Contributions to the study of algebras obtained by the Cayley Dickson process

Presentation of the habilitation thesis

Cristina Flaut

Braşov, 25 March 2016

This habilitation thesis summarizes original results obtained by the author in the study of algebras obtained by the Cayley-Dickson process.

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 presentation, we suppose that K is a commutative field with $charK \neq 2$ and A is an algebra over the field K.

We will 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, and the following multiplication on $A \oplus A$:

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

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:

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

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.

Algebras A_t of dimension 2^t obtained by the Cayley-Dickson process, described above, are 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 below. (See [Br; 67], [Fl; 12]).

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

Level and sublevel of algebras obtained by the Cayley-Dickson process

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.

From here, by straightforward computations, we obtain that the algebra A_i is a division algebra over the field $F_i = K(X_1, X_2, ..., X_i)$ of dimension 2^i.

From this construction, we can remark that the ground field is not big enough and must be extended.

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.

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

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

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 $m \in \mathbb{N}$.

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 $< \alpha_1, ...\alpha_n >$.

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.

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

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

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.

From the above, we remarked that for the quaternion division algebras (which is a noncommutative field) over a field, can have level 2^k or $2^k + 1$.We remark values $2^k + 1$which are different from the level of a commutative field. For the octonion division algebra, we have 2^k, $2^k + 1, 6$ and 7 as values for the level. Therefore, from here we can see that if we use these algebras, we can find other values. But algebras obtained by the Cayley-Dickson process are not division algebras, in generally. To solve this, we use the Brown's process and we found such a division algebras: A_i is a division algebra over the field $F_i = K(X_1, X_2, ..., X_i)$ of dimension 2^i. The problem is partial solved, since the ground field is not good and not big enough. We must extend the ground field.

For this purpose, we prove first the following results, denoted as in the habilitation thesis.

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

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 $K(X_1)\left(\sqrt{-X_1^2}\right)$.

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

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

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

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* $K_0(X_1, X_2, ..., X_t)(\varphi_{2^k+1})$.

Remark. 2.3.9. i) The algebra $A_t(n)$ has dimension 2^t and is not necessarily a division algebra, but this algebra is of level greater than 1.
ii) If ψ_m is anisotropic and φ_n is isotropic over K_n, then $s(A_t(n)) \in [m + 1, n]$.

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

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

for $t \geq 2$.□

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

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 tell us 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.

Further developments of this direction of study: **The study of isotropy over function fields of some special quadratic forms**

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?

The previous obtained results contribute to the development of this research domain and we intend to extend them in further papers. For this purpose, we recall some (open)problems which can be studied:

1. *An open problem.* As we can see above, the theory of quadratic forms gave us an application in the study of sums of squares in some algebraic structures. An open problem is IF exist quaternion division algebras of a prescribed level $n \in \mathbb{N} - \{0\}$?

2. *The study of isotropy over function fields of some special quadratic forms.* An important problem in the theory of quadratic forms is to determine which anisotropic forms become(or not) isotropic when such forms are extended to the function field of a given form. With the above notations, will be interesting to find

i) if $2^k \times < 1, -X_1 >$ is isotropic over $K_0(X_1)(\alpha_k)$ for $\alpha_k = (2^k + 1) \times < 1, -X_1 >$,

or

ii) if $n = s(A_t(n))$ then $(n-1) \times \mathbf{n}_C^{A_t(n)}$ is anisotropic over $K_0(X_1, X_2, ..., X_t)(\varphi_n)$.

3. *The study of the case of function fields of some special quadratic forms* (as for example Pfister forms - a quadratic form of the type $\varphi =< 1, a_1, a_2, ..., a_n, a_1a_2, ..., a_1a_2a_3, ..., a_1a_2...a_n >$) can give us some answers.

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

Some identities in algebras obtained by the Cayley-Dickson process 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 division algebra (the square of any commutator is in the center). 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.

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

$$(xy - yx)^2 z = z (xy - yx)^2 . \quad (3.2.7.)$$

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:*

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

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

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

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

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).

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 $\mathbb{Z}_2^n$.

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

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

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*:

□

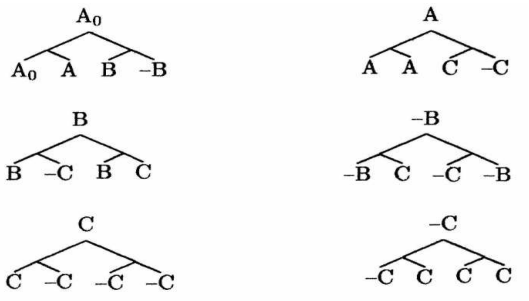

Fig. 1: Twist trees([1], Table 9)

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 trees. We remark that "00"= unchanged, "01" =left →right, "10"=right→ left, "11"=right → right.

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

$$e_1e_2, (e_1e_2)\, e_4, ..., ((e_{2^r}e_{2^{r+1}})\dots e_{2^k})e_{2^i},$$

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

$$\{1 = e_0, e_1, e_2, \dots, e_{2^{t-1}-1}, e_{2^{t-1}}, e_1e_{2^{t-1}}, e_2e_{2^{t-1}}, e_3e_{2^{t-1}}, \dots, e_{2^{t-1}-1}e_{2^{t-1}}\} \tag{3.3.2.}$$

with

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

Proposition 3.3.6. ([Fl, Sh; 15(1)]) *Let $A_t = \left(\frac{-1,...,-1}{\mathbb{R}}\right)$ 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*

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

$$((e_1e_{2^r})e_{2^{r+1}})\dots e_{2^k})e_{2^i} = (-1)^{k-r+3}\, e_{T+1}, \tag{3.3.5.}$$

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

$$e_1e_{2^i} = e_{2^i+1}. \tag{3.3.6.}$$

.

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

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*

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

, (3.3.9.)

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

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. A holomorphic function is a complex-valued function that is complex differentiable in a neighborhood of every point in its domain. If f is differentiable in $z_0 = x_0 + iy_0$, then u and v have continuos first partial derivatives with respect to x and y and satisfy the following relations

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

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. Therefore *if*

$$Df = 0 \tag{3.4.1,}$$

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

How we can generalize the definition of holomorphic functions to all algebras obtained by the Cayley-Dickson process?

Let $A_t = \left(\frac{\gamma_1,...,\gamma_t}{\mathbb{R}}\right)$, with $\gamma_1 = ... = \gamma_t = -1$, and the domain $\Omega \subset \mathbb{R}^{2^t}$. We denote with $\Omega_\zeta := \{\zeta = x_0 + x_1e_1 + \ldots + x_{n-1}e_{n-1} : (x_0, x_1, \ldots, x_{n-1}) \in \Omega\}$ a domain in A_t. The domain Ω_ζ is called *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 are continuos 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:

$$\phi_1 = x_0 + e_1x_1, \quad \phi_2 = \frac{1}{e_1}(x_0 + e_1x_1),$$

$$\rho_{2s-1}=x_{2s}-e_1x_{2s+1},\quad \rho_{2s}=-\frac{1}{e_1}(x_{2s}-e_1x_{2s+1}),\ \ s\in\{1,2,...,2^{t-1}-1\},$$

$$F_t(\zeta)=v(\phi_1,\phi_2)+v(\rho_1,\rho_2)e_2+v(\rho_3,\rho_4)e_4+[v(\rho_5,\rho_6)e_2]e_4+$$
$$+v(\rho_7,\rho_8)e_8+(v(\rho_9,\rho_{10})e_2)e_8+(v(\rho_{11},\rho_{12})e_4)e_8+[(v(\rho_{13},\rho_{14})e_2)e_4]e_8+...$$
$$...+\sum_{i=4}^{t-1}(\sum_{k=1}^{i}(\sum_{r=1}^{k-1}v(\rho_{M_{rki}-1},\rho_{M_{rki}})e_{2^r})e_{2^{r+1}}...)e_{2^k})e_{2^i})+\sum_{i=1}^{t-1}(v(\rho_{2^i-1},\rho_{2^i})e_{2^i}),$$

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

It results

$$F_t(\zeta)=v(\phi_1,\phi_2)+$$
$$+\sum_{i=1}^{t-1}(\sum_{k=1}^{i}(\sum_{r=1}^{k-1}v(\rho_{M_{rki}-1},\rho_{M_{rki}})e_{2^r})e_{2^{r+1}}...)e_{2^k})e_{2^i})+\sum_{i=1}^{t-1}(v(\rho_{2^i-1},\rho_{2^i})e_{2^i}),$$

or

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

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 $v(\phi_1,\phi_2)$ and $v(\rho_{2s-1},\rho_{2s})$ 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 $F_t(\zeta)$ 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 $t\geq 1$..*

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]).

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 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

$$\mathcal{S}^3=\{a\in\mathbb{O}(-1,-1,-1):\ \mathbf{n}(a)=1\},$$

$$\mathcal{S}^2 = \{a \in \mathbb{O}(-1,-1,-1) :\ t(a) = 0, \mathbf{n}(a) = 1\}.$$

We remark that for all elements $a \in \mathcal{S}^2$, we have $a^2 = -1$. Let $a \in \mathcal{S}^3, a = a_0 + a_1 f_1 + a_2 f_2 + a_3 f_3 + a_4 f_4 + a_5 f_5 + a_6 f_6 + a_7 f_7$. This element can be written under the form

$$a = \cos\lambda + w \sin\lambda,$$

where $\cos\lambda = a_0$ and

$$w = \frac{a_1 f_1 + a_2 f_2 + a_3 f_3 + a_4 f_4 + a_5 f_5 + a_6 f_6 + a_7 f_7}{\sqrt{a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_5^2 + a_6^2 + a_7^2}} =$$

$$= \frac{a_1 f_1 + a_2 f_2 + a_3 f_3 + a_4 f_4 + a_5 f_5 + a_6 f_6 + a_7 f_7}{\sqrt{1 - a_0^2}}.$$

Proposition 3.5.4. For $w \in \mathcal{S}^2$, we have $(\cos\lambda_1 + w\sin\lambda_1)(\cos\lambda_2 + w\sin\lambda_2) = \cos(\lambda_1 + \lambda_2) + w\sin(\lambda_1 + \lambda_2)$.

Proposition 3.5.5. (De Moivre formula for octonions) *With the above notations, we have that*

$$a^n = (\cos\lambda + w\sin\lambda)^n = \cos n\lambda + w\sin n\lambda,$$

where $a \in \mathcal{S}^3$, $n \in \mathbb{Z}$ *and* $\lambda \in \mathbb{R}$.

Proof. For $n > 0$, by induction.

Since $a^{-1} = \cos\lambda - w\sin\lambda = \cos(-\lambda) + w\sin(-\lambda)$, it results the asked formula for all $n \in \mathbb{Z}$.□

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. □

*

The nth term of Fibonacci 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

$$l_0 = 2; l_1 = 1; l_n = l_{n-1} + l_{n-2},\ n \geq 2$$

is called the Lucas number.

We know that

$$l_m l_p + 5 f_m f_p = 2 l_{m+p}, \forall\ m, p \in \mathbb{N}$$

and

$$f_m f_{m+p} = \frac{1}{5}\left(l_{2m+p} + (-1)^{m+1} \cdot l_p\right), \forall\ m, p \in \mathbb{N}.$$

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:

$$\boldsymbol{n}(F_n) = F_n \overline{F}_n = 3 f_{2n+3},$$

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 $\mathbb{H}$.

Let $F_n = f_n 1 + f_{n+1} e_2 + f_{n+2} e_3 + f_{n+3} e_4 \in \mathbb{H}(\beta_1, \beta_2)$ 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*

$$\boldsymbol{n}(F_n) = h_{2n+2}^{1-2\beta_2, -3\beta_2} + (-\beta_1 - 1) h_{2n+3}^{1-2\beta_2, -\beta_2} - 2(-\beta_1 - 1)(1 - \beta_2) f_n f_{n+1}. \tag{3.6.2.}$$

□

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*

$$\boldsymbol{n}\left(H_n^{p,q}\right) = p^2 h_{2n}^{1-2\beta_2,-3\beta_2} + p^2(-\beta_1\text{-}1)h_{2n+1}^{1-2\beta_2,-\beta_2} + q^2 h_{2n+2}^{1-2\beta_2,-3\beta_2} + q^2(-\beta_1\text{-}1)h_{2n+3}^{1-2\beta_2,-\beta_2} -$$

$$-2p\left(-\beta_1-1\right)\left(-p\beta_2+p+q\right)f_{n-1}f_n - 2q^2(-\beta_1-1)\left(1\text{-}\beta_2\right)f_n f_{n+1} +$$

$$+h_{2n+1}^{-2pq\beta_1,2pq\beta_1\beta_2} + 2pq\beta_1\beta_2(f_{2n}+f_{2n+3}) - 2pq\beta_2\left(1+\beta_1\right)f_{n+1}f_{n+2}. \quad (3.6.3.)$$

□

$E'(\beta_1,\beta_2) = \frac{1}{5}[(p+\alpha q)^2 - \beta_1\left(p\alpha+\alpha^2 q\right)^2 - \beta_2\left(p\alpha^2+\alpha^3 q\right)^2 +$
$+\beta_1\beta_2\left(p\alpha^3+\alpha^4 q\right)^2] =$
$= \frac{1}{5}\left(p+\alpha q\right)^2\left[1-\beta_1\alpha^2-\beta_2\alpha^4+\beta_1\beta_2\alpha^6\right] =$
$= \frac{1}{5}\left(p+\alpha q\right)^2 E(\beta_1,\beta_2).$

Therefore for all $\beta_1,\beta_2 \in \mathbb{R}$ with $E'(\beta_1,\beta_2) \neq 0$ in the algebra $\mathbb{H}\left(\beta_1,\beta_2\right)$ 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 $\mathbb{H}\left(\beta_1,\beta_2\right)$.*□

Remark 3.6.7. Algebra $\mathbb{H}\left(\beta_1,\beta_2\right)$ 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 $\mathbb{H}_{\mathbb{Q}}\left(\alpha,\beta\right)$ 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 $i^2 = \alpha, j^2 = \beta$, $k = ij = -ji$.

Let $\mathbb{Z}$ be a integers ring and $\mathbb{Q}$ their field of the fractions and let $\mathbb{H}_{\mathbb{Q}}(\alpha,\beta)$ be the generalized quaternion algebra. We recall that $\mathcal{O}$ is an order in $\mathbb{H}_{\mathbb{Q}}(\alpha,\beta)$ if $\mathcal{O}\subseteq\mathbb{H}_{\mathbb{Q}}(\alpha,\beta)$ and it is a finitely generated $\mathbb{Z}-$ submodule of $\mathbb{H}_{\mathbb{Q}}(\alpha,\beta)$ which is also a subring of $\mathbb{H}_{\mathbb{Q}}(\alpha,\beta)$ (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.

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.

Further developments of this direction of study: **Computational mathematics methods in the study of algebras obtained by the Cayley-Dickson process**

1. *The characterization of zero divisors in such algebras will be a very useful and an important subject of study.*

Algebras which contain zero divisors are usually avoided by the mathematicians, one of the reason can be that the most studied algebras, with a lot of applications, are division algebras. Therefore, the problem of the determination of the zero divisors in some special classes of algebras (as for example, algebras obtained by the Cayley-Dickson process) can have an increased interest. In [Ca; 04], the author studied the zero divisors for the Sedenion real algebra $\mathbb{S}$, constructed from Octonion division real algebra $\mathbb{O}$ as a subalgebra. Let $B=\{1,f_1,...,f_7,g_8,...,g_{15}\}$ be its basis, with $\{1,f_1,...,f_7\}$ a basis in $\mathbb{O}$. He found that all zeros divisors of the algebra $\mathbb{S}$ can be found in the algebra $\overline{\mathbb{O}}$ generated by $\{g_8,...,g_{15}\}$ and called the *quasi-octonion* algebra. This algebra not commute, not associate, is non-alternative, but is power-associative and has a quadratic form. This method can be extended to all algebras obtained by the Cayley-Dickson, trying to emphasize a maximal subset (structure) in which we can find zero divisors or non-zero divisors.

2. *Using dedicated software for study multilinear identities of degree $\leq n$.*

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 of algebras.

In [Br, He; 01], using computer calculations programed in Maple, Mathematica or Albert software (http://people.cs.clemson.edu/˜dpj/albertstuff/albert.html) the authors studied multilinear identities of degrees ≤ 5 over sedenions and proved that they are satisfied by all flexible quadratic algebras. Moreover, they proved that such an identity of degrees ≤ 5 is true in all algebras obtained by the Cayley-Dickson process if and only if it is true in the sedenion algebra. As a technique, they used matrix representation and converted the problem into a problem of linear algebra dealing with large matrices.

3) *Development of algorithms for computing elements in a basis of algebras obtained by the Cayley-Dickson process.*

In the habilitation thesis, I used two types of algebra multiplication. For $\gamma \in K$, we have :

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

in Chapter 2, for level and sublevel of algebras obtained by the Cayley-Dickson process, in Chapter 3, 3.1 and 3.2 for Hall identity and

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

in the rest of Chapter 3 and in Chapter 4.

From here, the following questions arise:

i) Why two kind of multiplication types for algebras obtained by the Cayley-Dickson process ?

ii) The obtained algebras are isomorphic?

iii) The obtained results are influenced by the chosen multiplication?

The answer at question ii) is YES, at question iii) is NO and at question i) is "**there are 8 such different products**". The answers of these questions was recently well systematized in the paper [Ba; 16], in which he catalogued all possible situations for the Cayley-Dickson doubling products. The author remarked that even if "it is recognized that there are several possible Cayley-Dickson doubling products, past researchers have restricted themselves to only two of them", namely, the two products used in this work, (1.3) and (1.3′) and denoted by Bales with P_3^T, respectively P_3.

For example, we can remark that in [Br; 67] and [Sc; 54] was used the product P_3^T and in [Sc; 66] was used the product P_3. As we can see, the same author, R.D.Schafer, used different products.

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 examples, structures 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].

As we can see from above, the study of some relations, properties and identities in algebras obtained by the Cayley-Dickson process are very useful but sometimes not so easy to prove, involving a lot of computations.

Some applications in Coding Theory

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. Therefore, 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) code. 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 output 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

$$d_{\min} = \min\{d_H(x, y), x \neq y, x, y \in \mathcal{C}\}.$$

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 4.1.4. 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 $k = \dim_{\mathbb{Z}_q} \mathcal{C}$, therefore the information rate of the code is $R = \frac{k}{n}$.

2) Let $\mathcal{C}$ be a code of the type $[n,k]$. A matrix G whose lines represent a basis in $\mathcal{C}$ over $\mathbb{Z}_q$ is called *a generating matrix* for the code $\mathcal{C}$.G has k lines and n columns.

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 $cH^t = 0$. H has has $n-k$ lines and n columns. We remark that $GH^t = 0$ and if G is given under the standard form $[I_k A]$, therefore $H = [-A^t \ I_{n-k}]$

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 $Hx^t = Hy^t$. Based on the received vector $r = c + e$, the receiver estimated of what was the transmitted codeword. Since errors of lower weight are more probable than errors of higher weight, the problem is to estimate an error e such that the weight of e is as small as possible.

Therefore, for decoding using the syndrome, we must follow the below algorithm:

-We compute the syndrome of the received vector r, $s(r)$;

-We search a representative e (with weight as small as possible) such that $s(e) = s(r)$;

-We will decode r by $c = r - e$.

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 $x^n - 1$.

In a simple way, a constellation can be regarded as a finite subset of the complex numbers. When a data will be transmitted, first of all, will be converted into sequences of elements of the chosen constellation ([He; 04]). A *constellation* diagram is a representation of a signal modulated by a digital modulation scheme, as for example QAM(quadrature amplitude modulation signal). The usually choices of signal constellations are:

1. A $n-$PSK(phase-shift keying) constellation, given by all n-roots of unity:

$$\{\rho / \ \rho^i = 1, i \in \{0, ..., n-1\}\};$$

2. A $n-$QAM constellation, usually n a power of two, regarded as n points in the complex plane (as a subset of $\mathbb{Z}[i]$):

$$\{a+bi\,, a, b \in \mathbb{Z},\ |a|\,, |b| < \sqrt{n}\};$$

3. HEX constellations regarded as finite subset of the Eisenstein integers. (see [He; 04].

Therefore the constellation diagram is a useful representation for QAM which is both an analogue and a digital modulation scheme. The data are usually binary and the number of the point in a grid are a power of two. For example the 64-QAM, 256QAM are often used in digital cable television. Usually the constellation points are arranged in a square grid with equal vertical and horizontal spacing.([3])

The design of error correcting codes for two dimensional signal spaces has been studied. Codes over Gaussian integers are suitable for coding over two dimensional signal spaces. Therefore it is important to use two dimensional signal constellations ([3]). Block codes over Gaussian integers were first studied by Huber and such codes can be used for coding over two-dimensional signal spaces, that means using QAM signals. In the most common transmission channels where QAM techniques are used, when an error in the message occurs, the probability that a signal point is received into a neighboring point is much larger than the probability that the signal point to be received into a more distant point. For this reason, the Hamming metric is not appropriate to protect the signal points (especially for a non binary code). Since the Hamming distance revealed to be inappropriate to deal with QAM signal sets and other related constellations, Huber introduced Mannheim distance(which is not a true metric since it does not fulfill the triangular inequality) as a performance measure of codes over Gaussian integers. Using Euclidian distance and Mannheim distance the best code words from the syndrome list can be chosen(soft-input decoding algorithm)([4]). For other details, please see [Be; 68].

The study of Integer Codes can be extended to codes over subsets of real algebras obtained by the Cayley-Dickson process. The results presented below, were obtained, by the author, in the papers [Fl; 16] and [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.

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.

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 $f : \mathbb{Z}_p \to \mathbb{Z}[i]_\pi$,

$$f(\mathbf{u}) = u\ mod\pi = u - \left[\frac{u\overline{\pi}}{\mathbf{n}(\pi)}\right]\pi = \beta, \tag{4.2.2.}$$

with $\mathbf{n}(\beta) < \mathbf{n}(\pi)$.

Remark 4.2.3. From the above, it results that $\mathbb{Z}[i]_\pi$ is isomorphic with $\mathbb{Z}_p$. 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], 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 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.

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]).

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.*

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 $\mathbf{n}(v) < \mathbf{n}(y)$.*

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* π.

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.*

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.*

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.

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:
$\mathbb{V}_\pi = \{0, 1, 2, 3, -3-w, -2-w, -1-w, -w, 1-w, 2-w,$
$3-w, 4-w, -2w-2, 2w-2, \mathbf{-2w}, \mathbf{-2w+1}, -2w+2,$
$2+2w, w-4, w-3, w-2, w-1, w, 1+w, 2+w, 3+w, -3, -2, -1\}$, with labels $\{\mathbf{0}, \mathbf{1}, \mathbf{2}, ..., \mathbf{27}, \mathbf{28}\}$, in this order.

Remark. Although $\mathbb{V}_\pi$ and $\mathbb{Z}_p$ are the same field, we will see in the following that when the field $\mathbb{Z}_p$ is represented as $\mathbb{V}_\pi$ offers significant advantages for coding over some signal constellations. [Hu, 94(1)]

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 $\mathbf{n}(\pi) = Mn + 1 = p$, $M, n \in \mathbb{Z}, n \geq 0$, such that there are β a primitive element (of order $p - 1$) in $\mathbb{V}_\pi$, with the properties $\beta^{\frac{p-1}{M}} = \beta^n = w$ or $\beta^{\frac{p-1}{M}} = \beta^n = -w$. 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 $\mathcal{C}$ 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 $e(x)$ 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*

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & ... & \beta^{n-1} \end{pmatrix}. \tag{4.5.3.}$$

It results that, the code $\mathcal{C}$ is able to correct all errors of the form $e(x) = e_i x^i$, with $0 \leq w_C(e_i) \leq 1$.

Theorem 4.5.12. *We consider $\mathcal{C}$ a code defined by the parity-check matrix*

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & ... & \beta^{n-1} \\ 1 & \beta^{M+1} & \beta^{2(M+1)} & ... & \beta^{(n-1)(M+1)} \end{pmatrix}. \tag{4.5.4.}$$

Then $\mathcal{C}$ can correct error patterns of the form $e(x) = e_i x^i$, with $e_i \in \mathbb{V}_\pi$, $0 \leq i \leq n-1$.

Theorem 4.5.13. *We consider $\mathcal{C}$ a code defined by the parity-check matrix*

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & ... & \beta^{n-1} \\ 1 & \beta^{M+1} & \beta^{2(M+1)} & ... & \beta^{(n-1)(M+1)} \\ 1 & \beta^{2M+1} & \beta^{2(2M+1)} & ... & \beta^{(n-1)(2M+1)} \end{pmatrix}. \tag{4.5.5.}$$

Then $\mathcal{C}$ can find the location and can correct error patterns of the form $e(x) = e_i x^i$, $0 \leq i \leq n-1$, with $e_i \in \mathbb{V}_\pi$.

Theorem 4.5.14. *Let $\mathcal{C}$ be a code defined by the following parity-check matrix*

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & ... & \beta^{n-1} \\ 1 & \beta^{M+1} & \beta^{2(M+1)} & ... & \beta^{(n-1)(M+1)} \\ 1 & \beta^{2M+1} & \beta^{2(2M+1)} & ... & \beta^{(n-1)(2M+1)} \\ 1 & \beta^{3M+1} & \beta^{2(3M+1)} & ... & \beta^{(n-1)(3M+1)} \end{pmatrix}. \tag{4.5.6.}$$

Then $\mathcal{C}$ can correct error patterns of the form $e(x) = e_i x^i + e_j x^j$, $0 \leq i, j \leq n-1$, where $e_i, e_j \in \mathbb{V}_\pi$.

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 more 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.

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, 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.

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.

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
```

Further developments of this direction of study: **Applications of some types of algebras in the Coding theory**

1) *Improvement of the above algorithm.* 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, 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, to study the minimum distance in general or in some special cases, etc. Mathematical software as Maple, GAP-GUAVA can be very usefull.

2) *Applications of division algebras in the study of Space Time Binary Block Codes.*

In the present days, with the Internet, the massive distribution of any kind of information became possible. A 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. Determining when some algebras (as for example algebras with involution) are division algebras is not always an easy problem, but their algebraic properties can be used to improve the design of good codes and justify their intensive study ([Un, Ma; 11], [He; 04]).

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])

3) *The study of the connections between binary block codes and BCK-algebras.*

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. 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 answer is partially "yes" and was found by the author in the papers [Fl; 15(2)] and [B,Fa, Fl, Ku; 15].

A set A with a binary operation " $*$ " and a fixed element denoted with "0" is called an algebra of type $(2,0)$.

We know that in the set theory, the following relations hold:

i) $(A-B)-(A-C)\subset(C-B)$,

ii) $A-(A-B)\subset B$, for A,B,C arbitrary sets.

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 $x*y=\theta$.

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:

$$w_x\preceq w_y \text{ if and only if } y_i\leq x_i, i\in\{1,2,...,n\}. \tag{1.1.}$$

In the paper [Ju, So; 11], the authors constructed binary block-codes associated to a BCK-algebra. At the end of the paper they put the following question: *for each binary block-code V, there is a BCK-algebra which determines V?* The answer of this question is partial affirmative, as we can see in Theorem 2.2 and Theorem 2.9.

Let $(X,\leq)$ be a finite partial ordered set with the minimum element θ . We define the following binary relation " $*$ " on X :

$$\begin{array}{c} \theta*x=\theta \text{ and } x*x=\theta, \forall x\in X; \\ x*y=\theta, \text{ if } \ x\leq y, \quad x,y\in X; \\ x*y=x, \text{ otherwise.} \end{array} \tag{2.1.}$$

Proposition 2.1. *With the above notations, the algebra $(X,*,\theta)$ is a non-commutative and non-implicative BCK-algebra.*

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

(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.

As we can see from above, using some types of algebras, as for examples algebras obtained by the Cayley-Dickson process or BCK-algebras, we studied their implications in the construction of some codes.

Therefore, another study direction can be **Applications of some types of algebras in the Coding theory.**

Career development

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 in 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) PN-II-RU-PRECISI-2015-9-9240, Cristina Flaut, Codes over a subset of Octonion Integers, Results Math., **Red zone**.

5) PN-II-RU-PRECISI-2015-9-9219, Cristina Flaut, BCK-algebras arising from block codes, J. Intell. Fuzzy Syst., **Yellow zone.**

6) PN-II-RU-PRECISI-2015-9-9303, Cristina Flaut, Diana Savin, Some examples of division symbol algebras of degree 3 and 5, Carpathian J. Math, 31(2)(2015), **Yellow zone.**

7) PN-II-RU-PRECISI-2015-9-10420 A. Borumand Saeid, H. Fatemidokht, C. Flaut and M. Kuchaki Rafsanjani, On Codes based on BCK-algebras, J. Intell. Fuzzy Syst, **Yellow zone**.

8) UNESCO-UNITWIN OCW/OER Initiative, Handong Global University, South Korea, 1 April 2012- 10 November 2012, April 2013-December 2013, January 2014-July 2014.

9) UNESCO-UNITWIN OCW/OER Initiative, Handong Global University, South Korea, 1 October 2011-20 January 2012.

10) UNESCO-UNITWIN OCW/OER Initiative, Handong Global University, South Korea, 1 September 2013- 31 March 2014.

11) UNESCO-UNITWIN OCW/OER Initiative, Handong Global University, South Korea, 1 April 2012- 10 November 2012.

12) UNESCO-UNITWIN OCW/OER Initiative, Handong Global University, South Korea, 1 October 2011-20 January 2012.

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: 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. I was invited referee to several journals.

Supplementary References

[Ba;16] Bales, J. W., *The Eight Cayley–Dickson Doubling Products*, accepted in Adv. Appl. Clifford Algebras, 11 January **2016**, DOI 10.1007/s00006-015-0638-6.

[Be; 68] Berlekamp, E.R., *Algebraic Coding Theory*, McGraw-Hill, 1968.

[Br, He; 01] Bremner, M., Hentzel, I., *Identities for algebras obtained by the Cayley-Dickson process*, Commun. Algebra, **29(8)(2001)**, 3523-3534.

[Ca; 04] Cawagas, R.,E., *On the Structure and Zero Divisors of the Cayley-Dickson Sedenion Algebra*, Discussiones Mathematicae: General Algebra and Applications **24(2004),** 251-265.

[He; 04] Hendrickson, A.,O.,F., *Space-Time Block Codes from Cyclic Division Algebras: An Introduction*, http://www.math.wisc.edu/˜boston/hendrickson.pdf

[Hu, 94(1)] Huber K., *Codes over Eisenstein-Jacobi integers*, Contemporary Mathematics, **168(1994)**, 165-179.

[1] https://learn.sparkfun.com/tutorials/analog-vs-digital
[2] https://en.wikipedia.org/wiki/Constellation_diagram
[3]https://books.google.ro/books?id=m0K7CgAAQBAJ&pg
=PA44&lpg=PA44&dq=mannheim+distance+and+qam+
signal&source=bl&ots=KFGyhYio1x&sig=V2bzredNqU
Sq1bM7KjLYMoAToQ8&hl=en&sa=X&ved=0ah
UKEwjLnbfAurnLAhXps3IKHYadDEwQ6AEIIjAC#v
=onepage&q=mannheim%20distance%20and%20qam%20signal&f=false
[4] https://books.google.ro/books?id=JJQZHiIjUwIC
&pg=PA109&lpg=PA109&dq=mannheim+distance+
and+qam+signal&source=bl&ots=DJtamU4oyQ&sig
=wmwsKmgtwWChDgNArz94cR5Xyxk&hl=en&sa=
X&ved=0ahUKEwiXgKWIubnLAhUl7XIKHXzZDU
MQ6AEIHjAB#v=onepage&q=mannheim%20
distance%20and%20qam%20signal&f=false
[5] http://www.google.com/patents/DE102004048312A1?cl=en