaternions over $\mathbb{Q}$ provide us an algebra structure. We can extend the study of this type of elements over octonions trying to obtain the similar results.

Some applications in Coding Theory

Codes over finite rings have been intensively studied in the last time, some of the earliest results of them are in [Bl; 72], [Sp; 78]. Ones of the most important finite rings in the coding theory are: the finite field $\mathbb{F}_q$ and the ring $\mathbb{Z}_q$, where $q = p^r$, for some prime number p and $r \in \mathbb{N}-\{0\}$. The class of cyclic codes is an important class of linear codes with a big interest in coding theory. Described as ideals in certain polynomial rings, they have a good algebraic structure and the cyclic codes over some special finite rings were recently described (see [Ab, Si; 07], [Al, Ha; 10], [Gr; 97], [Qi, Zh, Zhu; 05], etc). Two

classes of these main rings are: Galois rings and rings of the form $\mathbb{F}_q[u]/(u^i)$ or generalization of these, where $q = p^r$ for some prime number p and $r \in \mathbb{N} - \{0\}$. In paper [Fl; 13(1)], were investigated the structure of cyclic codes of arbitrary length over the rings: $\mathbb{F}_q[u]/(u^i), \mathbb{F}_q[u_1, ..., u_i]/(u_1^2, u_2^2, ..., u_i^2, u_1u_2 - u_2u_1, ..., u_ku_j - u_ju_k, ...)$,
$\mathbb{F}_q[u, v]/\left(u^i, v^j, uv - vu\right)$, $q = p^r$, where p is a prime number, $r \in \mathbb{N} - \{0\}$ and $\mathbb{F}_q$ is a field with q elements. The ranks and minimum Hamming distance of these codes were studied. Since the rings with Hamming weight cannot produce always better codes, a more relevant weights on the above mentioned rings can be studied. The remark above can constitute the starting point for further research.

Regarding a finite field as a residue field modulo a prime element from $\mathbb{V}$, where $\mathbb{V}$ is a subset of a real algebra obtained by the Cayley-Dickson process with a commutative ring structure, in [Fl; 16], we obtained an algorithm, called the Main Algorithm, which allows us to find codes with a good rate. This algorithm offers more flexibility than other methods known until now.

As a further research, we intend to improve this algorithm and to adapt it to all prime numbers.

Many people claim that we live in the so-called information age. With the Internet, the massive distribution of any kind of information became possible. These new flows of information need new technologies to expedite them. There are two problems that may occur: first is to provide secure transmission of messages, in the sense that errors that appeared during the transmission can be corrected and the second is that two or more persons can communicate safely, in the sense that confidentiality is guaranteed, data integrity, authentication and non-repudiation. Reliable high rate of transmission can be obtained using Space-Time coding. Space–time block coding is a technique used in wireless communications. With this technique, we can transmit multiple copies of a data stream across a number of antennas. In the same time, we can improve the reliability of data-transfer. For constructing Space-Time codes, division algebras were chosen as a new tool. Their algebraic properties can be used to improve the design of good codes and justify their intensive study.

One example is the Alamouti code, given in [Al; 98] which can be built from a quaternions division algebra. This code construction is used for a

wireless system with two transmit antennas. For this, we consider z_1 and z_2 two complex numbers which represent the information symbols which will be send (see [Be, Og; 13]). The code $\mathcal{C}$ is given as follows:

$$\mathcal{C} = \{\begin{pmatrix} z_1 & -\overline{z_2} \\ z_2 & \overline{z_1} \end{pmatrix} \ / \ z_1, z_2 \in \mathbb{C}\}. \tag{1.}$$

This code has the following property

$$\det(Z - Y) = |z_1 - y_1|^2 + |z_2 - y_2|^2 \geq 0$$

(fully diversity).

From relation (1) , we can remark that the code $\mathcal{C}$ can be done as the left representation of $\mathbb{H}$ over $\mathbb{C}$

$$\lambda : \mathbb{H} \to M_2(\mathbb{C}), \lambda(q) = \begin{pmatrix} z_1 & -\overline{z_2} \\ z_2 & \overline{z_1} \end{pmatrix},$$

where $q = z_1 + z_2 j$. For $Z = \begin{pmatrix} z_1 & -\overline{z_2} \\ z_2 & \overline{z_1} \end{pmatrix}$,We remark that $\det Z = \mathbf{n}(q)$ and $\mathbf{n}(q) = 0$ implies $q = 0$. Therefore the fully diversity is equivalent with the division property of the algebra $\mathbb{H}$. (see [Be, Og; 13])

In [Be, Re; 03], this code was generalised over a division generalised quaternion algebra $\mathbb{H}_K(\alpha, \beta)$ over a number field K,namely

$$\mathcal{C}_{\mathbb{H}_K(\alpha,\beta)} = \{\begin{pmatrix} a + b\sqrt{\beta} & \alpha(c - d\sqrt{\beta}) \\ c + d\sqrt{\beta} & a - b\sqrt{\beta} \end{pmatrix} \ / \ a, b, c, d \in K\}.$$

In [Pu, St; 15], the above code was generalized to quaternion nonassociative algebras. For other details the reader is referred to [Ho; 08], : [Og, Be, Vi; 07], : [Og, Vi; 04], [Un, Ma; 10], [Pu, Un; 10].

Other directions

BCK-algebras were first introduced in mathematics in 1966 by Y. Imai and K. Iseki, through the paper [Im, Is; 66], as a generalization of the concept of

set-theoretic difference and propositional calculi. The class of BCK-algebras is a proper subclass of the class of BCI-algebras and there exist several generalizations of BCK-algebras as for example generalized BCK-algebras [Ho, Ju; 03]. These algebras form an important class of logical algebras and have many applications to various domains of mathematics, such as: group theory, functional analysis, fuzzy sets theory, probability theory, topology, etc. For other details about BCK-algebras and about some new applications of them, the reader is referred to [Ho, Ju; 03] .

One of the recent applications of BCK-algebras was given in the Coding Theory. In Coding Theory, a block code is an error-correcting code which encode data in blocks. In the paper [Ju, So; 11], the authors constructed a finite binary block-codes associated to a finite BCK-algebra. At the end of the paper, they put the question if the converse of this statement is also true.

The results presented below were found by the author in the papers [Fl; 15(2)] and [B,Fa, Fl, Ku; 15].

Definition 1.1. An algebra $(X, *, \theta)$ of type $(2, 0)$ is called a *BCI-algebra* if the following conditions are fulfilled:

1) $((x * y) * (x * z)) * (z * y) = \theta$, for all $x, y, z \in X$;

2) $(x * (x * y)) * y = \theta$, for all $x, y \in X$;

3) $x * x = \theta$, for all $x \in X$;

4) For all $x, y, z \in X$ such that $x * y = \theta, y * x = \theta$, it results $x = y$.

If a BCI-algebra X satisfies the following identity:

5) $\theta * x = \theta$, for all $x \in X$, then X is called a *BCK-algebra*.

A BCK-algebra X is called *commutative* if $x * (x * y) = y * (y * x)$, for all $x, y \in X$ and *implicative* if $x * (y * x) = x$, for all $x, y \in X$.

The partial order relation on a BCK-algebra is defined such that $x \leq y$ if and only if $x * y = \theta$.

If $(X, *, \theta)$ and $(Y, \circ, \theta)$ are two BCK-algebras, a map $f : X \to Y$ with the property $f(x * y) = f(x) \circ f(y)$, for all $x, y \in X$, is called a *BCK-algebras morphism*. If f is a bijective map, then f is an *isomorphism* of BCK-algebras.

In the following, we will use some notations and results given in the paper [Ju, So; 11] .

From now on, all considered BCK-algebras are finite.

Let A be a nonempty set and let X be a BCK-algebra.

Definition 1.2. A mapping $f : A \to X$ is called a *BCK-function* on A. A *cut function of* f is a map $f_r : A \to \{0,1\}, r \in X$, such that

$$f_r(x) = 1, \text{ if and only if } r * f(x) = \theta, \forall x \in A.$$

A *cut subset* of A is the following subset of A

$$A_r = \{x \in A : r * f(x) = \theta\}.$$

Remark 1.3. Let $f : A \to X$ be a BCK-function on A. We define on X the following binary relation

$$\forall r, s \in X, r \sim s \text{ if and only if } A_r = A_s.$$

This relation is an equivalence relation on X and we denote with $\widetilde{r}$ the equivalence class of the element $r \in X$.

Remark 1.4. ([Ju, So; 11]) Let A be a set with n elements. We consider $A = \{1, 2, ..., n\}$ and let X be a BCK-algebra. For each BCK-function $f : A \to X$, we can define a binary block-code of length n. For this purpose, to each equivalence class $\widetilde{x}, x \in X$, will correspond the codeword $w_x = x_1x_2...x_n$ with $x_i = j$, if and only if $f_x(i) = j, i \in A, j \in \{0,1\}$.We denote this code with V_X.

Let V be a binary block-code and $w_x = x_1x_2...x_n \in V$, $w_y = y_1y_2...y_n \in V$ be two codewords. On V we can define the following partial order relation:

$$w_x \preceq w_y \text{ if and only if } y_i \leq x_i, i \in \{1, 2, ..., n\}. \quad (1.1.)$$

In the paper [Ju, So; 11], the authors constructed binary block-codes generated by BCK-functions. At the end of the paper they put the following question: *for each binary block-code* V, *there is a BCK-function which determines* V? The answer of this question is partial affirmative, as we can see in Theorem 2.2 and Theorem 2.9.

2. Main results

Let $(X, \leq)$ be a finite partial ordered set with the minimum element θ . We define the following binary relation " $*$ " on X :

$$\begin{cases} \theta * x = \theta \text{ and } x * x = \theta, \forall x \in X; \\ x * y = \theta, \text{ if } x \leq y, \quad x, y \in X; \\ \qquad x * y = x, \text{ otherwise.} \end{cases} \tag{2.1.}$$

Proposition 2.1. *With the above notations, the algebra $(X, *, \theta)$ is a non-commutative and non-implicative BCK-algebra.* □

If the above BCK-algebra has n elements, we will denote it with $\mathcal{C}_n$.

Let V be a binary block-code with n codewords of length n. We consider the matrix $M_V = (m_{i,j})_{i,j \in \{1,2,...,n\}} \in \mathcal{M}_n(\{0,1\})$ with the rows consisting of the codewords of V. This matrix is called *the matrix associated to the code V.*

Theorem 2.2. *With the above notations, if the codeword $\underbrace{11...1}_{n-\text{time}}$ is in V and the matrix M_V is upper triangular with $m_{ii} = 1$, for all $i \in \{1, 2, ..., n\}$, there are a set A with n elements, a BCK-algebra X and a BCK-function $f : A \to X$ such that f determines V.*

Proof. We consider on V the lexicographic order, denoted by $\leq_{lex}$. It results that $(V, \leq_{lex})$ is a totally ordered set. Let $V = \{w_1, w_2, ..., w_n\}$, with $w_1 \geq_{lex} w_2 \geq_{lex} ... \geq_{lex} w_n$. From here, we obtain that $w_1 = \underbrace{11...1}_{n-\text{time}}$ and $w_n = \underbrace{00...0}_{(n-1)-\text{time}}1$. On V we define a partial order $\preceq$ as in Remark 1.4. Now, $(V, \preceq)$ is a partial ordered set with $w_1 \preceq w_i, i \in \{1, 2, ..., n\}$. We remark that $w_1 = \theta$ is the "zero" in $(V, \preceq)$ and w_n is a maximal element in $(V, \preceq)$. We define on $(V, \preceq)$ a binary relation " $*$ " as in Proposition 2.1. It results that $X = (V, *, w_1)$ becomes a BCK-algebra and V is isomorphic to $\mathcal{C}_n$ as BCK-algebras. We consider $A = V$ and the identity map $f : A \to V, f(w) = w$ as a BCK-function. The decomposition of f provides a family of maps $V_{\mathcal{C}_n} = \{f_r : A \to \{0,1\} \ / \ \ f_r(x) = 1, \text{ if and only if } \ r * f(x) = \theta, \forall x \in A, r \in X\}$. This family is the binary block-code V relative to the order relation $\preceq$. Indeed,

let $w_k \in V, 1 < k < n$, $w_k = \underbrace{00...0}_{k-1} x_{i_k}...x_{i_n}$, $x_{i_k}...x_{i_n} \in \{0,1\}$. If $x_{i_j} = 0$, it results that $w_k \preceq w_{i_j}$ and $w_k * w_{i_j} = \theta$. If $x_{i_j} = 1$, we obtain that $w_{i_j} \preceq w_k$ or w_{i_j} and w_k can't be compared, therefore $w_k * w_{i_j} = w_k$.□

Remark 2.3. Using technique developed in [Ju, So; 11], we remark that a BCK-algebra determines a unique binary block-code, but a binary block-code as in Theorem 2.2 can be determined by two or more algebras(see Example 3.1). If two BCK-algebras, A_1, A_2 determine the same binary block-code, we call them *code-similar algebras,* denoted by $A_1 \sim A_2$. We denote by $\mathfrak{C}_n$ the set of the binary block-codes of the form given in the Theorem 2.2.

Remark 2.4. If we consider $\mathfrak{B}_n$, the set of all finite BCK-algebras with n elements, then the relation code-similar is an equivalence relation on $\mathfrak{B}_n$. Let $\mathfrak{Q}_n$ be the quotient set. For $V \in \mathfrak{C}_n$, an equivalent class in $\mathfrak{Q}_n$ is $\widehat{V} = \{B \in \mathfrak{B}_n$ / B determines the binary block-code $V\}$.

Proposition 2.5. *The quotient set* $\mathfrak{Q}_n$ *has* $2^{\frac{(n-1)(n-2)}{2}}$ *elements, the same cardinal as the set* $\mathfrak{C}_n$.

Proof. We will compute the cardinal of the set $\mathfrak{C}_n$. For $V \in \mathfrak{C}_n$, let M_V be its associated matrix. This matrix is upper triangular with $m_{ii} = 1$, for all $i \in \{1, 2, ..., n\}$. We calculate in how many different ways the rows of such a matrix can be written. The second row of the matrix M_V has the form $(0, 1, a_3, ..., a_n)$, where $a_3, ..., a_n \in \{0, 1\}$. Therefore, the number of different rows of this type is 2^{n-2} and it is equal with the number of functions from a set with $n-2$ elements to the set $\{0,1\}$. The third row of the matrix M_V has the form $(0, 0, 1, a_4, ..., a_n)$, where $a_4, ..., a_n \in \{0, 1\}$. In the same way, it results that the number of different rows of this type is 2^{n-3}. Finally, we get that the cardinal of the set $\mathfrak{C}_n$ is $2^{n-2}2^{n-3}...2 = 2^{\frac{(n-1)(n-2)}{2}}$.□

Remark 2.6. If $\mathfrak{N}_n$ is the number of all finite non-isomorphic BCK-algebras with n elements, then $\mathfrak{N}_n \geq 2^{\frac{(n-1)(n-2)}{2}}$.

Remark 2.7. 1) Let $V_1, V_2 \in \mathfrak{C}_n$ and M_{V_1}, M_{V_2} be the associated matrices. We denote by $r_j^{V_i}$ a row in the matrix $M_{V_i}, i \in \{1, 2\}$, $j \in \{1, 2, ..., n\}$. On $\mathfrak{C}_n$, we define the following totally order relation

$V_1 \succeq_{lex} V_2$ if there is $i \in \{2, 3, ..., n\}$ such that $r_1^{V_1} = r_1^{V_2}, ..., r_{i-1}^{V_1} = r_{i-1}^{V_2}$ and $r_i^{V_1} \geq_{lex} r_i^{V_2}$,

where $\geq_{lex}$ is the lexicographic order.

2) Let $V_1, V_2 \in \mathfrak{C}_n$ and M_{V_1}, M_{V_2} be the associated matrices. We define a partially order on $\mathfrak{C}_n$

$V_1 \ll V_2$ if there is $i \in \{2,3,...,n\}$ such that $r_1^{V_1} = r_1^{V_2}, ..., r_{i-1}^{V_1} = r_{i-1}^{V_2}$ and $r_i^{V_1} \preceq r_i^{V_2}$,

where $\preceq$ is the order relation given by the relation (1.1).

3) Let $\Theta = (\theta_{ij})_{i,j\in\{1,2,...,n\}} \in \mathcal{M}(\{0,1\})$ be a matrix such that $\theta_{ij} = 1$, $i \leq j$, for all $i, j \in \{1,2,...,n\}$ and $\theta_{ij} = 0$ in the rest. It results that the code Ω, such that $M_\Omega = \Theta$, is the minimum element in the partial ordered set $(\mathfrak{C}_n, \ll)$, where elements in $\mathfrak{C}_n$ are descending ordered relative to $\succeq_{lex}$ defined in 1). Using the multiplication " $*$ " given in relation (2.1) and Proposition 2.1, we obtain that $(\mathfrak{C}_n, *, \Omega)$ is a non-commutative and non-implicative BCK-algebra. Due to the above remarks and relation (2.1), this BCK-algebra determines a binary block-code $V_{\mathfrak{C}_n}$ of length $2^{\frac{(n-1)(n-2)}{2}}$. Obviously, $\widehat{V}_{\mathfrak{C}_n} \in \mathfrak{C}_{2^{\frac{(n-1)(n-2)}{2}}}$.

Proposition 2.8. *Let* $A = (a_{i,j})_{\substack{i\in\{1,2,...,n\}\\ j\in\{1,2,...,m\}}} \in \mathcal{M}_{n,m}(\{0,1\})$ *be a matrix with rows lexicographic ordered in the descending sense. Starting from this matrix, we can find a matrix* $B = (b_{i,j})_{i,j\in\{1,2,...,q\}} \in \mathcal{M}_q(\{0,1\})$, $q = n+m$, *such that* B *is an upper triangular matrix, with* $b_{ii} = 1, \forall i \in \{1,2,...,q\}$ *and* A *becomes a submatrix of the matrix* B.

Proof. We insert in the left side of the matrix A (from the right to the left) the following n new columns of the form $\underbrace{00...01}_{n}, \underbrace{00...10}_{n}, ..., \underbrace{10...00}_{n}$. It results a new matrix D with n rows and $n+m$ columns. Now, we insert in the bottom of the matrix D the following m rows: $\underbrace{00...010...00}_{n \quad m}$, $\underbrace{00...001...00}_{n+1 \quad m-1}$, ..., $\underbrace{000}_{n+m-1}$ 1. We obtained the asked matrix B.□

Theorem 2.9. *With the above notations, we consider* V *a binary block-code with* n *codewords of length* $m, n \neq m$, *or a block-code with* n *codewords of length* n *such that the codeword* $\underbrace{11...1}_{n-\text{time}}$ *is not in* V, *or a block-code with* n *codewords of length* n *such that the matrix* M_V *is not upper triangular. There are a natural number* $q \geq \max\{m,n\}$, *a set* A *with* m *elements and a*

BCK-function $f : A \to \mathcal{C}_q$ such that the obtained block-code $V_{\mathcal{C}_n}$ contains the block-code V as a subset.

Proof. Let V be a binary block-code, $V = \{w_1, w_2, ..., w_n\}$, with codewords of length m. We consider the codewords $w_1, w_2, ..., w_n$ lexicographic ordered, $w_1 \geq_{lex} w_2 \geq_{lex} ... \geq_{lex} w_n$. Let $M \in \mathcal{M}_{n,m}(\{0,1\})$ be the associated matrix with the rows $w_1, ..., w_n$ in this order. Using Proposition 2.8, we can extend the matrix M to a square matrix $M' \in \mathcal{M}_q(\{0,1\}), q = m + n$, such that $M' = \left(m'_{i,j}\right)_{i,j \in \{1,2,...,q\}}$ is an upper triangular matrix with $m_{ii} = 1$, for all $i \in \{1, 2, ..., q\}$. Since the first line of the matrix M' is not $\underbrace{11...1}_{q}$, then we insert the row $\underbrace{11...1}_{q+1}$ as a first row and the column $\underbrace{10...0}_{q}$ as a first column . Applying Theorem 2.2 for the matrix M', we obtain a BCK-algebra $\mathcal{C}_q = \{x_1, ..., x_q\}$,with $x_1 = \theta$ the zero of the algebra $\mathcal{C}_q$ and a binary block-code $V_{\mathcal{C}_q}$. Assuming that the initial columns of the matrix M have in the new matrix M' positions $i_{j_1}, i_{j_2}, ..., i_{j_m} \in \{1, 2, ..., q\}$, let $A = \{x_{j_1}, x_{j_2}, ..., x_{j_m}\} \subseteq \mathcal{C}_q$. The BCK-function $f : A \to \mathcal{C}_q, f(x_{j_i}) = x_{j_i}$, $i \in \{1, 2, ..., m\}$, determines the binary block-code $V_{\mathcal{C}_q}$ such that $V \subseteq V_{\mathcal{C}_q}$.□

3. Examples

Example 3.1. Let $V = \{0110, 0010, 1111, 0001\}$ be a binary block code. Using the lexicographic order, the code V can be written
$V = \{1111, 0110, 0010, 0001\} = \{w_1, w_2, w_3, w_4\}$. From Theorem 2.2, defining the partial order $\preceq$ on V, we remark that $w_1 \preceq w_i, i \in \{2, 3, 4\}, w_2 \preceq w_3, w_2$ can't be compared with w_4 and w_3 can't be compared with w_4. The operation " $*$ " on V is given in the following table:

$*$	w_1	w_2	w_3	w_4
w_1	w_1	w_1	w_1	w_1
w_2	w_2	w_1	w_1	w_2
w_3	w_3	w_3	w_1	w_3
w_4	w_4	w_4	w_4	w_1

.

Obviously, V with the operation " $*$ " is a BCK-algebra.

We remark that the same binary block code V can be obtained from the BCK-algebra $(A, \circ, \theta)$

$\circ$	θ	a	b	c
θ	θ	θ	θ	θ
a	a	θ	θ	a
b	b	a	θ	b
c	c	c	c	θ

with BCK-function, $f : V \to V, f(x) = x$.(see [Ju, So; 11] , Example 4.2). From the associated Cayley multiplication tables, it is obvious that the algebras $(A, \circ, \theta)$ and $(V, *, w_1)$ are not isomorphic. From here, we obtain that BCK-algebra associated to a binary block-code as in Theorem 2.2 is not unique up to an isomorphism. We remark that the BCK-algebra $(A, \circ, \theta)$ is commutative and non implicative and BCK-algebra $(V, *, w_1)$ is non commutative and non implicative. Therefore, if we start from commutative BCK-algebra $(A, \circ, \theta)$ to obtain the code V, as in [Ju, So; 11], and then we construct the BCK-algebra $(V, *, w_1)$, as in Theorem 2.2, the last obtained algebra lost the commutative property even that these two algebras are code-similar.

Example 3.2. Let X be a non empty set and $\mathfrak{F} = \{f : X \to \{0, 1\} \ / \ f$ function$\}$. On $\mathfrak{F}$ is defined the following multiplication

$$(f \circ g)(x) = f(x) - min\{f(x), g(x)\}, \forall x \in X.$$

$(\mathfrak{F}, \circ, \mathbf{0})$, where $\mathbf{0}(x) = 0, \forall x \in X$, is an implicative BCK-algebra([Sa, Az; 11], Theorem 3.3 and Example 1).

If X is a set with three elements, we can consider $\mathfrak{F} = \{000, 001, 010, 011, 100, 101, 110, 111\}$ the set of binary block-codes of length 3. We have the following multiplication table.

$\circ$	000	001	010	011	100	101	110	111	The obtained binary code-words
000	000	000	000	000	000	000	000	000	11111111
001	001	000	001	000	001	000	001	000	01010101
010	010	010	000	000	010	010	000	000	00110011
011	011	010	001	000	011	010	001	000	00010001
100	100	100	100	100	000	000	000	000	00001111
101	101	100	101	100	001	000	001	000	00000101
110	110	110	100	100	010	010	000	000	00000011
111	111	110	101	100	011	010	001	000	00000001

We obtain the following binary block-code
$V = \{11111111, 01010101, 00110011, 00010001,$
$00001111, 00000101, 00000011, 00000001\}$, with the elements lexicographic ordered in the descending sense. From Theorem 2.2, defining the partial order $\preceq$ on V and the multiplication " $*$ ", we have that $(V, *, 11111111)$ is a non-implicative BCK-algebra and the algebras $(V, *, 11111111)$ and $(\mathfrak{F}, \circ, \mathbf{0})$ are code-similar.

Example 3.3. Let $V = \{11110, 10010, 10011, 00000\}$ be a binary block code. Using the lexicographic order, the code V can be written
$V = \{11110, 10011, 10010, 00000\} = \{w_1, w_2, w_3, w_4\}$. Let $M_V \in \mathcal{M}_{4,5}(\{0,1\})$ be the associated matrix, $M_V = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$. Using Proposition 2.8, we construct an upper triangular matrix, starting from the matrix M_V. It results the following matrices:
$D = \begin{pmatrix} 1 & 0 & 0 & 0 & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} \\ 0 & 1 & 0 & 0 & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\ 0 & 0 & 1 & 0 & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ 0 & 0 & 0 & 1 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{pmatrix}$ and

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} \\ 0 & 1 & 0 & 0 & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\ 0 & 0 & 1 & 0 & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ 0 & 0 & 0 & 1 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Since the first row is not $\underbrace{11...1}_{9}$, using Theorem 2.8, we insert a new row $\underbrace{11...1}_{10}$ as a first row and a new column $\underbrace{10...0}_{10}$ as a first column. We obtain the following matrix: $B' = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ 0 & 1 & 0 & 0 & 0 & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} \\ 0 & 0 & 1 & 0 & 0 & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\ 0 & 0 & 0 & 1 & 0 & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ 0 & 0 & 0 & 0 & 1 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$.

The binary block-code $W = \{w_1, ..., w_{10}\}$, whose codewords are the rows of the matrix B', determines a BCK-algebra $(X, *, w_1)$. Let $A = \{w_6, w_7, w_8, w_9, w_{10}\}$ and $f : A \to X, f(w_i) = w_i, i \in \{6, 7, 8, 9, 10\}$ be a BCK-function which determines the binary block-code
$U = \{11111, 11110, 10011, 10010, 00000, 10000, 01000, 00100, 00010, 00001\}$. The code V is a subset of the code U.

In the results presented above, we proved that to each binary block-code V we can associate a BCK-algebra X such that the binary block-code generated by X, V_X, contains the code V as a subset. In some particular case, we have $V_X = V$.

From Example 3.1 and 3.2, we remark that two code-similar BCK-algebras can't have the same properties. For example, some algebras from the same

equivalence class can be commutative and other non-commutative or some algebras from the same equivalence class can be implicative and other non-implicative. As a further research, will be very interesting to study what common properties can have two code-similar BCK-algebras.

Due to this connection of BCK-algebras with Coding Theory, we can consider the above results as a starting point in the study of new applications of these algebras in the Coding Theory.

ANNEX 1

Lemma 7.3, [Sch; 85], p.133

Let P_0 be a $q-$preordering, that is

$$P_0 + P_0 \subset P_0, K^2 P_0 \subset P_0, P_0 \cap -P_0 = 0.$$

Then there exists a $q-$ordering P with $P_0 \subset P$ or $-P_0 \subset P$. (It is not necessary that $1 \in P_0$)

Theorem 3.7 from [O' Sh; 10]

For $n = m + 1 + [\frac{m}{3}], s(Q(n)) \in [m+1, n]$, where $Q(n) = \left(\frac{x,y}{F}\right) \otimes_F F\left(< 1 > \perp n \times T_P\right)$, F a field of characteristic different from two.

Lemma from [Sch; 85], p.151

Let $n = 2^k$ and $\alpha_1, \alpha_2, ..., \alpha_n, \beta_1, \beta_2, ..., \beta_n \in K$. Then there are $\gamma_2, ..., \gamma_n \in K$ such that

$$\left(\alpha_1^2 + \alpha_2^2 + ... + \alpha_n^2\right)\left(\beta_1^2 + \beta_2^2 + ... + \beta_n^2\right) = \left(\alpha_1\beta_1 + ... + \alpha_n\beta_n\right)^2 + \gamma_2^2 + ... + \gamma_n^2.$$

Proposition 2.2. from [La,Ma; 01]

Let $k \geq 1$ be an integer, $F = F_0(x)$ be the rational function field in one variable over the formally real field F_0. Then the quadratic forms

$$\left(2^k + 1\right) \times < 1 > \perp 2^k \times < x > \text{ and } 2^k \times < 1, -x >$$

stay anisotropic over $F_0(x)(\alpha_k)$, where $\alpha_k = (2^k + 1) \times < 1, -x >$.

Lemma 2.5, [Hoff; 08]

Let φ be a quadratic form over a formally real field F, $dim\varphi \geq 2$, and let P be an ordering on F. Then P extends to $F(\varphi)$ if and only if φ is indefinite at P. In this situation, if 3c8 is another form over F, then $dim(3c8_{F(\varphi)})_{an} \geq |sgn_P(3c8)|$.

Theorem 4.1, [Ka, Me; 03]

Let X and Y be anisotropic quadrics over a field F and suppose that Y is isotropic over $F(X)$. Then

i) $dim_{es}(X) \leq dim_{es}(Y)$;

ii) Moreover, the equality $dim_{es}(X) = dim_{es}(Y)$ *holds if and only if X is isotropic over $F(Y)$.*

Theorem 3.8. from [O' Sh; 10]

i) $s(O(n)) \in [n - [\frac{n}{8}], n]$, *for all n.*

ii) $\underline{s}(Q(n)) \in [n - [\frac{n+3}{4}], n]$, *for all n.*

iii) $\underline{s}(O(n)) \in [n - [\frac{n+7}{8}], n]$, *for all n, where* $O(n) = \left(\frac{x,y,z}{F}\right) \otimes_F F(< 1 > \perp n \times T_P)$.

Theorem 65, [Sm; 04]

Let $n \leq 3$. Any univariate 2^n-onic polynomial $P(x)$ having a unique monomial of highest degree $n > 0$, has at least one root.

Theorem 1, [Ei, Ni; 44]

Let $f(x) = a_0 x a_1 x ... x a_n + \phi(x)$ *be a polynomial with x, a_i real quaternions, $a_i \neq 0$, and $\phi(x)$ be a polynomial as a sum of a finite number of similar monomials with degree $< n$. Therefore the equation $f(x) = 0$ has at least one solution.*

ANNEX 2

Lenstra's elliptic curves algorithm

The following presentation use ideas from the beautiful book *Rational Points on Elliptic Curves* of Silverman and Tate, [Si, Ta; 92].

For a polynomial of the form $f = a_0 + b_0x + b_1y + c_0x^2 + 2c_1xy + c_2y^2 + ...$, plain algebraic curve is the set $\{(x, y) \in \mathbb{R}^2 \ / \ f(x, y) = 0\}$. This curve is nonsingular or regular in a point (x_0, y_0) on f if at least one of the partial derivatives of f in this point is non-zero, that means $\frac{\partial f}{\partial x}(x_0, y_0) \neq 0$ or/and $\frac{\partial f}{\partial y}(x_0, y_0) \neq 0$.

An elliptic curve is considered a plane algebraic curve defined by an equation of the form (Weierstrass normal form)

$$y^2 = x^3 + ax + b$$

which is nonsingular. On such a curve, we consider a point O, the point at infinity.

For an elliptic curve, if we consider the discriminant $\Delta = -16\left(4a^3 + 27b^2\right)$, the curve is considered regular if and only if $\Delta \neq 0$.

We remark that an elliptic curve is symmetric about the axis x, therefore for any given point P, we can take $-P$, the opposite point. We will consider $-O$ to be just O.

If P and Q are two points on the curve, we can uniquely find a third point, $P + Q$, as follows. In this way, we define a law and a group structure:

- We draw the line between P and Q. This line will intersect the curves in a third point, R. We consider $P + Q$ to be $-R$, its opposite.

-When one of the points is O, we define $P + O = P = O + P$, therefore O becomes the identity of the group.

We consider an elliptic curve $\mathcal{C} : y^2 = x^3 - px - q$ on the $\mathbb{Q}$. The rational points of $\mathcal{C}$ are these points on $\mathcal{C}$ whose all coordinates $\mathbb{Q}$, including the point

at infinity. We will denote this points with $\mathcal{C}(\mathbb{Q})$ and with the above law forms we obtain a group structure.

Therefore, if P and Q are two points on $\mathcal{C}$ and $R = P + Q = (x_R, -y_R)$, we have

$$\begin{aligned} x_R &= \frac{(y_P - y_Q)^2}{(x_P - x_Q)^2} - x_P - x_Q, \\ y_R &= y_P + \frac{y_P - y_Q}{x_P - x_Q}(x_R - x_P), \end{aligned}$$

for $x_P \neq x_Q$.

If $x_P = x_Q$, we have $y_P = -y_Q$ and we include here the situation when $y_P = y_Q = 0$.

If $y_P = y_Q \neq 0$, it results $R = 2P = (x_R, -y_R)$ and we have

$$\begin{aligned} x_R &= \frac{(3x_P^2 - p)^2}{4y_P^2} - 2x_P, \\ y_R &= y_P + \frac{3x_P^2 - p}{2y_P}(x_R - x_P). \end{aligned}$$

Pollard's $p-1$ Algorithm. Let $n \geq 2$ be a non prime integer. We want find its prime factors.

Step 1. We choose a number k such that $k = lcm[1, 2, 3, ..., K]$, K a fixed integer, therefore k is a product of small prime numbers at small powers.

Step 2. We choose an arbitrary integer a such that $1 < a < n$.

Step 3. We compute $d = gcd(a, n)$. If $d > 1$, therefore d is a nontrivial factor of the number n. Otherwise, we go to the Step 4.

Step 4. We compute $d = gcd(a^k - 1, n)$. If $1 < d < n$, then d is a nontrivial factor of n and the algorithm stops here. If $d = 1$, we go to the Step 1 and we chose a big integer k by increasing the value of K. If $d = n$, we go to the Step 2 and we choose another number a.

Complexity: $O(n^{1/2+\varepsilon})$.

The Pollard's algorithm uses the fact that the nonzero elements from $\mathbb{Z}_p$ forms a group of $p-1$ order. Therefore, if $(p-1) \mid k$, then $a^k = 1$ in this group. Lenstra had the idea to replace the group $\mathbb{Z}_p$ with the rational points on an elliptic curve, $\mathcal{C}(\mathbb{Z}_p)$, and to replace the integer a with a point $P \in \mathcal{C}(\mathbb{Z}_p)$. As in the Pollard's algorithm, we choose an integer k such that k is a product of

small primes at small powers. If the cardinal of the set $\mathcal{C}(\mathbb{Z}_p)$, denoted $|\mathcal{C}(\mathbb{Z}_p)|$, if $|\mathcal{C}(\mathbb{Z}_p)| \mid k$, we have $kP = O$ in $\mathcal{C}(\mathbb{Z}_p)$ and the fact that $kP = O$ in $\mathcal{C}(\mathbb{Z}_p)$ is used to find a nontrivial divisor of n.

The Lenstra's algorithm for elliptic curves. Let $n \geq 2$ be a integer. We want find the prime factors of the number n.

Step 1. We check if $gcd(n, 6) = 1$ and if is not on the form m^r for $r \geq 1$.

Step 2. We choose the integers $1 \leq b, x_1, y_1 \leq n$.

Step 3. We consider $c = y_1^2 - x_1^3 - bx_1 \bmod n$ and let C the elliptic curve

$$C : y^2 = x^3 + bx + c$$

with $P = (x_1, y_1) \in C$.

Step 4. We check if $D = gcd(4b^3 + 27c^2, n) = 1$. If $D = n$, we choose a new b. If $1 < b < n$, then $D \mid n$.

Step 5. We search a number k such that k is a product of small primes at small powers, $k = lcm[1, 2, 3, ..., K]$, K a fixed integer.

Step 6. We compute

$$kP = \left(\frac{a_k}{d_k^2}, \frac{b_k}{d_k^2}\right).$$

Step 7. We compute $D' = gcd(d_k, n)$. If $1 < D' < n$, then D' is a nontrivial factor of n. If $D = 1$, we go to the Step 5 and increase k or we go to Step 2 and we choose another curve. If $D = n$, then we go to Step 5 and decrease k.

With Pollard's $p - 1$ algorithm we use the groups of the form $\mathbb{Z}_p^*$, which p is a prime divisor of the number n. For a fixed n the group $\mathbb{Z}_p^*$ is fixed. If we use the Lenstra's algorithm on elliptic curves on the field $\mathbb{Z}_p$ we have various groups which can be utilized depending on the chosen curves and the chances to find a group whose order is not divisible with a big prime or with a power of big prime. With a Lenstra's algorithm we have a kind of flexibility which allow us to find another elliptic curve and we can restart the algorithm.

ANNEX 3

QAM-constelation

For the following presentation, we use Wikipedia.org. A constellation diagram is considered a representation for a signal modulated using a digital modulation scheme, as for example quadrature amplitude modulation, QAM. The signal is represented in a diagram in a two-dimensional complex plane with axes $X-Y$. Such a diagram represents as points in the complex plane a possible symbols which can be selected from a given modulation scheme. With such a diagram, we can recognize which type of interference and distortion for a signal we have.

The constellation diagram is useful for QAM, in which the constellation points can be usually arranged in a geometric figure as for example a square grid in which the vertical and horizontal spacing are equal. The number of points in the grid is usually a power of 2 since in digital telecommunications the data are usually binary. Therefore, we have 16-QAM, 64-QAM, etc. We must remark that, by moving to a higher-order constellation, it is possible to obtain a good advantage: to transmit more bits per symbol.

When a signal is received, the decoder examines the received symbol. This signal can be corrupted by the channel or the receiver. The decoder can estimate and select the closet point from the constellation diagram, using usually an Euclidean distance or another defined distances. Therefore it will decode incorrectly if the corruption has caused that the received symbol can be moved closer to another constellation point than the transmitted one. In this sense, the constellation diagram give us a straightforward visualization of this process.

See two constellations: $\mathbb{Z}[i]_\pi$ for $\pi = 2 + i$ and for $16-$QAM.

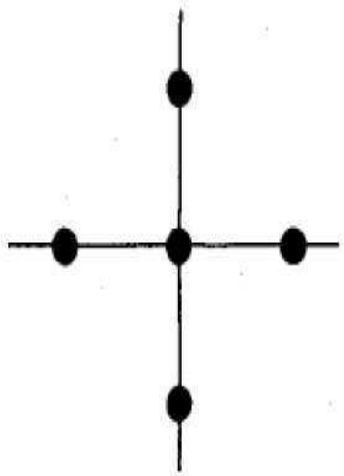

Fig. 1:(From [Hu; 09]) $\mathbb{Z}[i]_\pi$ for $\pi = 2 + i$

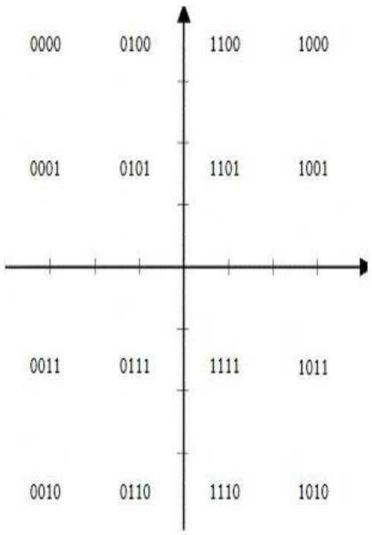

Fig. 2: 16-QAM, from Wikipedia.org

(B-iii) Bibliography

[Ab, Si; 07] Abualrub, T., Siap, I., *Cyclic codes over the rings* $\mathbb{Z}_2 + u\mathbb{Z}_2$ *and* $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$, Des Codes Cryptogr., **42(3)**(2007), 273–287.

[Al; 98] Alamouti, S.M., *A simple transmit diversity technique for wireless communications,* IEEE J. Selected Areas Communications, **16**(1998), 1451-1458.

[Al, Ha; 10] Al-Ashker, M. M., Hamoudeh, M., *Cyclic codes over* $\mathbb{Z}_2 + u\mathbb{Z}_2 + ... + u^{k-1}\mathbb{Z}_2$, Turk. J. Math. **34**(2010), 1–13.

[Al; 49] Albert, A. A., *Absolute-valued algebraic algebras*, Bull. Amer. Math. Soc., **55**(1949), 763-768.

[Al; 39] Albert, A. A., *Structure of algebras*, Amer. Math. Soc. Colloquium Publications, vol. **24**, 1939.

[Ak, Ke; 14] Akkus, I., Keçilioğlu, O., *Split Fibonacci and Lucas Octonions*, Advances in Applied Clifford Algebras, 2014,
http://link.springer.com/article/10.1007/s00006-014-0515-8.

[Ba; 01] Baez, J.C., *The Octonions*, B. Am. Math. Soc., **39(2)**(2001), 145-205, http://www.ams.org/journals/bull/
2002-39-02/S0273-0979-01-00934-X/S0273-0979-01-00934-X.pdf.

[Ba; 09] Bales, J. W., *A Tree for Computing the Cayley-Dickson Twist*, Missouri J. Math. Sci., **21(2)(**2009**)**, 83–93.

[Be, Re; 03] Belfiore, J.C., Rekaya, G., Quaternionic Lattices for Space-Time Coding, ITW2003, Paris,2003.

[Be, Og; 13] Berhuy, G., Oggier, F., *An Introduction to Central Simple Algebras and Their Applications to Wireless Communication,* AMS, 2013.

[Bl; 72] Blake, I. F., *Codes over certain rings*, Inf. Control **20**(1972), 396–404.

[B,Fa, Fl, Ku; 15] Borumand Saeid, A., Fatemidokht, H., **Flaut, C.**, Kuchaki Rafsanjanib, M., On codes based on BCK-algebras, Journal of Intelligent & Fuzzy Systems **29**(2015) 2133–2137.

[Br; 67] Brown, R. B., *On generalized Cayley-Dickson algebras*, Pacific J. of Math., **20(3)**(1967), 415-422.

[Ch; 98] Cho, E., *De-Moivre's formula for quaternions*, Appl. Math. Lett., **11**(6)(1998), 33-35.

[Co, Sm; 03] Conway, J.H. , Smith, D.A., *On Quaternions and Octonions*, A.K. Peters, Natick, Massachusetts, 2003.

[Co; 89] Cox, D., *Primes of the Form x^2+ny^2: Fermat, Class Field Theory and Complex Multiplication*, A Wiley - Interscience Publication, New York, 1989.

[Da, La, Pe; 80] Dai, Z.D., Lam, T. Y., Peng, C. K., *Levels in algebra and topology,* Bull. Amer. Math. Soc., **3**(1980),845-848.

[Da, Sa, Va; 03] Davidoff, G., Sarnak, P., Valette, A., *Elementary Number Theory, Group Theory, and Ramanujan Graphs*, Cambridge University Press, 2003.

[Dr, Gi, Gr, Wa; 03] Dress, A., Giegerich, R., Grűnewald, S., Wagner, H., *Fibonacci-Cayley Numbers and Repetition Patterns in Genomic DNA*, Ann. Comb. **7**(2003), 259–279.

[Ei, Ni; 44] Eilenberg, S., Niven, I., *The fundamental theorem of algebra for quaternions*, Bull. Amer. Math. Soc., **50** (1944), 246-248.

[Er, Oz; 13] Erdoğdu, M., Özdemir, M., *Two-sided linear split quaternionic equations with unknowns*, Linear and Multilinear Algebra, DOI:10.1080/03081087.2013.851196.

[Fl; 14] Flaut, C., *About some properties of algebras obtained by the Cayley-Dickson process,* Palestine Journal of Mathematics , **3(1)**(2014), 388-394, http://pjm.ppu.edu/vol_3_3/7.pdf , http://pjm.ppu.edu/?page=volumes&vol=3_3.

[Fl; 14(1)] Flaut, C., *A Clifford algebra associated to generalized Fibonacci quaternions,* Adv. Differ. Equ.-NY, 2014:279, p.1-7.

[Fl; 15(2)] Flaut, C., *BCK-algebras arising from block-codes,* Journal of Intelligent & Fuzzy Systems **28**(2015) 1829–1833.

[Fl; 15(1)] Flaut, C., *Codes over a subset of Octonion Integers,* Results Math., 68(3)(2015), 348-359.

[Fl; 16] Flaut, C., *Codes over subsets of algebras obtained by the Cayley-Dickson process,* submitted.

[Fl; 13(1)] Flaut, C., *Cyclic codes over some special rings*, Bull. Korean Math. Soc., **50(5)**(2013), 1513-1521.

[Fl; 11] Flaut, C., *Isotropy of some quadratic forms and its applications on levels and sublevels of algebras,* J. Math. Sci. Adv. Appl., **12(2)**(2011), 97-117.

[Fl; 13] Flaut, C., *Levels and sublevels of algebras obtained by the Cayley-Dickson process*, Ann. Mat. Pura Appl., **192(6)**(2013), 1099-1114.

[Fl; 01] Flaut, C., *Some equations in algebras obtained by the Cayley-Dickson process*, An. St. Univ. Ovidius Constanta, **9(2)**(2001), 45-68.

[Fl, Sa; 15] Flaut, C., Savin, D., *Quaternion Algebras and Generalized Fibonacci-Lucas Quaternions,* Adv. Appl. Clifford Algebras, **25(4)(**2015**),** 853-862.

[Fl, Sh; 13] Flaut, C., Shpakivskyi, V., *On Generalized Fibonacci Quaternions and Fibonacci-Narayana Quaternions*, Adv. Appl. Clifford Algebras, **23(3)**(2013), 673-688.

[Fl, Sh; 13(2)] Flaut, C., Shpakivskyi, V., *Real matrix representations for the complex quaternions*, Adv. Appl. Clifford Algebras, **23(3)**(2013), 657-671.

[Fl, Sh; 13(1)] Flaut, C., Shpakivskyi, V., *Some identities in algebras obtained by the Cayley-Dickson process,* Adv. Appl. Clifford Algebras, **23(1)**(2013), 63-76.

[Fl, Sh; 15(1)] Flaut, C., Shpakivskyi, V., *Holomorphic Functions in Generalized*

Cayley-Dickson Algebras, Adv. Appl. Clifford Algebras, **25(1)**(2015), 95-112.

[Fl, Sh; 15(2)] Flaut, C., Shpakivskyi, V., *An Efficient Method for Solving Equations in Generalized Quaternion and Octonion Algebras,* Adv. Appl. Clifford Algebras, **25(2)**(2015), 337–350.

[Fl, Sh; 15(3)] Flaut, C., Shpakivskyi, V., *Some remarks about Fibonacci elements in an arbitrary algebra*, Bull. Soc. Sci. Lettres Łódź Sér. Rech. Déform., **65(3)**(2015).

[Fl, Şt; 09] Flaut, C., Ştefănescu, M., *Some equations over generalized quaternion and octonion division algebras*, Bull. Math. Soc. Sci. Math. Roumanie, **52(4)**(100)(2009), 427–439.

[Ga, Pe; 11] Garibaldi, S., Petersson, H. P., *Wild Pfister forms over Henselian fields, K-theory, and conic division algebras*, J. Algebra, **327**(2011), 386-465.

[Gr; 97] Greferath, M., *Cyclic codes over finite rings*, Discrete Math. **177(1-3)**(1997), 273–277.

[Gh, Fr; 10] F. Ghaboussi, J. Freudenberger, *Codes over Gaussian integer rings*, 18th Telecommunications forum TELFOR 2010, 662-665.

[Gi, Mu; 91] Gilbert, J. E., Murray, M.A.M., *Clifford Algebras and Dirac Operators in Harmonic Analysis,* Cambridge University Press, 1991.

[Gu; 13] M. Güzeltepe, *Codes over Hurwitz integers*, Discrete Math., **313(5)(**2013**)**, 704-714.

[Ha; 12] Halici, S., *On Fibonacci Quaternions*, Adv. in Appl. Clifford Algebras **22(2)**(2012), 321-327.

[Ha; 43] Hall, M., *Projective planes*, Trans. Amer. Math. Soc. vol. **54**(1943), 229-277.

[He; 97] Hentzel, I. R., *Identities of Cayley-Dickson Algebras*, J Algebra, **188**(1997), 292-309.

[Hoff; 08] Hoffman, D. W., *Levels of quaternion algebras*, Archiv der Mathematik, **90(5)**(2008), 401-411.

[Hoff; 10] Hoffman, D. W, *Levels and sublevels of quaternion algebras,* Mathematical Proceedings of the Royal Irish Academy, **110A(1)**(2010), 95-98.

[Ho; 08] Hollanti, C., *Order-Theoretic Method for Space-Time Coding: Symmetric and Assymetric Designs,* TUCS Dissertations, No. 111, 2008.

[Ho, Ju; 03] Hong, S. M., Jun, Y. B., Öztürk, M. A., *Generalizations of BCK-algebras*, Sci. Math. Jpn. Online, **8(**2003**)**, 549–557.

[Ho; 61] Horadam, A. F., *A Generalized Fibonacci Sequence*, Amer. Math. Monthly, **68**(1961), 455-459.

[Ho; 63] Horadam, A. F., *Complex Fibonacci Numbers and Fibonacci Quaternions*, Amer. Math. Monthly **70**(1963), 289-291.

[Hu; 94] Huber, K., *Codes over Gaussian integers*, IEEE Trans. Inform. Theory, **40(**1994**),** 207–216.

[Im, Is; 66] Imai, Y., Iseki, K., *On axiom systems of propositional calculi*, Proc. Japan Academic, **42(**1966**)**, 19-22.

[Is; 84] Isaev, I. M., *Identities of a finite Cayley-Dickson Algebra*, Algebra i Logika, **23(4)**(1984), 407-418.

[Is, Ta; 78] Iséki, K., Tanaka, S., *An introduction to the theory of BCK-algebras*, Math. Jpn. **23(**1978**)**, 1–26.

[Ja, Op; 10] Janovská, D., Opfer, G., *A note on the computation of all zeros of simple quaternionic polynomials*, Siam J. Numer. Anal., **48(1)**(2010), 244-256.

[Ja, Op; 13] Janovská, D., Opfer, G., *Linear equations and the Kronecker product in coquaternions*, Mitt. Math. Ges. Hamburg **33** (2013), 181-196.

[Ju, So; 11] Jun, Y. B., Song, S. Z., *Codes based on BCK-algebras*, Inform. Sciences., **181(**2011**)**, 5102-5109.

[Ka, Me; 03] Karpenko, N.A., Merkurjev, A.S., *Essential dimension of quadratics*, Inventiones Mathematicae, **153**(2003), 361-372.

[Ki, Ou; 99] El Kinani, E. H., Ouarab, A., *The Embedding of $U_q(sl\,(2))$ and Sine Algebras in Generalized Clifford Algebras*, Adv. Appl. Clifford Algebr., **9(1)**(1999), 103-108.

[Kn; 76] Knebusch, M., *Generic splitting of quadratic forms I*, Proc. London Math. Soc. **33**(1976), 65-93.

[Kn; 88] Knus, M. A., *Quadratic Forms, Clifford Algebras and Spinors*, IMECC-UNICAMP, 1988.

[Ko; 10] Koç, C., *C-lattices and decompositions of generalized Clifford algebras,* Adv. Appl. Clifford Algebr., **20(2)**(2010), 313-320.

[Kos; 01] Koshy, T., *Fibonacci and Lucas Numbers with Applications*, A Wiley-Interscience publication, U.S.A, 2001.

[Ko, Ma, Mo; 10] H. Kostadinov, N. Manev, H. Morita, *On ($\pm$1) Error*

Correctable Integer Codes, http://math.nsc.ru/conference/acct2010/kostadinov-manev-morita.pdf.

[Ko, Mo, Ii, Ha, Ma; 10] Kostadinov, H., Morita, H., Iijima, N., Han Vinck, A. J., Manev, N., S*oft Decoding Of Integer Codes and Their Application to Coded Modulation*, IEICE Trans. Fundamentals, **E39A(7)(**2010**)**, 1363-1370.

[Ko; 98] Koprowski, P. *Sums of squares of pure quaternions*, Proc. Roy. Irish Acad., **98(1)**(1998),63-65.

[Kr, Wa; 91], Küskemper, M., Wadsworth, A., *A quaternion algebra of sublevel 3*, Bull. Soc. Math. Belg. Sér. B, **43(2)**(1991), 181-185.

[La; 04] Lam, T.Y., *Introduction to Quadratic Forms over Fields*, American Mathematical Society, 2004.

[La, Ma; 01] Laghribi A., Mammone P., *On the level of a quaternion algebra*, Comm. Algebra, **29(4)**(2001), 1821-1828.

[Le; 90] Leep, D. B., *Levels of division algebras*, Glasgow Math. J. **32**(1990), 365-370.

[Lew; 87] Lewis, D. W., *Levels and sublevels of division algebras*, Proc. Roy. Irish Acad. Sect. A, **87(1)**(1987), 103-106.

[Lew; 89] Lewis, D. W., *Levels of quaternion algebras*, Rocky Mountain J, Math. **19**(1989), 787-792.

[Lew; 06] Lewis, D. W., *Quaternion Algebras and the Algebraic Legacy of Hamilton's Quaternions*, Irish Math. Soc. Bulletin **57**(2006), 41–64.

[Li, Xi; 04] Ling, S., Xing, C., *Coding Theory: A First Course*, Cambridge University Press, 2004.

[Ma,Be, Ga; 09] Martinez, C., Beivide, R., Gabidulin, E., *Perfect codes from Cayley graphs over Lipschitz integers*, IEEE Trans. Inform. Theory **55(8)(**2009**),** 3552–3562.

[Ma, Ja; 13] Mamagani, A. B., Jafari, M., *On Properties of Generalized Quaternion Algebra*, J. Novel Appl. Sci., **2(12)**(2013), 683-689.

[Mc; 85] McCrimmon, K., *Nonassociative algebras with scalar involution*, Pacific J. of Math. **116(1)(**1985**)**, 85-108.

[McC; 80] McCrimmon, K., *Pre-book on Alternative Algebras*, 1980, http://mysite.science.uottawa.ca/neher/Papers/alternative/

http://mysite.science.uottawa.ca/neher/Papers/alternative/2.2.Composition%20algebras.pdf.

[Mi; 11] Mierzejewski, D. A., *Linear manifolds in sets of solutions of quaternionic polynomial equations of several types*, Adv. Appl. Clifford Alg., **21**(2011), 417-428.

[Mi; 10] Mierzejewski, D. A., *Spheres in sets of solutions of quadratic quaternionic equations of some types*, Bull. Soc. Sci. Lett. Lódź, Ser. Rech. Déform., **60**(1)(2010), 49-58.

[Mi, Sz; 08] Mierzejewski, D. A., Szpakowski, V. S., *On solutions of some types of quaternionic quadratic equations*, Bull. Soc. Sci. Lett. Lódź **58**, Ser. Rech. Déform., **55** (2008), 49-58.

[Mo, Ha, Ko; 04] Morita, H., Han Vinck, A. J., Kostadinov, H., *On Soft Decoding of Coded QAM Using Integer Codes*, International Symposium on Information Theory and its Applications, ISITA2004, Parma, Italy, 1321-1325.

[Ne, In, Fa, Pa; 01] da Neto, T.P.N., Interlando, J.C., Favareto, M.O., Elia, M., Palazzo Jr.,R., *Lattice constellation and codes from quadratic number fields*, IEEE Trans. Inform.Theory **47(4)(**2001**)** 1514–1527.

[Ni; 41] Niven, I. *Equations in Quaternions*, Amer. Math. Monthly, **48**(1941), 654-661.

[Ni, Hi; 08] Nishimura, S., Hiramatsu, T., *A generalization of the Lee distance and error correcting codes*, Discrete Appl Math., **156(**2008**)**, 588 – 595.

[Og, Be, Vi; 07] Oggier, F., Belfiore, J-C., Viterbo, E., *Cyclic Division Algebras: A Tool for Space-Time Coding,* Communications and Information Theory, **4**(2007), 1-95.

[Og, Vi; 04] Oggier, F., Viterbo, E., A*lgebraic Number Theory and Code Design for Rayleigh Fading Channels,* Communications and Information Theory, **3**(2004), 333-415.

[Om; 62] O'Meara, O.T., *Introduction to Quadratic Forms*, Springer Verlag, 1962.

[O' Sh; 07] O' Shea, J., *Levels and sublevels of composition algebras*, Indag. Mathem., **18(1)**(2007), 147-159.

[O' Sh; 07(2)] O' Shea, J., *New values for the level and sublevel of composition algebras*, preprint, 2007, 1-21.

[O' Sh; 10] O' Shea, J., *Bounds on the levels of composition algebras*, Mathematical Proceedings of the Royal Irish Academy **110A(1)**(2010), 21-30.

[O' Sh; 11] O' Shea, J., *Sums of squares in certain quaternion and octonion algebras*, C.R. Acad. Sci. Paris Sér. I Math, **349**(2011), 239-242.

[Oz; 09] Özdemir, M., *The roots of a split quaternion*, Appl. Math. Lett., **22**(2009) 258-263.

[Pf; 65] Pfister, A., *Zur Darstellung von-I als Summe von quadraten in einem Körper*, J. London Math. Soc. **40**(1965), 159-165.

[Pl, Sh; 11] Plaksa, S.A., Shpakovskii, V. S., *Constructive description of monogenic functions in a harmonic algebra of the third rank*, Ukr. Math. J., **62 (8)**(2011), 1251–1266.

[Po, Ke; 15] Polatli, E., Kesim, S., *On quaternions with generalized Fibonacci and Lucas number components*, Advances in Difference Equations (2015) 2015:169.

[Po, Ro; 10] Pogoruy, A., Rodrigues-Dagnino, R. M., *Some algebraic and analytical properties of coquaternion algebra*, Adv. Appl. Clifford Alg., **20**(2010), 79-84.

[Pu, As; 06] Pumplűn, S., Astier, V., *Nonassociative Quaternion Algebras over Rings*, Isr. J. Math., 155(1)(2006), 125-147.

[Pu; 13] Pumplűn, S., *How to Obtain Division Algebras used for fast Decodable Space-Time Blocks Codes*, 2013,
http://molle.fernuni-hagen.de/~loos/jordan/archive/iteralg/iteralg.pdf.

[Pu; 05] Pumplün, S., *Sums of squares in octonion algebras*, Proc. Amer. Math. Soc., **133**(2005), 3143-3152.

[Pu, St; 15] Pumplűn, S., Steele, A., *The Nonassociative Algebras used to BuildFast-Decodable space-time Block-Codes,* 2015,
http://arxiv.org/pdf/1504.00182.pdf.

[Pu, Un; 11] Pumplűn, S., Unger T., *Space-time block codes from nonassociative division algebras*, Advances in Mathematics of Communications, **5(3)**(2011), 449-471.

[Qi, Zh, Zhu; 05] Qian, J.-F., Zhang, L.-N., Zhu, A.-X., *Cyclic codes over* $\mathbb{F}_p + u\mathbb{F}_p + \cdots + u^{k-1}\mathbb{F}_p$, IEICE Trans. Fundamentals Vol. E88-A, **3**(2005), 795–797.

[Ra; 88] Racine, M. L., *Minimal Identities of Octonions Algebras*, J Algebra, **115**(1988), 251-260.

[Ram; 15] Ramırez, J.L., *Hessenberg Matrices and the Generalized Fibonacci-Narayana Sequence*, Filomat, **29(7)**(2015), 1557–1563.

[Ri; 95] Rifà, J., *Groups of Complex Integer Used as QAM Signals*, IEEE Transactions on Information Theory, **41(5)**(1995), 1512-1517.

[Sa, Az; 11] Samaei, Z., Azadani, M. A., Ranjbar, L., *A Class of BCK-Algebras*, Int. J. Algebra, **5(28)(2011)**, 1379 - 1385.

[Sa-Mu; 82] Satyanarayana Murthy, P. V., *Fibonacci-Cayley Numbers,* The Fibonacci Quarterly, **20(1)**(1982), 59-64.

[Sc; 66] Schafer, R. D., *An Introduction to Nonassociative Algebras,* Academic Press, New-York, 1966.

[Sc; 54] Schafer, R. D., *On the algebras formed by the Cayley-Dickson process,* Amer. J. Math., **76**(1954), 435-446.

[Sch; 85] Scharlau, W., *Quadratic and Hermitian Forms,* Springer Verlag, 1985.

[Sh; 11] Shpakivskyi, V.S., *Linear quaternionic equations and their systems*, Adv. Appl. Clifford Alg., **21**(2011), 637-645.

[Si, Ta; 92] Silverman, J. H., Tate, J. T., *Rational Points on Elliptic Curves*, Springer-Verlag New York, 1992.

[Smi; 50] Smiley, M. F., *A remark on a theorem of Marshall Hall,* Proceedings of the American Mathematical Society, **1**(1950), 342-343.

[Sm; 91] Smith T. L., *Decomposition of Generalized Clifford Algebras*, Quart. J. Math. Oxford, **42**(1991), 105-112.

[Sm; 04] Smith, W. D., *Quaternions, octonions and now, 16-ons and* 2^n-*ons; New kinds of numbers*,
scorevoting.net/WarrenSmithPages/homepage/nce2.ps, 2004.

[Sp; 78] Spiegel, E., *Codes over* $\mathbb{Z}_m$ *revisited,* Inform. and Control **37(1)**(1978), 100–104.

[St; 09] Stankewicz, J., *Quaternion Algebras and Modular Forms*, 2009, http://stankewicz.net/quatalg.pdf.

[Sw; 73] Swamy, M. N. S., *On generalized Fibonacci Quaternions*, The Fibonacci Quaterly **11(5)**(1973), 547-549.

[Sz; 09] Szpakowski, V. S., *Solution of general quadratic quaternionic equations*, Bull. Soc. Sci. Lettres Łódź, Ser. Rech. Déform. **58**(2009), 45 – 58.

[Ta; 08] Tamm, U., *Integer Codes in Coding and Computing*, http://ita.ucsd.edu/workshop/10/files/paper/paper_250.pdf.

[Ta; 07] Tamm, U., *On Integer Codes*, http://ita.ucsd.edu/workshop/06/papers/149.pdf.

[Ta, Yi, Sa; 16] Tan, E., Yilmaz, S., Sahin, M., *On a new generalization of Fibonacci quaternions*, Chaos, Solitons & Fractals, **82**(2016), 1-4.

[Ti; 00] Tian,Y., *Matrix reprezentations of octonions and their applications,* Adv. in Appl. Clifford Algebras **10(1)**(2000), 61-90.

[Ti; 00(1)] Tian,Y., *Matrix Theory over the Complex Quaternion Algebra,* arXiv:math/0004005v1, 1 April 2000.

[Ti; 99] Tian, Y., *Similarity and cosimilarity of elements in the real Cayley-Dickson algebras*, Adv. Appl. Clifford Algebras, **9(1)**(1999), 61-76.

[Ti, Va; 87] Tignol, J.-P., Vast, N., *Representation de -1 comme somme de carré dans certain algèbres de quaternions*, C.R. Acad. Sci. Paris Sér. Math. 305, **13**(1987), 583-586.

[Un, Ma; 11] Unger, T., Markin, N., *Quadratic Forms and Space-Time Block Codes from Generalized Quaternion and Biquaternion Algebras*, Information Theory, IEEE Transactions, **57(9)**(2011), 6148-6156.

[Va; 75] Van Lint, J.H., *A survey of perfect codes*, Rocky Mt. J. Math., **5(2)**(1975), 199-223.

[Vi, Mo; 98] Vinck, A.J.H., Morita, H., *Codes over the ring of integers modulo m*, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E81–A, **10**(1998), 2013 – 2018.

[Vo; 14] Voight, J., *The arithmetic of quaternion algebras*, 2014, https://math.dartmouth.edu/˜m125s14/quat-book-041914.pdf.

[Wa; 87] Waterhouse, W.C., *Nonassociative quaternion algebras*, Algebras Groups Geom., **4(3)**(1987), 365-378.

[Wi; 08] Wilkins, D. R., *Course 214 Section 1: Basic Theorems of Complex Analysis,* 2008, http://www.maths.tcd.ie/~dwilkins/Courses/214/214S1_0708.pdf.

[Xi, Zh, Li; 05] Xing-min Li, Zhao Kai, Li-zhong Peng, *Characterization of octonionic analytic functions,* Complex Variables, Theory and Appl., **50(13)**(2005), 1031–1040.