

# Hypercomputation on $\{0, 1\}$

F. Chaitin–Chatelin<sup>1</sup>, A. N. Zaoui<sup>2</sup>

CERFACS<sup>3</sup> Technical Report No. TR/PA/02/73

## Abstract

This work looks further into the structure of the hypercomplex binary algebras  $B_k$ ,  $k \geq 0$ , introduced in [2, 3] and developed in [4]. The two main results are:

- i) the emergence of computation mod 2, 4, 8 and 16 on  $\mathbb{Z}$  for  $k = 0$  to 3. The link, exact for  $k = 0$  and 1, becomes inexact for  $k = 2$  and fuzzy for  $k = 3$ .
- ii) the analysis of the resolution of  $a \times x = b$  in  $B_k$ , for  $k \geq 0$ , for  $a$  such that  $a^2 = 1$  and  $a^2 = 0$ .  $B_0$  and  $B_1$  play a special role as the 2 necessary steps to define the general recursion for  $k \geq 2$  which starts at  $B_2$ .

**Keywords:** binary algebra, zero-divisor, hypercomplex multiplication, binary quaternions and octonions, geometric order, complex logic of dimension 2, 4 and 8, computation mod 2, 4, 8 and 16.

## 1 Introduction

The source of this work is the computing power of Geometry as it was first presented in [6]. It elaborates on the geometric ordering which is necessary to understand the meaning of the multiplication of binary sequences of dimension  $2^k$  in the algebras  $B_k$  for  $k > 0$ , on  $B_0 = \mathbb{Z}_2 = \{0, 1\}$ . The existence of such an order was first stated [1, 2, 3] for the complex binary algebra  $B_1 \sim B_0 \times B_0$  which becomes isomorphic to  $\mathbb{Z}_4$  with this ordering.

The idea was further developed in [4]. The multiplication tables of the algebras  $B_1$  and  $B_2$ , equipped with the geometric ordering, were used, from a computational point of view, for the analysis of hypercomplex division in

---

<sup>1</sup>Université Toulouse I and CERFACS. E-mail: [chatelin@cerfacs.fr](mailto:chatelin@cerfacs.fr)

<sup>2</sup>CERFACS. E-mail: [zaoui@cerfacs.fr](mailto:zaoui@cerfacs.fr)

<sup>3</sup>CERFACS, 42 av. G. Coriolis, 31057 Toulouse cedex, France

the presence of zero-divisors, when the computation is realized on  $\mathbb{Z}_2$ .

In the work to follow, we first take another look at  $B_1$  and  $B_2$ , as well as at the first 32 elements of  $B_3$ , the complex algebra of dimension  $8 = 2^3$  and cardinality  $256 = 2^{2^3}$ . This time, we present an analysis of the *flow of information from bottom up* which takes place in these lgebras as a result of hypermultiplication to allow the emergence of computation on  $\mathbb{Z} \bmod 2, 4, 8$  and 16. This flow of information is highly structured, since it reflects the recursive definition for  $k \geq 1$  of  $B_k$  from  $B_{k-1}, B_0 = \mathbb{Z}_2$ , by the Dickson process [2]. Second, we revisit the equation  $a \times x = b$  in an arbitrary binary algebra  $B_k$  of dimension  $2^k, k \geq 1$ .

The terms hypercomputation, hypermultiplication (or hyperproduct) were introduced in [4] as substitutes for the mathematically well defined expressions hypercomplex computation, and hypercomplex multiplication (or product) respectively. They are used throughout the text to refer to these precise mathematical notions.

## 2 A partial geometric order for $B_3$

### 2.1 The $32 \times 32$ multiplication table

The first 32 elements of  $B_3$  are ordered as follows: to each sequence of eight bits is associated a decimal integer which represents its place in the ordered set of 32 such sequences.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	1
0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	1
0	0	0	1	1	1	1	1	1	1	1	0	0	0	1	1
0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0
0	0	0	0	0	1	1	1	1	1	1	1	1	0	1	0
0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0
0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1

	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1	0
0	1	0	1	0	0	1	0	0	0	1	0	0	1	0	1	1
1	0	0	0	1	0	0	0	0	1	1	0	0	0	0	1	1
0	1	1	0	0	0	0	0	1	0	0	1	1	1	1	0	1
1	0	1	0	1	0	1	0	0	0	0	1	0	0	1	1	0
1	1	0	0	0	0	1	1	1	0	0	0	0	1	0	1	1
1	0	0	0	1	0	1	1	0	0	0	0	0	1	1	1	1
1	1	1	1	0	1	0	0	0	1	0	0	1	1	0	0	0

Table 2.1. Partial order in  $B_3$ .

We use this ordering/labeling to display the multiplication table  $T(32)$  of these 32 elements [5].

Due to space constraints, we display this table as four blocks of size  $16 \times 16$  each denoted  $T_i, i = 1, \dots, 4$ , such that:

$$T(32) = \frac{T_1 \mid T_2}{T_3 \mid T_4}$$

The commutativity of multiplication in  $B_3$  implies that  $T_3 = T_2^T$ .

$\times$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>	<u>0</u>
1	<u>0</u>	<u>1</u>	<u>2</u>	<u>3</u>	<u>4</u>	<u>5</u>	<u>6</u>	<u>7</u>	<u>8</u>	<u>9</u>	<u>10</u>	<u>11</u>	<u>12</u>	<u>13</u>	<u>14</u>	<u>15</u>
2	<u>0</u>	<u>2</u>	■	0	■	0	■	<u>0</u>	<u>2</u>	0	■	0	■	■	■	■
3	<u>0</u>	<u>3</u>	■	1	4	7	■	<u>5</u>	<u>8</u>	<u>11</u>	■	9	12	■	■	■
4	<u>0</u>	<u>4</u>	0	4	<u>0</u>	12	0	<u>12</u>	<u>0</u>	<u>4</u>	0	4	<u>0</u>	12	<u>8</u>	8
5	<u>0</u>	<u>5</u>	■	7	12	1	■	<u>3</u>	<u>8</u>	<u>13</u>	■	■	4	9	■	15
6	<u>0</u>	<u>6</u>	0	■	0	■	0	<u>10</u>	<u>0</u>	<u>6</u>	0	■	0	■	■	■
7	<u>0</u>	<u>7</u>	■	<u>5</u>	<u>12</u>	<u>3</u>	<u>10</u>	<u>1</u>	<u>8</u>	■	<u>6</u>	<u>13</u>	<u>4</u>	<u>11</u>	■	■
8	<u>0</u>	<u>8</u>	<u>0</u>	<u>8</u>	<u>0</u>	<u>8</u>	<u>0</u>	<u>8</u>	<u>0</u>	<u>8</u>	<u>0</u>	<u>8</u>	<u>0</u>	<u>8</u>	<u>0</u>	0
9	<u>0</u>	<u>9</u>	<u>2</u>	<u>11</u>	<u>4</u>	<u>13</u>	<u>6</u>	■	<u>8</u>	<u>1</u>	<u>10</u>	<u>3</u>	<u>12</u>	<u>5</u>	<u>14</u>	15
10	<u>0</u>	<u>10</u>	0	■	0	■	0	<u>6</u>	<u>0</u>	<u>10</u>	0	■	0	■	■	■
11	<u>0</u>	<u>11</u>	■	9	4	■	■	<u>13</u>	<u>8</u>	<u>3</u>	■	1	12	7	■	■
12	<u>0</u>	<u>12</u>	0	12	<u>0</u>	4	0	<u>4</u>	<u>0</u>	<u>12</u>	0	12	<u>0</u>	4	<u>8</u>	8
13	<u>0</u>	<u>13</u>	■	■	12	9	■	<u>11</u>	<u>8</u>	<u>5</u>	■	7	4	1	■	15
14	<u>0</u>	<u>14</u>	■	■	<u>8</u>	■	■	■	<u>0</u>	<u>14</u>	■	■	<u>8</u>	■	0	■
15	<u>0</u>	<u>15</u>	■	■	8	15	■	■	0	15	■	■	8	15	■	0

Table 2.2. Table  $T_1$ .

$\times$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	0	16	■	■	4	■	■	■	8	■	■	12	■	■	■	■
17	0	17	8	20	0	17	8	20	0	17	8	20	0	17	8	0
18	0	18	8	18	0	18	8	18	0	18	8	18	0	18	0	0
19	0	19	■	28	8	■	■	■	0	19	■	28	8	■	■	17
20	0	20	8	17	0	20	8	17	0	20	8	17	0	20	8	0
21	0	21	12	■	0	■	4	■	0	21	12	■	0	■	■	20
22	0	22	■	■	12	■	10	■	8	■	6	■	4	■	■	■
23	0	23	10	31	4	■	■	■	8	■	2	■	12	■	■	■
24	0	24	■	■	12	■	■	■	8	■	■	■	4	■	■	■
25	0	25	4	25	0	■	12	■	0	25	4	25	0	■	18	■
26	0	26	4	26	0	■	12	■	0	26	4	26	0	■	■	18
27	0	27	10	■	4	■	■	■	8	■	2	■	12	■	14	15
28	0	28	■	19	8	■	■	■	0	28	■	19	8	■	■	20
29	0	29	10	■	4	■	■	■	8	■	2	■	12	■	■	■
30	0	30	■	■	8	■	■	■	0	30	■	■	8	■	18	8
31	0	31	■	23	4	■	■	■	8	■	■	■	12	■	■	■

Table 2.3. Table  $T_2 = T_3^T$ .

$\times$	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
16	1	17	■	■	20	21	■	■	■	26	25	■	■	■	■	■
17	17	0	0	0	0	0	17	17	20	8	8	17	0	20	0	20
18	■	0	0	8	0	8	■	18	■	0	0	18	8	■	0	18
19	■	0	8	0	0	20	■	19	28	■	■	■	0	■	20	28
20	20	0	0	0	0	0	20	20	17	8	8	20	0	17	0	17
21	21	0	8	20	0	0	■	■	■	12	12	■	17	■	20	■
22	■	17	■	■	20	■	1	■	■	■	■	■	■	■	■	■
23	■	17	18	19	20	■	■	1	■	25	26	■	28	■	■	3
24	■	20	■	28	17	■	■	■	1	■	■	■	19	■	■	■
25	26	8	0	■	8	12	■	25	■	0	0	25	■	■	■	25
26	25	8	0	■	8	12	■	26	■	0	0	26	■	■	18	26
27	■	17	18	■	20	■	■	■	■	25	26	1	■	■	30	■
28	■	0	8	0	0	17	■	28	19	■	■	■	0	■	17	19
29	■	20	■	■	17	■	■	■	■	■	■	■	■	1	■	■
30	■	0	0	20	0	20	■	■	■	■	18	30	17	■	0	■
31	■	20	18	28	17	■	■	3	■	25	26	■	19	■	■	1

Table 2.4. Table  $T_4$ .

The elements marked as ■ are binary octonions which appear in the geometric order with an ordinal  $> 32$ . Therefore they cannot be converted

into a decimal number. They are not recognized by the partial order. The meaning of the underlining in  $T_1$  will be given in Section 4, §4.2.

## 2.2 Structure of $T(32)$

The table  $T(32)$  represents the  $(1, 1)$  block of the full multiplication table of  $B_3$ , with a partition of the full set of elements  $\{0, 1, \dots, 255\}$  into eight equal subsets of 32 elements.

The structure of  $T(32)$  is less apparent than this was the case for the multiplication tables of  $B_k, k = 0, 1, 2$  [4]. The structure will emerge more clearly, if we look at the features it does not retain, which were present in the previous algebras. By doing so, we relate to the recursive definition of the algebras.

We therefore proceed to study, from the point of view of the flow of emergent information, the 3 algebras  $B_0, B_1, B_2$  which are the algebras of binary numbers, binary complex numbers and binary quaternions. We do this by an analysis of the matrix representation  $M(u)$  of the linear map  $z \rightarrow u \times z$  in  $B_k$  [3, 4].

## 3 Information flow in $B_k, k = 0, 1, 2$

### 3.1 The binary logic $B_0 = \mathbb{Z}_2$ of dimension 1

The set of two distinct numbers  $B_0 = \{0, 1\}, 0 \neq 1$ , is the only binary division algebra in the family  $B_k$ . It is a commutative field. As a multiplicative group of order 2, it admits one proper subgroup:  $\{1\}$  of order 1, which is equal to  $B_0^*$ , the group of units of  $B_0$ :  $B_0$  has no other unit than its unity 1.  $M(u)$  is generated by the unique number 1, for  $u \in \mathbb{Z}_2$ . There is only one possible ordering in  $B_0 : 0 < 1$ .

### 3.2 The complex logic $B_1$ of dimension 2

We look at  $M(u) = u_0I + u_1L$ , for  $u = (u_0, u_1) \in B_1$  where

$$I = I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } L = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

It is easily checked that  $u \times z = (u_0, u_1) \times (a, b)$  is equal to

$$M(u) \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} u_0a + u_1b \\ u_0b + u_1a \end{pmatrix}.$$

$I$  and  $L$  are *two* regular matrices with respective eigenvalues  $(1, 1)$  and  $(1, -1)$ . Their multiplication table is

$$\begin{array}{c|cc} \times & I & L \\ \hline I & I & L \\ L & L & I \end{array} \quad (1)$$

Therefore, they form a multiplicative group of order 2, with a proper subgroup  $\{I\}$  of order 1. This subgroup differs from  $B_1^* = \{1, 3\}$ , the group of units of  $B_1$ .

As we saw [4], there is not a unique way to define an order on  $B_1$ . The geometric order that we chose ensures that  $B_1$  is isomorphic to  $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ , the ring of integers modulo 4.

### 3.3 The quaternionic logic $B_2$ of dimension 4

The analysis of the structure of the matrix  $M(u)$  for  $A_2 = \mathbb{H}$ , the algebra of *real* quaternions, was done in [3]. On  $\mathbb{Z}_2$ , the structure is even simpler. It involves the four matrices:

$$H_0 = I_4 = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix}, H_1 = \begin{pmatrix} L & 0 \\ 0 & L \end{pmatrix}, H_2 = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}, H_3 = \begin{pmatrix} 0 & L \\ L & 0 \end{pmatrix}$$

which are such that

$$M(u) = u_0I + u_1H_1 + u_2H_2 + u_3H_3 \quad (2)$$

for  $u = (u_0, u_1, u_2, u_3) \in \mathbb{Z}^4$ .

The *four* matrices  $H_i, i = 0$  to  $3$ , of order 4, are obtained from  $I$  and  $L$ , of order 2, by the Kronecker multiplication  $\otimes$ :

$$H_0 = I \otimes I, H_1 = I \otimes L, H_2 = L \otimes I, H_3 = L \otimes L.$$

The corresponding multiplication table is:

$$\begin{array}{c|cccc} \times & I & H_1 & H_2 & H_3 \\ \hline I & I & H_1 & H_2 & H_3 \\ H_1 & H_1 & I & H_3 & H_2 \\ H_2 & H_2 & H_3 & I & H_1 \\ H_3 & H_3 & H_2 & H_1 & I \end{array} \quad (3)$$

This table allows to check the property  $M(u)M(v) = M(u \times v)$ . The matrices  $\{H_i\}_{i=0}^3$  form a commutative group of order 4 with four proper subgroups:  $\{I\}$  of order 1, and the 3 groups  $\{I, H_i\}$  of order 2,  $i = 1, 2, 3$ . The group of order 4 is isomorphic to a subgroup of the group of permutations  $S_4$ , of order  $4! = 24$  (Cayley).

### 3.4 Componentwise versus global analysis

The structure of the matrix  $M(u)$  shows how the multiplication by  $u$  is realized with the components  $u_i$ . This structure is strongly recursive, as will be seen in Section 4. This detailed analysis of hypermultiplication in  $B_k$  can be called *componentwise*.

It should be contrasted with the *global* analysis performed by means of the order put on the elements of  $B_k$ . In such an approach, each element is identified with a global label which represents its ordinal place in the chosen order. Apart from  $B_0$ , several orders can be considered on  $B_k$ . Amongst them, the geometric order enables to relate, fully (for  $k = 0$  and 1) or partially (for  $k \geq 2$ ), the multiplication table to that of multiplication modulo 2, 4, 8 for  $k = 0, 1, 2$  respectively.

We look more closely at the case  $B_2$ . The geometric order presented in [4] is such that

- i) the first eight elements favour regularity and order,
- ii) the remaining last eight elements favour creativity by mixing 0 and 1.

The resulting multiplication table (Table 4.1 presented in [4]) displays globally a remarkable pattern. In addition, the upper left corner of size  $8 \times 8$  reproduces almost the multiplication table modulo 8. Only the two diagonal elements  $2^2 = (2, 2)$  and  $6^2 = (6, 6)$  as well as  $(2, 6)$  and  $(6, 2)$  differ: their nonzero value 4 (modulo 8) is set to 0 in  $B_2$ . This can be interpreted as an influence of mod 4 on mod 8 for the 4 elements  $(2, 2)$ ,  $(6, 6)$ ,  $(6, 2)$  and  $(2, 6)$ .

How much of the hypermultiplication table  $\mathcal{H}_k$  of  $B_k$ ,  $k = 0, 1, 2, 3$  reproduces the multiplication table  $\mathcal{M}_k$  modulo  $m = 2^{k+1}$ ? And if the match is not complete, how can we quantify the difference? This yields Table 3.1 below:

$k$	Size $N_k = 2^{2^k}$	Area $N_k^2 = N_{k+1}$	Computation mod $2^{k+1}$	Error rate
0	2	$4 = 2^2$	2	0
1	4	$16 = 2^4$	4	0
2	16	$256 = 2^8$	8	$2^{-4} \sim 0.06$
3	256	$65536 = 2^{16}$	16	$\frac{125}{256} \sim \frac{1}{2}$

**Table 3.1.** Emergence of computation mod  $2^{k+1}$ .

We remark that  $2^{k+1} = \log_2 N_{k+1} = 2 \log_2 N_k$ . For  $k = 0$  and 1,  $B_0$  and  $B_1$  are the multiplication tables mod 2 and 4 for

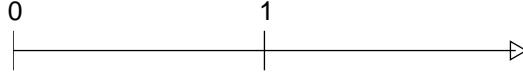


Figure 1: *Unique order in  $B_0$ .*

$\{0, 1\}^1$  and  $\{0, 1\}^2$  on the totality of the  $N_0^2$  and  $N_1^2$  elements respectively. For  $k = 2$ , the match is almost exact on one fourth of the table, that is for  $\frac{N_2^2}{4} = N_2 \times 4$  elements. The error rate is  $\frac{4 \times 4}{N_2^2} = \frac{1}{N_2}$  on the upper left block of order  $8 : \frac{1}{16} < 1\%$ .

For  $k = 3$ , the match is possible on the upper left block  $T_1$  of order 16. In this block  $T_1$ , the error rate is given by Table 2.2 which displays  $T_1$  where the matching values are underlined. There are 131 matching values and 125 non matching. The agreement rate is 0.512 and the error rate is 0.488, close to  $\frac{1}{2}$ . Note that  $131 = 128 + 3$ ,  $125 = 128 - 3$  and  $128 = \frac{N_3}{2}$ . We shall come back to the case  $k = 3$  in paragraph 4.2.

Another instructive information is given by the correspondence between the binary and reverse binary and the geometric orders, provided below for  $k = 0, 1, 2$ . By reverse binary (denoted r-binary) we mean binary expansion written from left to right (the leftmost place has exponent 0): 011 means  $0 + 2^1 + 2^2 = 6$ .

i)  $k = 0$ : the two orders are identical in  $B_0$  (See Figure 1).

ii)  $k = 1$ : (See Figure 2).

The right plot b) corresponds to the other possible ordering in  $B_1$ , for which  $(00) = 0$  and  $(10) = 1$ . It sets  $(01) = 2$  and  $(11) = 3$ . The left plot indicates binary and r-binary versus geometric.

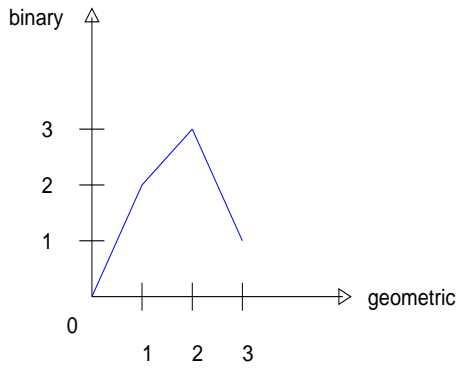
iii)  $k = 2$ : (See Figure 3).

The plot given in Figure 3 represents graphically the correspondence:

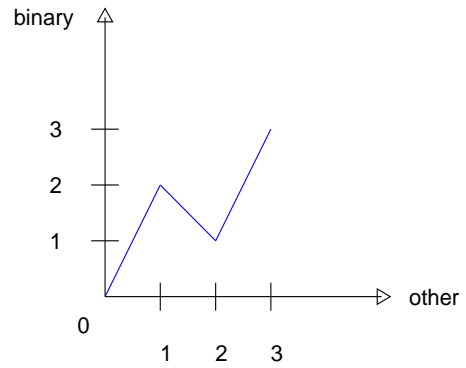
<i>geometric</i>	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
<i>binary</i>	0	8	12	14	15	7	3	1	11	5	9	2	13	6	10	4
<i>r - binary</i>	0	1	3	7	15	14	12	8	13	10	9	4	11	6	5	2

The difference between the role of first eight elements (order) and the last eight ones (mixing) appears clearly. By comparison, the case  $k = 1$  for  $B_1$  gives order (plot a)) and mixing (plot b)).

The reverse-binary is obviously closer to the geometric ordering than binary.



a)



b)

Figure 2: *The two possible orders in  $B_1$  versus binary (and  $r$ -binary).*

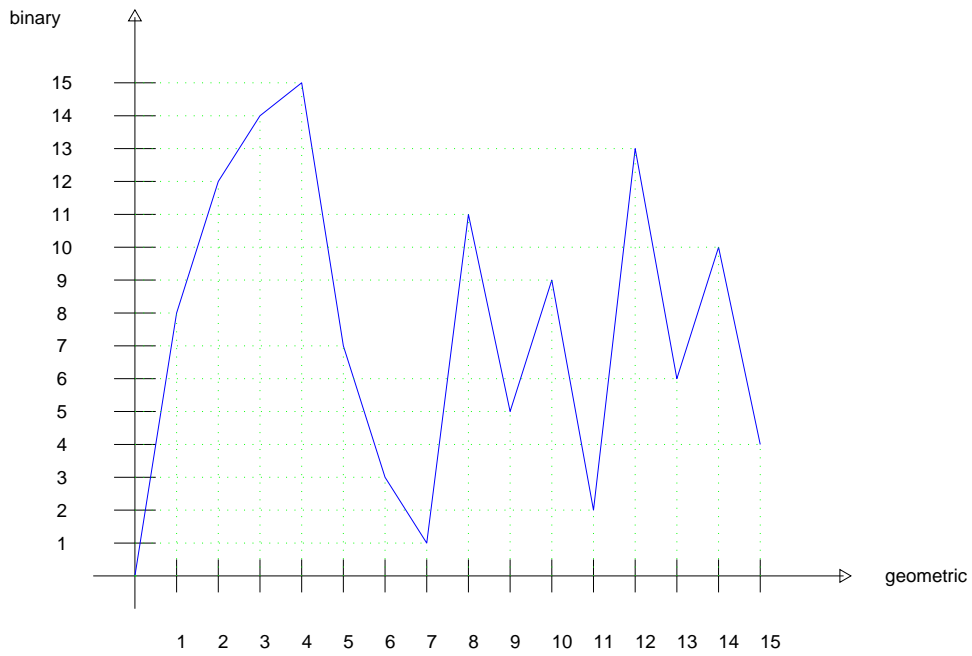


Figure 3: *Binary versus geometric order in  $B_2$ .*

## 4 Information flow in $B_3$

### 4.1 Componentwise analysis

The structure will emerge by induction from the matrix representation  $M(u)$  of the hypercomplex multiplication in  $B_k, k \geq 0$ . We present it first for binary octonions in  $B_3$ .

- a) To represent  $M(u)$  as a linear combination of eight matrices  $G_i, i = 0, 1, \dots, 7$ , we set:

$$\begin{aligned} G_i &= I \otimes H_i \text{ for } i = 0, 1, 2, 3 \text{ and} \\ G_i &= L \otimes H_i \text{ for } i = 4, 5, 6, 7. \end{aligned}$$

We remark that  $G_0 = I \otimes H_0 = I_8 = I$ .

It is easily checked that

$$M(u) = \sum_{i=0}^7 u_i G_i, \text{ for } u = (u_i)_{0 \leq i \leq 7} \in \mathbb{Z}^8. \quad (4)$$

and

$$M(u) = \begin{pmatrix} u_0 & u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & u_7 \\ u_1 & u_0 & u_3 & u_2 & u_5 & u_4 & u_7 & u_6 \\ \hline u_2 & u_3 & u_0 & u_1 & u_6 & u_7 & u_4 & u_5 \\ u_3 & u_2 & u_1 & u_0 & u_7 & u_6 & u_5 & u_4 \\ \hline u_4 & u_5 & u_6 & u_7 & u_0 & u_1 & u_2 & u_3 \\ u_5 & u_4 & u_7 & u_6 & u_1 & u_0 & u_3 & u_2 \\ \hline u_6 & u_7 & u_4 & u_5 & u_2 & u_3 & u_0 & u_1 \\ u_7 & u_6 & u_5 & u_4 & u_3 & u_2 & u_1 & u_0 \end{pmatrix}$$

The multiplication table for  $\{G_i\}_0^7$  is given by Table 4.1.

$\times$	$G_0$	$G_1$	$G_2$	$G_3$	$G_4$	$G_5$	$G_6$	$G_7$
$G_0$	$I$	$G_1$	$G_2$	$G_3$	$G_4$	$G_5$	$G_6$	$G_7$
$G_1$	$G_1$	$I$	$G_3$	$G_2$	$G_5$	$G_4$	$G_7$	$G_6$
$G_2$	$G_2$	$G_3$	$I$	$G_1$	$G_6$	$G_7$	$G_4$	$G_5$
$G_3$	$G_3$	$G_2$	$G_1$	$I$	$G_7$	$G_6$	$G_5$	$G_4$
$G_4$	$G_4$	$G_5$	$G_6$	$G_7$	$I$	$G_1$	$G_2$	$G_3$
$G_5$	$G_5$	$G_4$	$G_7$	$G_6$	$G_1$	$I$	$G_3$	$G_2$
$G_6$	$G_6$	$G_7$	$G_4$	$G_5$	$G_2$	$G_3$	$I$	$G_1$
$G_7$	$G_7$	$G_6$	$G_5$	$G_4$	$G_3$	$G_2$	$G_1$	$I$

**Table 4.1.** *Multiplication table for  $G_i$ .*

The matrices  $\{G_i\}_0^7$  form a commutative group of order 8 with nine proper subgroups:  $\{I\}$  of order 1,  $\{I, G_i\}, i = 1, 2, \dots, 7$  of order 2, and  $\{I, G_1, G_2, G_3\}$  of order 4.

- b) For an arbitrary  $k$ , the matrix  $M(u)$  can be represented in a basis of  $2^k$  matrices  $M_i^{(k)}, i = 0, \dots, 2^k - 1$ . These matrices are defined from the basis  $\{M_i^{(k-1)}\}$  at level  $k - 1$  by  $M_i^{(k)} = I \otimes M_i^{(k-1)}$  for  $i = 0, \dots, 2^{k-1} - 1$  and  $M_i^{(k)} = L \otimes M_i^{(k-1)}$  for  $i = 2^{k-1} + 0, 1, \dots, 2^k - 1$ .

It is easy to show by induction that

$$(I \otimes M_i)(L \otimes M_j) = (L \otimes M_j)(I \otimes M_i) = L \otimes M_i M_j, \quad \text{if } M_i M_j = M_j M_i$$

$$(L \otimes M_i)(L \otimes M_j) = I \otimes M_i M_j = (I \otimes M_i)(I \otimes M_j)$$

From the hypothesis of commutativity  $M_i M_j = M_j M_i$  at level  $k - 1$  follows the commutativity at level  $k$ .

## 4.2 Global analysis and emergence of meaning on $\mathbb{Z}$

We look at the fourth line in Table 3.1, corresponding to  $k = 3$ :

$k$	Size $N_k$	Area $N_k^2$	$\text{mod } 2^{k+1}$	Error rate
3	256	65536	16	$\frac{125}{256} \sim \frac{1}{2}$

The trend which began to manifest itself for  $k = 0, 1$  and  $2$  is now, for  $k = 3$ , clearly visible:

**Computation on  $\mathbb{Z} \text{ mod } 2^{k+1}$  can emerge on the upper left block of order  $2^{k+1}$  for  $k = 0$  up to 3.**

For  $k = 0$  and  $1$ , the values  $2^{2^k}$  and  $2^{k+1}$  can be matched exactly. For  $k = 2$ ,  $N_2 = 16$  and  $2^3 = 8$  can be matched on one fourth of the array of length  $N_2, \frac{N_2}{2} = 8$ . This is realised with an error rate of  $\frac{1}{8 \times 2} = 0.0625 = 2^{-4}$ . For  $k = 3$ ,  $N_3 = 256$  and  $2^4 = 16$  can be matched by means of a block of order  $\frac{N_3}{8} = 32$  for labeling. This is why we have proposed the geometric order on the 32 first elements of  $B_3$  presented in Section 2. Of this block of order 32, only one fourth (the array  $T_1$ ) is susceptible of matching with the

multiplication table mod 16. Although the structure of the multiplication table is clearly visible, the error rate has deteriorated from  $2^{-4}$  to almost  $2^{-1}$ , which means it has been amplified by a factor  $8 = 2^3 : 2^{-4} \times 2^3 = 2^{-1}$ .

A new phenomenon, which takes place for  $k \geq 3$ , is the appearance in  $T_1$  of a significant number of elements whose ordinal is  $> 31$ . Elements which are far in the geometrically ordered sequence of elements of  $B_3$  are obtained as the hyperproduct of leading elements: see, for example,  $2 \times 3 = 00110000 (= 48$  in binary), and  $2 \times 7 = 00000011 (= 3$  in binary). This did not happen for  $B_k, k = 0, 1, 2$ .

On the other hand, the following remarkable property is true for  $B_1, B_2$  and the part  $32 \times 32$  of  $B_3$  that we have examined: the central line and column  $2^k, k = 1, 2, 3$  consist only of terms equal to 0 or  $2^k$ , the zero/nonzero distribution matches that of the diagonal. This is all the more remarkable that this distribution is not uniform.

The correspondence between the geometric and binary orders for the first 32 elements in  $B_3$  is as follows (the r-binary order is given for the first eleven terms):

<i>geometric</i>	0	1	2	3	4	5	6	7	8	9	10
<i>binary</i>	0	128	192	224	240	248	252	254	255	127	63
<i>r - binary</i>	0	1	3	7	15	31	63	127	255	254	252
	11	12	13	14	15	16	17	18	19	20	21
	31	15	7	43	225	47	85	153	65	170	5
	22	23	24	25	26	27	28	29	30	31	
	206	22	161	96	144	25	215	26	238	118	

It is displayed on Figure 4, with different scales on the two axes: 0 to 31 on the horizontal axis, and 0 to 255 on the vertical axis. The order on  $\mathbb{N}$  which emerges as  $k$  increases can be described as follows: for  $k = 0$ , the binary and reverse binary give the same order:  $0 < 1$ . For  $k \geq 1$ , the *reverse binary* make the  $2^k$  odd integers, of the form  $2^p - 1, p = 1, 2, 3$

to  $2^k$ , emerge, after 0, at places 1 to  $2^k$ :

$p$	1	2	3	4	5	6	7	8
$k = 1$	1	3						
$k = 2$	1	3	7	15				
$k = 3$	1	3	7	15	31	63	127	255

For  $k = 4$ , with the same geometric ordering for, at least, the  $2^4 + 1 = 17$  leading elements we would get, after 0, the 16 Mersenne numbers  $M_p = 2^{p-1}$  for  $p = 1$  to  $16 = 2^4$ , ordered by r-binary.

The direct and reverse binary orders agree for the last Mersenne value ( $p = 2^k$ ), which is equal to  $N_k - 1 = 2^{2^k} - 1 = M_{2^k}$  and is assigned to  $\mathbf{e}_k$ . It is the largest possible integer value which can be assigned to any element of  $B_k$ .

These last Mersenne numbers  $M_{2^k} = N_k - 1$  are respectively, for  $k = 0$  to 4, equal to 1, 3, 15, 255 and 65535. They are associated with the 5 smallest Fermat numbers  $F_k = N_k + 1$ ,  $k = 0, \dots, 4$ , which are known to be *prime*. These numbers appear quite naturally in the arithmetic triangle mod 2, known as the Sierpinski triangle. In the full sequence of 16 Mersenne numbers ordered by the algebra  $B_4$ , five of them are prime besides 1 : 3, 7, 31, 127 and 8191, corresponding to  $p = 2, 3, 5, 7$  and 13.

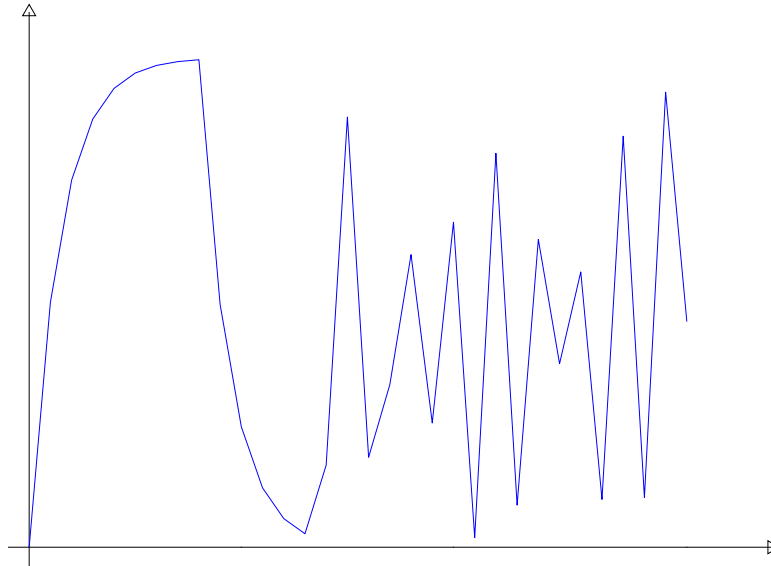


Figure 4: *Binary versus geometric order in  $B_3$ .*

## 5 The role of computation mod $2^k$ , $k = 1$ to 4

### 5.1 Computation in $\mathbb{Z}_{2^k}$ , $k = 1$ to 4

The four binary algebras  $B_0$  to  $B_3$  are the necessary structures required for computation to take place and evolve dynamically. They define the binary skeleton. The flesh of meaning will be produced by hypercomputation with  $\mathbb{R}$  as the basis field, as we recall in the next paragraph.

In order to have the computation in  $\mathbb{Z}_{2^k}$  emerge, one has to choose for  $k \geq 1$  an appropriate geometric ordering which transforms binary sequences into integers, running from 0 to  $2^k - 1$ . There is no free choice for  $k = 0$ , and for  $k = 1$ , there are only 2 possible orderings. But for  $k = 2$  and 3, the choice is enormous (respectively  $16! \sim 2 \times 10^{13}$  and  $256! \sim \sqrt{512\pi} \left(\frac{256}{e}\right)^{256}$  possibilities).

### 5.2 Emergence of meaning through multiplication on $\mathbb{R}$

It has been explained in [7] that the Newcomb-Borel paradox presented in [8] can be easily understood if one uses for a number  $x \in \mathbb{R}^+$  its (dynamic) *multiplicative* floating point representation in base  $\beta$ :

$$x = \beta^{\lfloor \log_\beta x \rfloor + 1} \times \beta^{\{\log_\beta x\} - 1} \quad (\text{Newcomb}),$$

rather than the more widespread (static) *additive* representation:

$$x = [x] + \{x\} \quad (\text{Borel}),$$

where  $[x]$  is the integer part of  $x$ , and  $0 \leq \{x\} < 1$ .

The Newcomb law (the first digit has 3 times more chances to be 1 than 9 in base 10) allows to discriminate between the *leading* digits which bear meaning, and the *trailing* digits which are uniformly distributed.

The reason behind Newcomb's law is the Lévy law of large numbers which rules Computation. The Lévy law (1939) states that the sum mod 1 of  $N$  random variables has a uniform distribution in the limit as  $N \rightarrow \infty$  [7]. This law is of critical importance for Computation:

- i) in floating point computation on the reals, it yields the uniform distribution of the logarithms of the mantissae (Newcomb),
- ii) in complex multiplication, the arguments add mod  $2\pi$ , therefore they become uniformly distributed after a number of successive multiplications.

It is therefore not surprising that the binary algebras  $B_0$  to  $B_3$  conspire at this emergence of meaning by an appropriate labeling. The top components will be ruled (exactly or approximately) by the law of computation in  $\mathbb{Z}_2^k$ ,  $k = 1$  to 4.

## 6 Odd and even partition of $B_k$ , $k \geq 1$

As stated in [2], any binary algebra  $B$  of the type  $B_k$ ,  $k \geq 0$ , is a particular case of *quadratic* algebra such that for any  $x \in B$ ,  $x^2 = 0$  or 1, that is  $x^2$  is a scalar in  $\mathbb{Z}_2$ . This remark allows to partition  $B$  into two equal parts  $E$  and  $O$ , respectively defined as:

- i) the *even* part  $E = \{x \in B; x^2 = 0\} = \{x \in B; x \text{ has an } \textit{even} \text{ number of zero and non zero components}\}$ ,
- ii) the *odd* part  $O = \{x \in B; x^2 = 1\} = \{x \in B; x \text{ has an } \textit{odd} \text{ number of zero and non zero components}\}$ .

For  $k \geq 1$ , the even and odd parts of  $B_k$  can easily be characterized from the even and odd parts of  $B_{k-1}$ , if we set  $x = (x_1, x_2) \in B_k$ , with  $x_1, x_2 \in B_{k-1}$ .

**Lemma 6.1**  *$x$  belongs to  $E_k$  (resp.  $O_k$ ) iff  $x_1$  and  $x_2$  belong to the same class, either  $E_{k-1}$  or  $O_{k-1}$  (resp. to the two different classes  $E_{k-1}$  and  $O_{k-1}$ ), for  $k \geq 1$ .*

**Proof:**  $x^2 = (x_1^2 + x_2^2, 0)$ . Therefore  $x^2 = 0 \Leftrightarrow x_1^2 = x_2^2 = 0$  or 1, and  $x^2 = 1 \Leftrightarrow x_1^2 \neq x_2^2$ .

□

The *even* part of  $B_k$  is created by choosing two elements in the *same* class of  $B_{k-1}$ . Whereas the *odd* class of  $B_k$  is created by *mixing*: it concatenates two elements chosen in each of the two different classes of  $B_{k-1}$ ,  $k \geq 1$ . Addition has the same effect as indicated by

**Lemma 6.2** *The (vector) sum  $x + y$  belongs to  $E$  (resp.  $O$ ) iff  $x$  and  $y$  are in the same class (resp. two different classes).*

**Proof:** Easy by induction. We get the following table for +:

+	$E$	$O$
$E$	$E$	$O$
$O$	$O$	$E$

□

## 6.1 The sequence of ones $\mathbf{e}_k = (11 \cdots 1) \in B_k, k \geq 1$

We consider in this paragraph the particular vector  $\mathbf{e}_k$  in  $B_k$ , whose  $2^k$  components are all 1. Therefore  $\mathbf{e}_k^2 = 0$  for  $k \geq 1$ . The case  $k = 0$  is exceptional:  $e_0 = 1 = e_0^2 \neq 0$ .

We mentioned in [4] that, for  $k = 1$  and 2, the element  $\mathbf{e}_k$ , equal respectively to (11) and (1111), plays a special role with respect to multiplication. We study here the properties of  $\mathbf{e}_k$  for any  $k \geq 1$ .

**Lemma 6.3** *For any  $x$  in  $B_k, k \geq 1, x \times \mathbf{e}_k = 0$  iff  $x \in E_k$ , and  $x \times \mathbf{e}_k = \mathbf{e}_k$  iff  $x \in O_k$ .*

**Proof:** We proceed by induction on  $k$ . For  $k = 1, (x_1, x_2) \times (1, 1) = (x_1 + x_2, x_1 + x_2) = (x_1 + x_2)\mathbf{e}_1$ .

It follows easily that, for an arbitrary  $k, x \times \mathbf{e}_k = (\sum_{i=1}^{2^k} x_i)\mathbf{e}_k$ , where  $x_i \in \mathbb{Z}_2$ . Next  $\sum_i x_i = 0$  (resp.  $= 1$ ) iff  $x \in E_k$  (resp.  $O_k$ ).

□

## 6.2 The equation $a \times x = b$ (1) revisited

We analyzed (1) in [4] for  $k = 0, 1, 2$ . What can be said about (1) in general, using the notion of odd and even parts for  $B_k, k > 0$  ?

$B = E \cup O$  denotes a generic binary algebra of dimension  $2^k, k \geq 1$ .

The algebra  $B_0 = \{0, 1\}$  is exceptional because  $e = 1$  is such that  $e^2 = 1$  and not 0 as is the case for  $k \geq 1 : \mathbf{e}^2 = 0$ .

We introduce the

### Definition 6.1

*The set of zerodivisors in  $E$  relative to  $a \in B$  is  $Z(a) = \{x; a \times x = 0\}$ .*

*The set of solutions of (1) in  $B$  is  $S(a, b) = \{x; a \times x = b\}$ .*

*For  $a \in B, \bar{a} = \mathbf{e} + a$  denotes the binary sequence of complements to 1.*

□

$Z(a) = \text{Ker } M(a)$  was introduced in [4], where it is proved that  $Z(a) = \{0\} \Leftrightarrow a \in O$  for  $k \geq 0$ . Moreover  $S(a, b) = \{x = a \times b\}$  consists of a unique element  $x \Leftrightarrow a \in O$ .

In this paragraph, we consider the case  $a \in E$ .

For  $a = b = \mathbf{e} \in E$ , Lemma 6.3 shows that  $Z(\mathbf{e}) = E$  and  $S(\mathbf{e}, \mathbf{e}) = O \cup E = B$ . For  $a = 0, Z(0) = B$  and  $S(0, b) = \emptyset$  for  $b \neq 0$ , whereas  $S(0, 0) = B$  for  $b = 0$ .

The case  $k = 1$  is particular because  $E = \{0, \mathbf{e}\}$  and the only nonzero value for  $a$  is  $\mathbf{e}$ . The general case begins with  $k = 2$  where the case  $a \neq \mathbf{e}$  is possible. Therefore  $a \notin \{0, \mathbf{e}\}$  is possible. Note that  $a \neq a + e = \bar{a}$  is always true.

**Lemma 6.4** *For  $k \geq 2$ ,  $Z(a)$  contains at least four distinct elements, which, for  $a \notin \{0, \mathbf{e}\}$ , are  $\{0, \mathbf{e}, a, \bar{a}\} = N(a)$ .*

**Proof:** Clear for  $a = 0$  and  $a = \mathbf{e}$ . For  $a \notin \{0, \mathbf{e}\}$  then  $N(a)$  is closed under the complementation operation  $a \rightarrow \bar{a}$ .  $a \in Z(a)$  because  $a^2 = a \times a = 0$ , and  $\bar{a} \in Z(a)$  because  $a \times (a + \mathbf{e}) = 0 + a \times \mathbf{e} = 0$  for any  $a$  in  $E$ , by Lemma 6.3.

□

We now look at the structure of  $S(a, b) = \xi + Z(a)$ , where  $\xi$  is a particular solution of (1) [4].

We first note that  $a \times x = b$  for  $a \in E$  requires  $a \times b = 0$ , that is  $b \in Z(a) \subset E$ . Clearly  $\xi \in O$  (resp.  $E$ ) implies  $S(a, b) \subset O$  (resp.  $E$ ).

**Lemma 6.5**

- i) *When  $x \in O$  is a solution of (1)  $a \times x = b$ , it is also a solution of (2)  $b \times x = a$  and (3)  $\bar{a} \times x = \bar{b}$ .*
- ii) *When  $x \in E$  is a solution of (1), it is also a solution of (4)  $\bar{a} \times x = b$  and (5)  $b \times x = 0$ .*

**Proof:** i) (1) with  $x^2 = 1$  implies (2). And (1), (3) imply  $\mathbf{e} \times x = \mathbf{e}$  which is true for any  $x \in O$ .

ii) (1) and  $x^2 = 0$  imply (5), that is  $x \in Z(b) \subset Z(Z(a))$ . (1) and (4) imply  $\mathbf{e} \times x = 0$  which is satisfied for any  $x \in E$ .

□

Depending whether  $x$  belongs to  $O$  or  $E$ ,  $x$  satisfies (1) together with (2), (3) or with (4), (5). When at least one solution  $x$  exists, then unless  $a = b = 0$  (resp.  $\mathbf{e}$ ), in which case  $S(0, 0)$  (resp.  $S(\mathbf{e}, \mathbf{e}) = B = E \cup O$ ),  $x$  belongs to  $O$  or  $E$ , with an *exclusive* or, by Lemma 6.3.

To describe the solutions of (1), we see emerging the iterated set  $Z(Z(a)) = Z^2(a)$ , the set of zero divisors relative to the zero divisors of  $a$ .

**Lemma 6.6** *For  $k \geq 2$ ,  $Z^2(a) = \bigcup_{b \in Z(a)} Z(b) = E$ .*

**Proof:** For  $k \geq 1$ ,  $x = \mathbf{e}$  satisfies  $a \times \mathbf{e} = b \times \mathbf{e} = 0$  for any  $a, b \in E$ . Therefore  $\mathbf{e} \in Z(a)$  and  $E \supseteq Z^2(a) \supset Z(\mathbf{e}) = E$ .

□

The choice of  $\mathbf{e}$  as a particular solution for (1) implies that  $S(a, b) = Z(a) \subset E$ . It is remarkable that  $S(a, b)$  is independent of  $b$ .

What can be said for the choice of particular solutions in  $O$  ?

We define  $\xi \in O$  as a particular solution of (1),  $i = 1, 2, 3$ . We get for  $S(a, b)$  the 3 representations  $S(a, b) = \xi_1 + Z(a) = \xi_2 + Z(\bar{a}) = \xi_3 + Z(b)$ , where  $b \in Z(a)$ . The 3 representations should agree for  $k \geq 2$ , where we know that  $Z(a), Z(\bar{a}) \supset \{0, \mathbf{e}, a, \bar{a}\}$  and  $Z(b) \supset \{0, \mathbf{e}, b, \bar{b}\}$ .

**Proposition 6.1** *For  $k \geq 2$ , and  $a, b \notin \{0, \mathbf{e}\}$  the set  $S(a, b)$  contains at least 4 solutions to (1) and less than  $2^{2^k-1} = \frac{N_k}{2}$ .*

**Proof:** Clear. See Table 4.1 in [4] for  $k = 2$ .

□

The values  $\frac{N_k}{2}$  and  $N_k$  can be obtained for exceptional values of  $(a, b)$ :

- 1) for  $a = b = \mathbf{e}$ ,  $\mathbf{e} \times x = \mathbf{e}$  has the *two* particular solutions  $\xi = \mathbf{e}$  in  $E$  and  $\xi = 1$  in  $O$ :  $\mathbf{e} \times (1 + \mathbf{e}) = \mathbf{e}$ . Therefore  $S(\mathbf{e}, \mathbf{e}) = E \cup O = B$ . The same is true for  $a = b = \bar{\mathbf{e}} = 0$ :  $S(0, 0) = B$ .
- 2) for  $a = \mathbf{e}$ , solutions exist only for  $b = 0$  ( $S(\mathbf{e}, 0) = E$ ) and  $b = \mathbf{e}$  ( $S(\mathbf{e}, \mathbf{e}) = B$ ).
- 3) for  $b = \mathbf{e}$ , solutions exist for  $a = \mathbf{e}$  only.
- 4) for  $a = 0$ , solutions exist for  $b = 0$  only:  $S(0, 0) = B$ . In particular  $S(0, \mathbf{e}) = \emptyset$ .

One last remark: in general  $\xi$  in  $O$  depends on  $b$ . For the case  $a = b$ ,  $\xi = 1$  is a particular solution in  $O$  of  $a \times x = a$ . Therefore  $S(a, a) \subset O$  for  $a \neq 0$  and  $\neq \mathbf{e}$ .

The non symmetric role of the 4 exceptional points  $(0, 0)$  and  $(\mathbf{e}, \mathbf{e}) \Rightarrow S = B$ ,  $(0, \mathbf{e}) \Rightarrow S = \emptyset$  and  $(\mathbf{e}, 0) \Rightarrow S = E$  is illustrated on Figure 6.1, where  $a$  (resp.  $b$ ) can take any of the  $\frac{N}{2}$  discrete even values in  $E$  on the horizontal (resp. vertical) axis.  $N$  is generic for  $N_k = 2^{2^k}$ ,  $k \geq 2$ .

## 7 Conclusion

This work has studied the algebras  $B_k$  of binary sequences of dimension  $2^k$ ,  $k \geq 0$ , equipped with a structure of hypercomplex multiplication. We

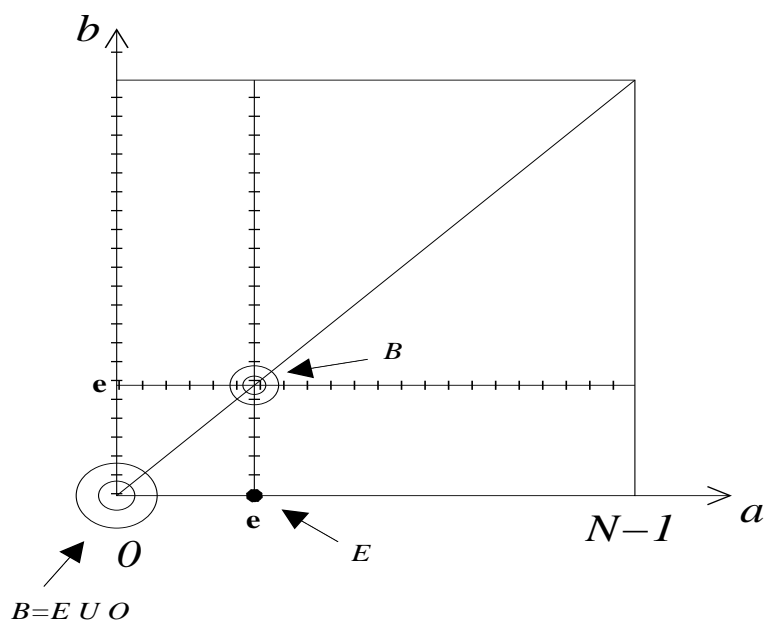
showed that with an appropriate order, the structure of  $B_k$  can be related, partially or totally, to that of  $\mathbb{Z}_{2^{k+1}}$ , for small enough  $k$ .

For  $k = 0$  and  $1$ , the relation is total and exact. For  $k = 2$  and  $3$ , the relation is partial, and approximate. The error rate grows from  $2^{-4}$  to  $\sim 2^{-1}$  when  $k$  increases from  $2$  to  $3$ .

The resolution of  $a \times x = b$  in  $B_k = E_k \cup O_k$ ,  $k \geq 1$ , has also been investigated. We proved the remarkable fact that for any  $k \geq 2$ , the equation (1) has always at least 4 solutions for  $a, b \in E - \{0, \mathbf{e}\}$ .

## References

- [1] F. Chaitin–Chatelin, T. Meškauskas, Computation With Hypercomplex Numbers, *Nonlinear Analysis* **47**, pp. 3391–3400 (2001). (Also available as CERFACS Technical Report TR/PA/00/69).
- [2] F. Chaitin–Chatelin, T. Meškauskas, A. N. Zaoui, About real and binary algebras: the interplay between Geometry and Algebra, *CERFACS Technical Report* TR/PA/00/74 (2000).
- [3] A. N. Zaoui, Deux Contributions au Calcul Scientifique I- Sur la convergence de la méthode des Itérations Simultanées couplée à l’algorithme d’Arnoldi itératif II-Autour du Calcul Hypercomplexe, *Ph. D. dissertation*, CERFACS and Université Toulouse I, TH/PA/00/78 (2000).
- [4] F. Chaitin–Chatelin, T. Meškauskas, A. N. Zaoui, Hypercomplex division in the presence of zero-divisors on  $\mathbb{R}$  and  $\mathbb{Z}_2$ , *CERFACS Technical Report* TR/PA/02/29 (2002).
- [5] T. Meškauskas, Private communication, *CERFACS*, March 2002.
- [6] F. Chaitin-Chatelin, The computing power of Geometry, In D. F. Griffiths and G. A. Watson, editors, *Numerical Analysis 1999*, CRC Press LLC (1999). (Also available as CERFACS Technical Report TR/PA/99/24).
- [7] F. Chaitin-Chatelin, E. Traviesas, Qualitative Computing, *CERFACS, Technical Report* TR/PA/02/58, 2002. *To appear in the SIAM book: Bo Einarsson Ed., Handbook of Computation, IFIP WG 2.5.*
- [8] F. Chaitin-Chatelin, Les ordinateurs calculent faux et c’est tant mieux, *Journées Observatoire de Paris*, Juin 1991.



**Figure 6.1.** The 4 exceptional points  $(a, b) \in \{0, \mathbf{e}\}$  for the set of solutions  $S(a, b)$ ,  $a, b \in E$ .