Tatra Mt. Math. Publ. **9x** (2026), 1–20
DOI: 10.2478/tmmp-2026-0017

TATRA MOUNTAINS
Mathematical Publications

THREE REMARKS ON GROUPOIDS WITH PRESCRIBED NUMBER OF ASSOCIATIVE TRIPLES

Otokar Grošek[1,2] — Marián Kňazovický[2]

[1]Institute of Mathematics, Slovak Academy of Sciences, Bratislava, Slovakia

[2]Department of Informatics and Mathematics, Slovak Technical University, Bratislava, Slovakia

ABSTRACT. In this work, based on the results of A. C. Climescu: *Études sur la théorie des systémes multiplicatifs uniformes I. L'indice de non-associativité*, we construct an algorithm for generating a finite groupoid with the required number of elements and associative triples. This algorithm is practically limited only by the set of available symbols (alphabet) of groupoids. It can be randomized by finding new (random) examples of groupoids with a prescribed number of associative triples for $n = 3, 4, 5$, which is an easy task for a computer.

We also investigate associativity classes of a groupoid with exactly i associative triples and present a new two-parameter form for the symbol-frequency table on an associativity class. Finally, we present a hypothesis that could give a new proof of the Climescu Theorem for $n \geq 4$.

1. Introduction

The central concept in this work is the concept of a *groupoid*, i.e., a non-empty finite set G together with the binary operation $*$, which can also be understood as a function

$$f\colon G \times G \to G, \quad \forall a, b \in G \implies a * b \in G.$$

Let $A(G)$ stands for the set of associative triples of G, i.e., the set of all ordered triples (a, b, c) of elements of G such that

$$\forall (a, b, c) \in A(G) \iff (a * b) * c = a * (b * c).$$

© 2026 Mathematical Institute, Slovak Academy of Sciences.
2020 Mathematics Subject Classification: 20N02.
Keywords: groupoids with prescribed number of associative triples.
Supported by the Grant VEGA 2/0119/23 and VEGA 2/0054/24.
Licensed under the Creative Commons BY-NC-ND 4.0 International Public License.

Clearly, non-associative triples of G form the complement in $G \times G \times G = G^3$, i.e., $NA(G) = G^3 \setminus A(G)$. The cardinality of the set $|NA(G)| = k$ is called *index of non-associativity*.

(1) According to the definition of the non-associativity index, a semigroup has index $k = 0$.

(2) For the non-associativity index, we have possible values $0 \leq k \leq n^3$, where n is the number of elements (order) of the groupoid.

(3) Groupoids of given order n can be divided into disjoint classes according to the value of the non-associativity index k.

(4) Analogously, we define the associativity index $i = n^3 - k$.

Let M, $|M| = n \geq 3$, be the underlying set. Climescu [2] proved that there exists a binary operation (function f_i) such that the cardinality of all associative triples $|A(M, f_i)| = i$ for all $i = 0, 1, \ldots, n^3$. Another approach to this problem is presented in [4].

The use of groupoids as algebraic structures is not used in practice to the same extent as, for example, groups, rings, and fields. However, the generalization of these structures and their properties has influenced some cryptographic schemes and areas of research. Next, we briefly introduce the practical use of groupoids in cryptography.

In the work [8], the author presents a generalized Anshel-Anshel-Goldfield Key Establishment Protocol (AAG KEP) for groupoids. This is a new concept of non-associative public-key cryptography (PKC).

Homomorphic encryption allows some mathematical operations on encrypted texts. In the work [9], the authors constructed an example of an El-Gamal cryptosystem using non-associative operations, which is homomorphic to group and quasi-group operations.

Partially associative groupoids can replace classical operations (e.g., XOR or Galois field multiplication) and introduce a new nonlinearity that is harder to analyze for linear and differential cryptanalysis [11]. For example, instead of the traditional XOR in a cipher round, we can use an associative groupoid operation only for some inputs.

Some cryptographic primitive designs consider using algebraic operations similar to those in groupoids. These operations are based on non-commutative and/or non-associative structures, which allow the creation of one-time keys or encryption operations that are harder to analyze for quantum algorithms [6, 7].

Another reason to use groupoids in cryptography is the following fact: To evaluate the product of n elements of a groupoid, we must know where the parentheses are. The number of their possible distribution is given by the Catalan

number C_{n-1} [12], where

$$C_n = \frac{1}{n+1}\binom{2n}{n} \quad \text{and} \quad C_n \approx \frac{1}{(1+n)\sqrt{\pi n}}2^{2n}.$$

Our contribution to this study is as follows:

In Section 2, based on some lemmas of Climescu [2], we present an algorithm to find a groupoid G of order n with a prescribed number of associative triples, say k.

In Section 3, we present a two-parameter form for the symbol-frequency table of an associativity class.

In Section 4, a new hypothesis is presented which would lead to a new proof of the Climescu theorem. Groupoids of this type are partially presented in the amendment.

2. How to find a groupoid of order n with k associative triples

The construction of a groupoid with a prescribed number of non-associative triples k is based on six lemmas. The main idea of the proof is as follows. First of all, we need Cayley tables for $n = 3, 4, 5$ with all possible indices of non-associativity k. Then we define their special extension $n+1, n+2, n+3$ to cover all possible classes of groupoids with possible indices of non-associativity. Using these tables, we will introduce an Algorithm with INPUT n, k and OUTPUT a groupoid G with required parameters n, k.

Lemma 2.1. *Let G be a groupoid of order n and index of non-associativity k. Then we can construct a groupoid of order $n+1$ with the same index of non-associativity k.*

Let $x_1, x_2, \ldots, x_n$ be elements of the former groupoid with the new element $x_{n+1} = a$, and let the new Cayley table to Lemma 2.1 be as follows:

	x_1	$\ldots$	x_n	a
x_1	$\ldots$		$\ldots$	a
$\vdots$	$\vdots$		$\vdots$	$\vdots$
x_n	$\ldots$		$\ldots$	a
a	a	$\ldots$	a	a

Lemma 2.2. *Let G be a groupoid of order n and index of non-associativity k. Then we can construct a groupoid of order $n+2$ and index of non-associativity $k + 4n^2 + 4n + 8$.*

Let $x_1, x_2, \ldots, x_n$ be elements of the former groupoid with the new elements $x_{n+1} = a$, $x_{n+2} = b$, and let the new Cayley table to Lemma 2.2 be as follows:

	x_1	$\ldots$	x_n	a	b
x_1	$\ldots$		$\ldots$	b	a
$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$
x_n	$\ldots$		$\ldots$	b	a
a	a	$\ldots$	a	b	b
b	a	$\ldots$	a	a	a

Lemma 2.3. *Let G be a groupoid of order n and index of non-associativity k. Then we can construct a groupoid of order $n+2$ and index of non-associativity $k + 4n^2 + 8n + 8$.*

The new groupoid of order $n+2$ with $x_{n+1} = a$, $x_{n+2} = b$ and the new Cayley table to Lemma 2.3 is as follows:

	x_1	$\ldots$	x_n	a	b
x_1	$\ldots$		$\ldots$	b	a
$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$
x_n	$\ldots$		$\ldots$	b	a
a	b	$\ldots$	b	b	a
b	a	$\ldots$	a	b	a

Lemma 2.4. *Let G be a groupoid of order n and index of non-associativity k. Then we can construct a groupoid of order $n+3$ and index of non-associativity $k + 6n^2 + 18n + 27$.*

The new groupoid of order $n+3$ with $x_{n+1} = a$, $x_{n+2} = b$, $x_{n+3} = c$ and the new Cayley table to Lemma 2.4 is as follows:

	x_1	$\ldots$	x_n	a	b	c
x_1	$\ldots$		$\ldots$	b	c	a
$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$
x_n	$\ldots$		$\ldots$	b	c	a
a	b	$\ldots$	b	b	c	a
b	c	$\ldots$	c	b	c	a
c	a	$\ldots$	a	b	c	a

Lemma 2.5. *Let G be a groupoid of order n and index of non-associativity k. Then we can construct a groupoid of order $n+3$ and index of non-associativity $k + 6n^2 + 27n + 27$.*

The new groupoid of order $n+3$ with $x_{n+1} = a$, $x_{n+2} = b$, $x_{n+3} = c$ and the new Cayley table to Lemma 2.5 is as follows:

	x_1	$\dots$	x_n	a	b	c
x_1	$\dots$		$\dots$	b	c	a
$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$
x_n	$\dots$		$\dots$	b	c	a
a	a	$\dots$	a	b	c	a
b	a	$\dots$	a	b	c	a
c	a	$\dots$	a	b	c	a

Lemma 2.6. *Let G be a groupoid of order n and index of non-associativity k. Then we can construct a groupoid of order $n+3$ and index of non-associativity $k + 9n^2 + 27n + 27$.*

The new groupoid of order $n+3$ with $x_{n+1} = a$, $x_{n+2} = b$, $x_{n+3} = c$ and the new Cayley table to Lemma 2.6 is as follows:

	x_1	$\dots$	x_n	a	b	c
x_1	$\dots$		$\dots$	b	a	a
$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$
x_n	$\dots$		$\dots$	b	a	a
a	c	$\dots$	c	b	a	a
b	c	$\dots$	c	b	a	a
c	b	$\dots$	b	b	a	a

From the previous six lemmas, one can prove the main theorem of Climescu [2]

Theorem 2.7. *For arbitrary $n \geq 3$, there exist groupoids of order n and index of non-associativity $k = 0, 1, 2, \dots, n^3$.*

2.1. Algorithm to construct a groupoid with n, k.

In this subsection, we present our new Algorithm. Groupoids from Amendment can be replaced with arbitrary ones with the same k. The index of the groupoid in the list represents its k value. [1]

Algorithm 1.

$bases[][][]$ = list of groupoids with index of non-associativity $0 \leq k \leq 125$
$G[n][n]$ = variable with allocated memory for storage of resulting groupoid
function GenerateGroupoid(G, n, k)
    if $k < 0$ **or** $k > n^3$ **then**

[1] In the original list of groupoids [2], the groupoid for $n = 4$, $k = 50$, did not have the required $k = 50$.

```
        raise ValueError: Non-valid index k.
    end if
    if n ≤ 5 then
        if (n = 3 ∧ k ≤ 27) ∨ (n = 4 ∧ 28 ≤ k ≤ 64) ∨ (n = 5 ∧ 96 ≤ k ≤ 125)
then
            if i ≤ 64 then
                for i ← 1 to n do
                    for j ← 1 to n do
                        G[i][j] ← bases_below64[k][i][j]
                    end for
                end for
                return G
            end if
            if i ≥ 96 then
                for i ← 1 to n do
                    for j ← 1 to n do
                        G[i][j] ← bases_above96[k − 96][i][j]
                    end for
                end for
                return G
            end if
        else if (n = 4 ∧ k ≤ 27) ∨ (n = 5 ∧ k ≤ 64) then
            G ← GenerateGroupoid(G, n − 1, k)
            return Lemma1(G, n − 1)
        else if 65 ≤ k ≤ 83 ∧ n = 5 then
            k′ ← k − 4 · (n − 2)^2 − 4 · (n − 2) − 8
            G ← GenerateGroupoid(G, n − 2, k′)
            return Lemma2(G, n − 2)
        else if 68 ≤ k ≤ 95 ∧ n = 5 then
            i′ ← k − 4 · (n − 2)^2 − 8 · (n − 2) − 8
            G ← GenerateGroupoid(G, n − 2, k′)
            return Lemma3(G, n − 2)
        end if
    else if k < (n − 1)^3 then
        G ← GenerateGroupoid(G, n − 1, k)
        return Lemma1(G, n − 1)
    else if 4·(n−3)^2+12·(n−3)+16 ≤ k ≤ (n−3)^3+7·(n−3)^2+15·(n−3)+17
then
        k′ ← k − 4 · (n − 2)^2 − 4 · (n − 2) − 8
        G ← GenerateGroupoid(G, n − 2, k′)
        return Lemma2(G, n − 2)
```

else if $4\cdot(n-3)^2+16\cdot(n-3)+20 \leq k \leq (n-3)^3+7\cdot(n-3)^2+19\cdot(n-3)+21$ **then**
  $k' \leftarrow k - 4\cdot(n-2)^2 - 8\cdot(n-2) - 8$
  $G \leftarrow$ GENERATEGROUPOID$(G, n-2, k')$
  return LEMMA3$(G,\ n-2)$
else if $6\cdot(n-3)^2+18\cdot(n-3)+27 \leq k \leq (n-3)^3+6\cdot(n-3)^2+18\cdot(n-3)+27$ **then**
  $k' \leftarrow k - 6\cdot(n-3)^2 - 18\cdot(n-3) - 27$
  $G \leftarrow$ GENERATEGROUPOID$(G, n-3, k')$
  return LEMMA4$(G,\ n-3)$
else if $6\cdot(n-3)^2+27\cdot(n-3)+27 \leq k \leq (n-3)^3+6\cdot(n-3)^2+27\cdot(n-3)+27$ **then**
  $k' \leftarrow k - 6\cdot(n-3)^2 - 27\cdot(n-3) - 27$
  $G \leftarrow$ GENERATEGROUPOID$(G, n-3, k')$
  return LEMMA5$(G,\ n-3)$
else if $9\cdot(n-3)^2+27\cdot(n-3)+27 \leq k \leq (n-3)^3+9\cdot(n-3)^2+27\cdot(n-3)+27$ **then**
  $k' \leftarrow k - 9\cdot(n-3)^2 - 27\cdot(n-3) - 27$
  $G \leftarrow$ GENERATEGROUPOID$(G, n-3, k')$
  return LEMMA6$(G,\ n-3)$
end if
end function

The algorithm utilizes individual lemmas and is a practical verification of Theorem 2.7. It is based on recursion. It nests into the depth, gradually decreasing n (except in the case of Lemma 2.1, which also decreases k), until it reaches the stage when one of the base groupoids is selected. Subsequently, when emerging from the recursion, it gradually applies *coverings* (in the sense of the representation in the Cayley table) to this groupoid with new elements that represent individual lemmas.

For the convenience of the reader, we indicate which lemma is applied each time we use it. Then we can observe the individual steps of the algorithm. We present the algorithm's progress in the following example.

EXAMPLE. Let the input to the Algorithm be $n = 13$, $k = 1393$.

The output of the algorithm will be as follows:

```
Using Lemma 1, choosing groupoid of order 12 with k 1393
Using Lemma 2, choosing groupoid of order 12 with k 1393
Using Lemma 6, choosing groupoid of order 10 with k 945
Using Lemma 5, choosing groupoid of order 7 with k 288
Choosing groupoid of order 4 with k 57
```

```
Groupoid of order 13 with k 1393:

['d', 'c', 'b', 'c', 'f', 'g', 'e', 'i', 'h', 'h', 'l', 'k', 'm']
['b', 'a', 'd', 'a', 'f', 'g', 'e', 'i', 'h', 'h', 'l', 'k', 'm']
['b', 'd', 'b', 'a', 'f', 'g', 'e', 'i', 'h', 'h', 'l', 'k', 'm']
['b', 'c', 'd', 'd', 'f', 'g', 'e', 'i', 'h', 'h', 'l', 'k', 'm']
['e', 'e', 'e', 'e', 'f', 'g', 'e', 'i', 'h', 'h', 'l', 'k', 'm']
['e', 'e', 'e', 'e', 'f', 'g', 'e', 'i', 'h', 'h', 'l', 'k', 'm']
['e', 'e', 'e', 'e', 'f', 'g', 'e', 'i', 'h', 'h', 'l', 'k', 'm']
['j', 'j', 'j', 'j', 'j', 'j', 'j', 'i', 'h', 'h', 'l', 'k', 'm']
['j', 'j', 'j', 'j', 'j', 'j', 'j', 'i', 'h', 'h', 'l', 'k', 'm']
['i', 'i', 'i', 'i', 'i', 'i', 'i', 'i', 'h', 'h', 'l', 'k', 'm']
['k', 'k', 'k', 'k', 'k', 'k', 'k', 'k', 'k', 'k', 'l', 'l', 'm']
['k', 'k', 'k', 'k', 'k', 'k', 'k', 'k', 'k', 'k', 'k', 'k', 'm']
['m', 'm', 'm', 'm', 'm', 'm', 'm', 'm', 'm', 'm', 'm', 'm', 'm']
```

In the output, we observe recursive nesting unless we encounter a base groupoid of order 4 with the non-associative index $k = 57$. The condition for selection from the list of base groupoids *bases* is met. We select a groupoid with $k = 57$, which is in the Cayley table notation groupoid:

	a	b	c	d
a	d	c	b	c
b	b	a	d	a
c	b	d	b	a
d	b	c	d	d

The next step is to use Lemma 2.5. Since we have been nesting recursively, we will use the individual lemmas in the order of emergence, i.e., from bottom to top. Lemma 2.5 will increase the order to $n + 3 = 7$ and the index to $k + (6 \cdot n^2 + 27 \cdot n + 27) = 57 + (6 \cdot 16 + 27 \cdot 4 + 27) = 57 + 231 = 288$. Recall what the use of Lemma 2.5 looks like.

	x_1	$\dots$	x_n	a	b	c
x_1	$\dots$		$\dots$	b	c	a
$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$
x_n	$\dots$		$\dots$	b	c	a
a	a	$\dots$	a	b	c	a
b	a	$\dots$	a	b	c	a
c	a	$\dots$	a	b	c	a

Not to be confused with the element labels, we recall that the elements $x_1, \dots, x_n$ represent the current alphabet, and the elements a, b, c represent the new elements in the alphabet after the extension to $n + 3$.

In our example, the alphabet used so far has size $n = 4$ and elements a, b, c, d. The new elements will be e, f, g. Thus, $x_1, \ldots, x_n = a, b, c, d$ and the elements a, b, c will correspond to the elements e, f, g. Then the new groupoid after applying Lemma 2.5 will be as follows:

	a	b	c	d	e	f	g
a	d	c	b	c	f	g	e
b	b	a	d	a	f	g	e
c	b	d	b	a	f	g	e
d	b	c	d	d	f	g	e
e	e	e	e	e	f	g	e
f	e	e	e	e	f	g	e
g	e	e	e	e	f	g	e

which exactly corresponds to the selection of the first 7 rows and first 7 columns in the output of the resulting groupoid.

Let us look at the next statement. Lemma 2.6 was used, and the order increased by 3, so $n + 3 = 7 + 3 = 10$. It added three more elements h, i, j to the alphabet. The index increases to $k+(9\cdot n^2+27\cdot n+27) = 288+(9\cdot 49+27\cdot 7+27) = 288 + 657 = 945$.

In the following statement we see that Lemma 2.2 has been used. This lemma increases the order by 2 from 10 to 12. It adds new elements k and l to the alphabet. The index increases to $k+(4\cdot n^2+4\cdot n+8) = 945+(4\cdot 100+4\cdot 10+8) = 945 + 448 = 1393$.

The last statement (first in the output) is the application of Lemma 2.1. This lemma adds 1 new element, so it increases the order by $1, n + 1 = 12 + 1 = 13$, and does not increase the index $k = 1393$.

3. On the symbol-frequency table of an associativity class

An exhaustive computer search would give us precise answers to the statistical properties of the occurrence of elements in groupoids, as well as to their decomposition into associativity classes. However, we must realize that the number of groupoids grows super-exponentially in the number of elements of a groupoid.

For each pair $a, b \in G$, we must define the result of the binary operation $*$. This can be expressed by an $n \times n$ matrix, where each element represents the result of the operation for a particular pair of elements (Cayley table). Each of these n^2 pairs has n possibilities for the result of the binary operation (because $*$ is closed on M, $|M| = n$). This means that there are n^{n^2} such tables that we can create.

For illustration, the number of all groupoids by the number of elements is as follows:

- $n = 2 : 2^{2^2} = 16 = 2^4$
- $n = 3 : 3^{3^2} = 19683 \doteq 2^{14}$
- $n = 4 : 4^{4^2} = 4294967296 \doteq 2^{32}$
- $n = 5 : 5^{5^2} \doteq 2.9802322 \cdot 10^{17} \doteq 2^{58}$
- $n = 6 : 6^{6^2} \doteq 1.0314425 \cdot 10^{28} \doteq 2^{93}$

3.1. A preliminary computer search

A complete search and subsequent statistics for $n = 3$ and $n = 4$ was performed. For a fixed order n and a fixed index of associativity i in the corresponding class of groupoids K_i, we investigated the frequency of occurrence of individual elements. We found that, e.g., for $n = 3$ and $i = 4$, there is a unique assignment between the frequency table of elements a, b, c at a given position (cell) and the number of associative triples:

TABLE 1. Ocurrences of elements a, b, c for Cayley tables $n = 3$ and $i = 4$ associative triples. Number of groupoids in K_4 is $m = 504$.

32, 236, 236	138, 138, 228	138, 228, 138
	236, 32, 236	228, 138, 138
		236, 236, 32

Thus, for given $(n, i, m) = (3, 4, 504)$, there exists numbers x, y included in Table 2 and vice versa:

TABLE 2. Frequency of elements a, b, c for Cayley tables $n = 3$ and $i = 4$ associative triples expressed by m, x, y.

$x, \frac{m-x}{2}, \frac{m-x}{2}$	$\frac{m-y}{2}, \frac{m-y}{2}, y$	$\frac{m-y}{2}, y, \frac{m-x}{2}$
	$\frac{m-x}{2}, x, \frac{m-x}{2}$	$y, \frac{m-y}{2}, \frac{m-y}{2}$
		$\frac{m-x}{2}, \frac{m-x}{2}, x$

By exhaustive search, we have Tables 3 and 4, i.e., for each i the values n, x, y for $n = 3$ and $n = 4$ (see Amendment) are presented.

We were unable to prove this observation, but an anonymous reviewer provided the evidence we are presenting below in Lemma 3.1 through a very thorough review: *This observation can be proved as a corollary of orbit-counting under the relabelling and opposite-groupoid symmetries for all $n \geq 3$. I attach a proof. The authors are free to use the proof in their revised version of the paper.*

TABLE 3. Table for groupoids of order $n = 3$, and elements $\{a, b, c\}$, with number of associative triples $i \in \{0, 1, \ldots, n^3\}$.

i	m	x	y	i	m	x	y	i	m	x	y
0	52	0	26	9	1456	256	570	18	840	448	238
1	12	0	6	10	1290	294	528	19	939	451	227
2	96	0	44	11	1266	344	498	20	732	392	164
3	276	12	122	12	1208	368	442	21	569	270	144
4	504	32	228	13	1350	444	462	22	432	272	60
5	468	28	204	14	1212	456	428	23	369	235	65
6	628	48	244	15	1296	528	412	24	168	120	20
7	936	124	280	16	1008	428	286	25	198	136	16
8	966	98	386	17	1212	554	340	26	60	44	4
								27	113	79	17

3.2. A two-parameter form for the symbol-frequency table of an associativity class

Throughout, a *groupoid* is a finite set with a binary operation (a magma). Fix an integer $n \geq 3$ and identify the underlying set with $[n] = \{1, \ldots, n\}$. For a groupoid G on $[n]$, we write $G_{r,c}$ for the entry in row r, column c of its Cayley table, i.e., the product of the r-th and c-th elements. A triple (x, y, z) is *associative* in G if $(x * y) * z = x * (y * z)$.

LEMMA 3.1. *Let $n \geq 3$ and let i be an integer. Let K_i be the set of groupoids on $[n]$ with exactly i associative triples, and put $m = |K_i|$. For a cell $(r, c) \in [n]^2$ and a symbol $s \in [n]$, define the count*

$$N_{(r,c)}(s) = \#\{\, G \in K_i : G_{r,c} = s \,\}.$$

Then there exist numbers x, y (depending on n and i) such that, for every cell (r, c) and symbol s,

$$N_{(r,c)}(s) = \begin{cases} x, & r = c = s \quad \textit{(diagonal cell, its own label)}, \\ \dfrac{m - x}{n - 1}, & r = c \neq s \quad \textit{(diagonal cell, a foreign label)}, \\ \dfrac{m - (n-2)\,y}{2}, & r \neq c,\ s \in \{r, c\} \quad \textit{(off-diagonal, row or column label)}, \\ y, & r, c, s \textit{ pairwise distinct} \quad \textit{(off-diagonal, neither label)}. \end{cases}$$

In particular, the entire frequency table is determined by the two numbers x, y (together with m).

P r o o f. Let $\mathcal{G}_n$ be the set of all groupoids on $[n]$. Two maps act on it.

Relabeling. For $\sigma \in S_n$, define $\sigma{\cdot}G$ by $(\sigma{\cdot}G)_{\sigma r,\,\sigma c} = \sigma(G_{r,c})$; this is the isomorphic image of G under σ.

Transposition. Define $\mathrm{op}\,{\cdot}G = G^{\mathrm{op}}$ by $(G^{\mathrm{op}})_{r,c} = G_{c,r}$, the opposite groupoid.

Both maps are bijections of $\mathcal{G}_n$, hence elements of $\mathrm{Sym}(\mathcal{G}_n)$. Let

$$\Gamma = \langle\, S_n,\ \mathrm{op} \,\rangle \ \le\ \mathrm{Sym}(\mathcal{G}_n)$$

be the subgroup they generate. Since $\mathrm{op}^2 = \mathrm{id}$ and $(\sigma \cdot G)^{\mathrm{op}} = \sigma \cdot (G^{\mathrm{op}})$ for all σ (relabeling and transposing commute), op is a central involution and

$$\Gamma \ \cong\ S_n \times \mathbb{Z}/2\mathbb{Z}, \qquad |\Gamma| = 2\,n!.$$

Step 1: Γ permutes K_i. Isomorphic groupoids have the same number of associative triples, so each $\sigma \in S_n$ maps K_i bijectively to itself. For op: if (x, y, z) is associative in G, then (z, y, x) is associative in G^{op}, and the map $(x, y, z) \mapsto (z, y, x)$ is a bijection of $[n]^3$; hence G and G^{op} have equally many associative triples, so op also maps K_i bijectively to itself. Therefore, every element of Γ restricts to a bijection of K_i.

Step 2: Induced action on triples, and invariance of N. The same group Γ acts on the position–symbol triples $(r, c, s) \in [n]^3$ by

$$\sigma \cdot (r, c, s) = (\sigma r,\ \sigma c,\ \sigma s), \qquad \mathrm{op}\,{\cdot}(r, c, s) = (c,\ r,\ s).$$

(On triples $\mathrm{op}^2 = \mathrm{id}$ and op commutes with the diagonal S_n-action, so this is again an action of $S_n \times \mathbb{Z}/2$.) Because the two generators are bijections of K_i,

$$N_{(r,c)}(s) = N_{(\sigma r,\,\sigma c)}(\sigma s) \quad (\sigma \in S_n), \qquad N_{(r,c)}(s) = N_{(c,r)}(s).$$

Indeed, $G \mapsto \sigma \cdot G$ permutes K_i and $G_{r,c} = s$ if and only if $(\sigma \cdot G)_{\sigma r,\,\sigma c} = \sigma s$, which gives the first identity; and $G \mapsto G^{\mathrm{op}}$ permutes K_i with $(G^{\mathrm{op}})_{c,r} = G_{r,c}$, which gives the second. Hence, N is constant on the Γ-orbits of $[n]^3$.

Step 3: The orbits. The orbit of a triple (r, c, s) depends only on its equality pattern (which of r, c, s coincide): the diagonal S_n-action preserves the pattern and, for $n \ge 3$, is transitive within each pattern. The five set-partitions of the three slots are

$$\{r{=}c{=}s\}, \quad \{r{=}c \ne s\}, \quad \{r{=}s \ne c\}, \quad \{c{=}s \ne r\}, \quad \{r, c, s \text{ distinct}\}.$$

The generator op swaps the first two slots, so it fixes the patterns $\{r{=}c{=}s\}$, $\{r{=}c \ne s\}$ and $\{r, c, s \text{ distinct}\}$, and interchanges $\{r{=}s \ne c\}$ with $\{c{=}s \ne r\}$. Hence, Γ has exactly four orbits on $[n]^3$:

$$A:\ r = c = s, \qquad B:\ r = c \ne s, \qquad C:\ r \ne c,\ s \in \{r, c\}, \quad D:\ r, c, s \text{ distinct}.$$

Let x, b, p, y denote the (constant) value of N on A, B, C, D, respectively.

Step 4: Two column-sum identities. Each groupoid places exactly one symbol in a given cell, so for every cell (r, c),

$$\sum_{s\in[n]} N_{(r,c)}(s) = m.$$

At a diagonal cell ($r = c$) the symbol $s = r$ lies in A and the other $n-1$ symbols lie in B, giving $x + (n-1)\,b = m$. At an off-diagonal cell ($r \neq c$) the symbols $s = r$ and $s = c$ lie in C and the remaining $n-2$ symbols lie in D, giving $2p + (n-2)\,y = m$. Therefore

$$b = \frac{m-x}{n-1}, \qquad p = \frac{m-(n-2)\,y}{2}.$$

Substituting these into the orbit description from Step 3 yields the stated formula. □

4. Conclusions

As we mentioned above, this issue has not been the subject of much research. However, we believe this topic has greater, yet undiscovered potential, especially in the field of quantum computers. Algorithms for creating groupoids with specific desired properties will be necessary and useful in the design and cryptanalysis of post-quantum encryption algorithms and also in other areas of algebra and computer science. Although the number of possible locations for parentheses increases with n, there are at most n possible outcomes only. Therefore, further research on this connection is necessary.

In our work, at the end of Section 2, we designed an algorithm that outputs a groupoid with the required number of elements n of the alphabet M and non-associative triples k. We based this algorithm on the theoretical results in the work [2]. As mentioned above, the output may be randomized.

In Section 3, we investigated the probability distribution of the occurrence of groupoid elements at individual positions. We present a proof that for a fixed range of the alphabet n and a fixed index of associativity i in the corresponding class K_i with i associative triples, the following holds: Let $|K_i| = m$. Then there exist numbers x, y such that at a given position of the Cayley table, the frequencies of occurrence of characters in the table are fixed for the selected i.

Finally, we presented the list of groupoids required to run Algorithm 1. The groupoids for $n = 3$ are taken from the paper of Climescu [2]. The other coincide with our new hypothesis.

Hypothesis 4.1. *Let $n \geq 4$ and let k be an integer. Let G_k, $k = 0, 1, \ldots, n^3$, be the set of groupoids on $[n]$ with exactly k non-associative triples, and put G_0 the groupoid (semilatice) with binary operation defined as $f_0(x, y) = \min\{x, y\}$. Then there exists a sequence of groupoids $G_0, G_1, \ldots, G_k, \ldots, G_{n^3}$ with binary operations $*_{k+1}$*

$$f_{k+1}(x, y) = x *_{k+1} y = \begin{cases} f_k(x, y), & \text{if } (x, y) \neq (r, c); \\ s, & s \in [n] \text{ otherwise}; \end{cases} \tag{1}$$

such that the number of non-associative triples in G_{k+1} is exactly $k + 1$.

In other words, by changing the product of a single suitably chosen pair of elements (r, c), we obtain from the groupoid G_k a groupoid with $k + 1$ non-associative triples. We were able to find such sequences up to $n = 9$. Partial examples of such sequences for $n = 4, 5$ are included in the Amendment below. Moreover, we can describe all operations f_1 and f_2 in this case.

Acknowledgment. The authors would like to express sincere gratitude to the anonymous referee for his insightful comments and suggestions that greatly contributed to improving the quality of this article.

5. Amendment: The list of used groupoids

The list contains several entries consisting of only the element $'a'$. These are the indices of groupoids $65 - 95$, which can be calculated from the previous groupoids by using one of the lemmas. These entries are not impacting the resulting groupoid. They are included only to accommodate the indices of other groupoids following them. These entries can be replaced with an arbitrary groupoid, provided the indexing of other entries is preserved, or the algorithm is adjusted, and provided they are not deleted. Moreover, groupoids $0 - 27$ are taken from the original work [2]. The other groupoids $28 - 125$ satisfy the hypothesis, i.e., the next groupoid differs from the previous one by one cell. Groupoids for $27 \leq k \leq 96$ are redundant as they can be calculated using Lemmas 2.1, 2.2, and 2.3 (see Algorithm 1).

```
bases_below64 = [
    [['a', 'b', 'c'], ['c', 'b', 'c'], ['c', 'b', 'c']],
    [['a', 'a', 'a'], ['a', 'a', 'a'], ['a', 'b', 'a']],
    [['a', 'a', 'a'], ['a', 'a', 'b'], ['a', 'b', 'b']],
    [['a', 'a', 'a'], ['b', 'b', 'b'], ['c', 'c', 'a']],
    [['a', 'a', 'a'], ['a', 'a', 'c'], ['a', 'b', 'a']],
    [['a', 'b', 'a'], ['b', 'a', 'a'], ['a', 'b', 'a']],
    [['a', 'a', 'b'], ['b', 'b', 'c'], ['c', 'c', 'a']],
    [['a', 'a', 'b'], ['a', 'a', 'b'], ['a', 'b', 'b']],
    [['a', 'a', 'a'], ['a', 'a', 'b'], ['a', 'b', 'a']],
    [['a', 'a', 'a'], ['c', 'b', 'b'], ['b', 'a', 'c']],
    [['b', 'b', 'a'], ['a', 'b', 'a'], ['a', 'a', 'c']],
    [['b', 'b', 'a'], ['a', 'a', 'b'], ['a', 'a', 'a']],
    [['b', 'b', 'b'], ['a', 'a', 'b'], ['c', 'c', 'a']],
    [['b', 'b', 'b'], ['a', 'b', 'a'], ['a', 'a', 'a']],
    [['c', 'b', 'a'], ['a', 'b', 'b'], ['b', 'b', 'c']],
    [['b', 'b', 'b'], ['a', 'a', 'b'], ['a', 'a', 'c']],
    [['b', 'b', 'a'], ['a', 'a', 'a'], ['c', 'c', 'a']],
    [['b', 'b', 'a'], ['a', 'a', 'b'], ['c', 'c', 'a']],
    [['b', 'b', 'a'], ['a', 'a', 'a'], ['c', 'c', 'a']],
    [['b', 'b', 'a'], ['b', 'a', 'a'], ['c', 'c', 'a']],
    [['b', 'b', 'a'], ['b', 'c', 'a'], ['b', 'c', 'b']],
    [['b', 'b', 'a'], ['b', 'c', 'a'], ['b', 'c', 'b']],
    [['b', 'c', 'a'], ['b', 'c', 'a'], ['b', 'c', 'b']],
    [['b', 'a', 'a'], ['b', 'a', 'c'], ['b', 'a', 'a']],
    [['b', 'c', 'b'], ['a', 'a', 'a'], ['c', 'b', 'a']],
    [['b', 'c', 'a'], ['b', 'c', 'a'], ['b', 'c', 'a']],
    [['b', 'b', 'c', 'a'], ['c', 'd', 'd', 'a'], ['a', 'a', 'd', 'c'], ['a', 'b', 'c', 'd']],
    [['b', 'b', 'd', 'a'], ['c', 'd', 'd', 'a'], ['a', 'a', 'd', 'c'], ['a', 'b', 'c', 'd']],
    [['b', 'b', 'd', 'a'], ['c', 'd', 'd', 'a'], ['b', 'a', 'd', 'c'], ['a', 'b', 'c', 'd']],
    [['b', 'b', 'd', 'd'], ['c', 'd', 'd', 'a'], ['b', 'a', 'd', 'c'], ['a', 'b', 'c', 'd']],
```

```
[['b', 'a', 'd', 'd'], ['c', 'd', 'd', 'a'], ['b', 'a', 'd', 'c'], ['a', 'b', 'c', 'd'],
 ['b', 'a', 'd', 'd'], ['c', 'd', 'd', 'a'], ['a', 'a', 'd', 'c'], ['a', 'b', 'c', 'd'],
 ['b', 'a', 'd', 'd'], ['c', 'd', 'd', 'a'], ['c', 'a', 'd', 'c'], ['a', 'b', 'c', 'd'],
 ['b', 'a', 'd', 'b'], ['c', 'd', 'd', 'a'], ['c', 'a', 'd', 'c'], ['a', 'b', 'c', 'd'],
 ['c', 'a', 'd', 'b'], ['c', 'd', 'd', 'a'], ['c', 'a', 'd', 'c'], ['a', 'b', 'c', 'd'],
 ['c', 'a', 'd', 'b'], ['b', 'd', 'd', 'a'], ['c', 'a', 'd', 'c'], ['a', 'b', 'c', 'd'],
 ['c', 'a', 'd', 'b'], ['b', 'd', 'd', 'a'], ['c', 'a', 'a', 'c'], ['a', 'b', 'c', 'd'],
 ['d', 'a', 'd', 'b'], ['b', 'd', 'b', 'a'], ['c', 'a', 'a', 'c'], ['a', 'b', 'c', 'd'],
 ['d', 'a', 'd', 'b'], ['b', 'd', 'b', 'a'], ['c', 'a', 'a', 'a'], ['a', 'b', 'c', 'd'],
 ['d', 'a', 'd', 'b'], ['b', 'd', 'b', 'a'], ['c', 'd', 'a', 'a'], ['a', 'c', 'c', 'd'],
 ['d', 'c', 'a', 'b'], ['b', 'd', 'b', 'a'], ['c', 'd', 'a', 'a'], ['a', 'c', 'c', 'd'],
 ['d', 'c', 'a', 'b'], ['b', 'd', 'b', 'a'], ['b', 'd', 'a', 'a'], ['a', 'c', 'c', 'd'],
 ['d', 'c', 'd', 'b'], ['b', 'c', 'b', 'a'], ['b', 'd', 'a', 'a'], ['a', 'c', 'c', 'd'],
 ['d', 'c', 'd', 'b'], ['b', 'c', 'b', 'a'], ['b', 'd', 'a', 'a'], ['a', 'c', 'c', 'd'],
 ['d', 'c', 'd', 'b'], ['b', 'c', 'b', 'a'], ['b', 'd', 'a', 'a'], ['a', 'c', 'c', 'd'],
 ['d', 'c', 'c', 'b'], ['b', 'c', 'b', 'a'], ['b', 'd', 'a', 'a'], ['a', 'c', 'd', 'd'],
 ['d', 'c', 'c', 'b'], ['b', 'c', 'b', 'a'], ['b', 'd', 'a', 'a'], ['a', 'c', 'd', 'd'],
 ['d', 'c', 'c', 'b'], ['b', 'c', 'c', 'a'], ['b', 'd', 'a', 'a'], ['a', 'c', 'd', 'd'],
 ['d', 'c', 'b', 'b'], ['b', 'c', 'c', 'a'], ['b', 'd', 'b', 'a'], ['a', 'c', 'd', 'd'],
 ['d', 'c', 'b', 'b'], ['b', 'c', 'd', 'a'], ['b', 'd', 'b', 'a'], ['a', 'c', 'd', 'd'],
 ['d', 'c', 'b', 'b'], ['b', 'c', 'd', 'a'], ['b', 'd', 'b', 'a'], ['b', 'c', 'd', 'd'],
 ['d', 'c', 'b', 'b'], ['b', 'a', 'd', 'a'], ['b', 'd', 'b', 'a'], ['b', 'c', 'd', 'd'],
 ['d', 'a', 'b', 'c'], ['b', 'a', 'd', 'a'], ['b', 'd', 'b', 'a'], ['b', 'c', 'd', 'd'],
 ['b', 'a', 'b', 'c'], ['b', 'a', 'd', 'a'], ['b', 'd', 'b', 'a'], ['b', 'c', 'b', 'd'],
 ['b', 'a', 'b', 'c'], ['b', 'a', 'b', 'a'], ['b', 'd', 'b', 'a'], ['b', 'c', 'b', 'd'],
 ['b', 'a', 'b', 'c'], ['b', 'c', 'b', 'a'], ['b', 'a', 'b', 'a'], ['b', 'c', 'b', 'a']]
```

```
bases_above96 = [
    [['c', 'b', 'd', 'a', 'd'], ['c', 'c', 'c', 'c', 'a'], ['e', 'd', 'd', 'd', 'e'],
     ['e', 'e', 'e', 'b', 'a'], ['b', 'b', 'c', 'd', 'e']],
    [['b', 'b', 'd', 'a', 'd'], ['c', 'c', 'c', 'c', 'a'], ['e', 'd', 'd', 'd', 'e'],
     ['e', 'e', 'e', 'b', 'a'], ['b', 'b', 'c', 'd', 'e']],
    [['b', 'b', 'b', 'a', 'd'], ['c', 'c', 'c', 'c', 'a'], ['e', 'd', 'd', 'd', 'e'],
     ['e', 'e', 'e', 'b', 'a'], ['b', 'b', 'c', 'd', 'e']],
    [['b', 'b', 'e', 'b', 'a'], ['b', 'b', 'c', 'c', 'a'], ['e', 'd', 'd', 'd', 'e'],
     ['e', 'e', 'e', 'b', 'a'], ['b', 'b', 'c', 'd', 'e']],
    [['b', 'b', 'e', 'b', 'a'], ['b', 'c', 'c', 'd', 'e'], ['e', 'd', 'd', 'd', 'e'],
     ['e', 'e', 'e', 'b', 'a'], ['b', 'b', 'c', 'd', 'e']],
    [['b', 'b', 'e', 'e', 'd'], ['c', 'c', 'c', 'a', 'a'], ['e', 'd', 'a', 'd', 'e'],
     ['e', 'e', 'e', 'b', 'a'], ['b', 'b', 'c', 'd', 'e']],
    [['b', 'b', 'e', 'e', 'd'], ['c', 'c', 'c', 'a', 'a'], ['e', 'a', 'a', 'd', 'e'],
     ['e', 'e', 'e', 'b', 'a'], ['b', 'b', 'c', 'd', 'e']],
    [['b', 'b', 'e', 'e', 'd'], ['c', 'c', 'c', 'a', 'a'], ['e', 'a', 'a', 'e', 'e'],
     ['e', 'e', 'e', 'b', 'a'], ['b', 'b', 'c', 'd', 'e']],
    [['b', 'b', 'e', 'e', 'd'], ['c', 'c', 'c', 'a', 'a'], ['e', 'a', 'a', 'e', 'e'],
     ['e', 'e', 'e', 'b', 'a'], ['b', 'b', 'c', 'd', 'e']],
    [['b', 'b', 'b', 'c', 'd'], ['c', 'c', 'c', 'a', 'a'], ['e', 'a', 'a', 'e', 'd'],
     ['e', 'e', 'e', 'b', 'a'], ['b', 'b', 'c', 'd', 'e']],
    [['b', 'b', 'b', 'c', 'd'], ['c', 'c', 'c', 'a', 'a'], ['e', 'a', 'a', 'd
```

```
[['b', 'b', 'b', 'b', 'd'], ['c', 'c', 'c', 'a', 'a'], ['a', 'a', 'a', 'a', 'd'],
 ['a', 'e', 'e', 'a', 'a'], ['b', 'b', 'c', 'd', 'e']],
 [['b', 'b', 'b', 'b', 'd'], ['c', 'c', 'c', 'a', 'a'], ['a', 'a', 'a', 'a', 'e'],
 ['a', 'e', 'e', 'a', 'a'], ['b', 'b', 'c', 'd', 'e']],
 [['b', 'b', 'b', 'b', 'd'], ['c', 'c', 'c', 'a', 'a'], ['a', 'a', 'a', 'a', 'a'],
 ['a', 'e', 'e', 'a', 'a'], ['b', 'b', 'c', 'd', 'e']],
 [['b', 'b', 'b', 'b', 'b'], ['c', 'c', 'c', 'a', 'a'], ['a', 'a', 'a', 'a', 'a'],
 ['a', 'e', 'e', 'a', 'a'], ['b', 'b', 'c', 'd', 'e']],
 [['b', 'b', 'b', 'b', 'b'], ['c', 'c', 'c', 'a', 'a'], ['a', 'a', 'a', 'a', 'a'],
 ['a', 'a', 'e', 'a', 'a'], ['b', 'b', 'c', 'd', 'e']],
 [['b', 'b', 'b', 'b', 'b'], ['c', 'c', 'c', 'a', 'a'], ['a', 'a', 'a', 'a', 'a'],
 ['a', 'a', 'a', 'a', 'a'], ['b', 'b', 'c', 'd', 'e']],
 [['b', 'b', 'b', 'b', 'b'], ['c', 'c', 'c', 'a', 'a'], ['a', 'a', 'a', 'a', 'a'],
 ['a', 'a', 'a', 'b', 'b'], ['c', 'c', 'c', 'a', 'a'], ['a', 'a', 'a', 'a', 'a'],
 [['b', 'b', 'b', 'b', 'b'], ['c', 'c', 'c', 'a', 'a'], ['a', 'a', 'a', 'a', 'a'],
 ['a', 'a', 'a', 'a', 'a'], ['b', 'b', 'c', 'd', 'e']],
 [['b', 'b', 'b', 'b', 'b'], ['c', 'c', 'c', 'a', 'a'], ['a', 'a', 'a', 'a', 'a'],
 ['a', 'a', 'a', 'a', 'a'], ['b', 'a', 'c', 'd', 'e']],
 [['b', 'b', 'b', 'b', 'b'], ['c', 'c', 'c', 'a', 'a'], ['a', 'a', 'a', 'a', 'a'],
 ['a', 'a', 'a', 'a', 'a'], ['b', 'a', 'c', 'd', 'e']],
 [['b', 'b', 'b', 'b', 'b'], ['c', 'c', 'c', 'a', 'a'], ['a', 'a', 'a', 'a', 'a'],
 ['a', 'a', 'a', 'a', 'a'], ['b', 'a', 'c', 'd', 'e']],
 [['b', 'b', 'b', 'b', 'b'], ['c', 'c', 'c', 'a', 'a'], ['a', 'a', 'a', 'a', 'a'],
 ['a', 'a', 'a', 'a', 'a'], ['b', 'a', 'c', 'd', 'a']],
 [['b', 'b', 'b', 'b', 'b'], ['c', 'c', 'c', 'a', 'a'], ['a', 'a', 'a', 'a', 'a'],
 ['a', 'a', 'a', 'a', 'a'], ['b', 'd', 'c', 'd', 'a']],
 [['b', 'b', 'b', 'b', 'd'], ['c', 'c', 'c', 'a', 'a'], ['a', 'a', 'a', 'a', 'a'],
 ['a', 'a', 'a', 'a', 'a'], ['b', 'd', 'c', 'c', 'a']],
 [['b', 'b', 'b', 'b', 'd'], ['c', 'c', 'c', 'c', 'c'], ['a', 'a', 'a', 'a', 'a']]
]
```

TABLE 4. Table for groupoids of order $n = 4$, and elements $\{a, b, c, d\}$, with number of associative triples $i \in \{0, 1, \ldots, n^3\}$.

i	m	x	y	i	m	x	y
0	421560	0	69657	33	77027640	32126424	23210136
1	146808	3456	22942	34	66761976	28712172	20435526
2	489744	8286	81820	35	56488608	25037892	17589156
3	1189368	18024	205178	36	48365502	22003758	15288279
4	2558184	48306	448846	37	40366712	18889454	12974558
5	4863240	120132	864268	38	33793812	16203573	11020947
6	8942184	283014	1610586	39	27524400	13541448	9129620
7	15168288	602496	2776828	40	22797008	11473241	7666388
8	24897384	1187760	4637246	41	18044496	9342552	6168228
9	38478504	2176200	7295604	42	14628492	7728501	5068190
10	56840712	3709680	10989090	43	11340928	6142462	3997204
11	78919272	5866284	15586740	44	9132648	5032470	3256732
12	104844996	8825238	21142696	45	6802992	3838962	2467610
13	131872696	12590152	27163442	46	5431400	3114329	1993091
14	158798160	17189376	33386636	47	3958080	2316006	1472874
15	182391504	22358034	39159264	48	3116268	1850925	1170462
16	202423572	28096002	44347788	49	2192560	1334032	836442
17	216203472	33749244	48348828	50	1677600	1031868	645616
18	225548796	39373584	51470644	51	1127112	711768	440736
19	229256648	44369048	53386386	52	854596	543622	335765
20	229329042	48712458	54490238	53	538128	350172	216362
21	224832024	51983466	54515218	54	413460	270405	166349
22	217809764	54371330	53860376	55	244400	161606	99808
23	207757608	55601424	52385888	56	194622	128133	79092
24	196501890	55956624	50509916	57	103368	68910	42668
25	182950224	55176924	47935448	58	81744	54126	33268
26	169950264	53962077	45356150	59	40032	26760	16564
27	155223552	51714372	42204344	60	35244	23118	14294
28	141674700	49302108	39211086	61	12928	8644	5140
29	127306032	46101300	35869554	62	9600	6522	3892
30	114371796	43011837	32764795	63	2976	1992	1160
31	100806200	39292760	29394714	64	3492	2331	1348
32	89086284	35902650	26402103				

REFERENCES

[1] CLIFFORD, A. H.—PRESTON, G. B.: *The Algebraic Theory of Semigroups*, Vol. I, Mathematical Surveys 7, AMS, 1961.

[2] CLIMESCU, A. C.: *Études sur la théorie des systémes multiplicatifs uniformes I. L'indice de non-associativité*, Bull. École Polytech. Jassy **2** (1947), 347–371.

[3] DRÁPAL, A.—LISONĚK, P.: *Maximal nonassociativity via nearfields*, Finite Fields Appl. **62** (2020), Art. 101610.

[4] DRÁPAL, A.—KEPKA, T.: *Sets of Associative Triples* Eur. J. Comb. **6** (1985), 227–231.

[5] GROŠEK, O.—HORÁK, P.: *On quasigroups with few associative triples*, Des. Codes Cryptogr. **64** (2012), 221–227.

[6] HECHT, P.: *PQC: R-Propping of Public-Key Cryptosystems Using Polynomials over Non-commutative Algebraic Extension Rings*, Cryptology ePrint Archive, Paper 2020/1102 (2020).

[7] HECHT, P.: *Post-Quantum Cryptography(PQC): Generalized ElGamal Cipher over GL(8,F251)*, CoRR **abs/1702.03587** (2017).

[8] KALKA, A. G.: *Non-associative public-key cryptography*, CoRR (2012); `https://arxiv.org/abs/1210.8270v1`.

[9] KATYSHEV, S. Y.—ZYAZIN, A. V.—BARYSHNIKOV, A. V.: *Application of non-associative structures for construction of homomorphic cryptosystems*, Math. Issues Cryptogr. (In Russian: Mat. Vopr. Kriptografii) **11** (2020), 31–39.

[10] MARKOV, V. T.—MYKHALEV, A. V.—KYSLITSYN, E. S.: *Non-associative structures in homomorphic encryption*, J. Math. Sci. **262** (2022), 735–739.

[11] NAZLI, S.—ALI, A.—SHAH, T.—GHAZANFAR, F.: *Non-associative algebra redesigning block cipher with color image encryption*, Comput. Mater. Contin. **11** (2020), 31–39.

[12] STANLEY, R. P.: *Catalan Numbers*, Cambridge University Press, 2015.

Received August 28, 2025
Revised June 18, 2026
Accepted September 1, 2026
Publ. online November 30, 2026

Otokar Grošek
Mathematical Institute
Slovak Academy of Sciences
Štefánikova 49
814 73 Bratislava
SLOVAKIA

Department of Informatics and Mathematics
Faculty of Electrical Engineering
Slovak Technical University
Ilkovičova 3
841 04 Bratislava
SLOVAKIA
E-mail: otokar.grosek@stuba.sk

Marián Kňazovický
Department of Informatics and Mathematics
Faculty of Electrical Engineering
Slovak Technical University
Ilkovičova 3
841 04 Bratislava
SLOVAKIA
E-mail: marianknazo@gmail.com