Séminaire Lotharingien de Combinatoire **80** (2019), Article B80c

LAVER TABLES AND COMBINATORICS

PHILIPPE BIANE

ABSTRACT. The Laver tables are finite combinatorial objects with a simple elementary definition, which were introduced by R. Laver in [*Adv. Math.* **91** (1992), 209–231] from considerations of logic and set theory. Although these objects exhibit some fascinating properties, they seem to have escaped notice from the combinatorics community. My aim is to give a short introduction to this topic, presenting the definition and main properties and stating a few open problems, which should arouse the interest of combinatorialists.

CONTENTS

Key words and phrases. Laver tables.

1. Introduction

In the 1990's the logician R. Laver [11, 12], motivated by questions in the theory of large cardinals, introduced the so-called Laver tables, which are the subject of this paper. In short, a Laver table is a finite set endowed with a binary operation $\star$, which is left distributive, meaning that $p \star (q \star r) = (p \star q) \star (p \star r)$ holds for all p, q, r, and in which one of the elements acts, by right multiplication, as a cyclic permutation of the elements of the set. The formal definition is given in Section 2 below. Laver established the existence and uniqueness of such a structure for sets of cardinality 2^n, for some integer n. Moreover he discovered many of their interesting combinatorial properties. Some further work was done at that time, mainly by logicians and algebraists, notably by Dehornoy, Dougherty, Drápal, Jech, however it seems that this subject has been largely ignored by combinatorialists despite the fact that the Laver tables have a strong and highly non-trivial combinatorial content. In this paper I will present some of the most basic properties of Laver tables, from a combinatorial perspective, but I will also try to give some indications on the notions of set theory which lead to their discovery. I hope that this paper might encourage combinatorialists to look deeper into this beautiful subject. As I mentioned above, the Laver tables carry a left distributive operation. The study of such operations is not part of the mainstream of algebraic combinatorics, rather it comes from two other sources, set theory and the theory of braids. A lot of information about these subjects may be found in Dehornoy's book [1] or his recent preprint [3]. The difficulty in studying left distributive structures comes from the fact that the left distributive identity $p \star (q \star r) = (p \star q) \star (p \star r)$ does not have the same number of terms on each side. This implies that computing with operations satisfying this identity leads to deep recursions. On the other hand, experimental study of the Laver tables, which can be made, up to rather large size, using computers, shows that these tables seem both to satisfy many regularity properties and yet to escape any global description. In particular some basic questions have surprising answers: Laver has proved, using a large cardinal axiom, which is not provable in usual ZFC theory, that the projective limit of the Laver tables is a free system. As we shall see below, this statement has a very concrete translation into properties of the Laver tables: it asserts that a certain sequence, with an elementary combinatorial definition, is unbounded. However, up to now no proof is known of this fact which does not use this large cardinal axiom. It is a challenge for combinatorialists to find an elementary proof of this fact (or to disprove it ...). This situation bears some resemblance with the study of the iteration of rational maps on the complex plane in complex dynamics, which gives rise to Julia sets or the Mandelbrot set (see e.g. [14]): these objects are also constructed by very simple recursive laws, they exhibit some regularity and beautiful features, which can be seen on the computer generated pictures that are easily found on the internet, yet their structure is very complicated and many questions concerning them are still open. I hope that Laver tables might attract similar attention from the combinatorialists which would lead to much progress.

This paper is organized as follows: in the next section we give the definition of Laver tables and make some general comments on left distributive operations. In Section 3 we give some basic properties of Laver tables, then, in Section 4, we explain how these objects were discovered by Laver, starting from considerations of set theory. We continue with some further properties of Laver tables in Sections 5 and 6. We explain in Section 7 why these are interesting and subtle combinatorial objects. In particular we state some difficult open problems. In Section 8, we show that the periods of Laver tables have asymptotic frequencies, which define a probability measure on $\mathbf{N}\cup\{\infty\}$. It would be interesting to describe more precisely this probability distribution. Finally, in Section 9, we introduce a particular class of elements of the Laver tables. These are, in some sense, the simplest elements, and a remarkable property of these elements is that they form a subset which is stable under the operation of the Laver table. Moreover they are parameterized by binary partitions, which are objects related to more mainstream algebraic combinatorics. Most of the results of this paper are not new, except perhaps the contents of Sections 8 and 9, and can be found in the papers cited in the bibliography, although sometimes in slightly different form, so that I did not try to track down the exact reference for each of them.

I would like to thank Patrick Dehornoy for introducing me to this beautiful subject, as well as Ales Drápal for communicating me his preprint [10]. Both of them made useful remarks on a first version of this paper.

2. What are Laver tables?

2.1. **A binary operation.** Let N be a positive integer, there exists a unique binary operation $\star$ on the set $\{1,2,\dots,N\}$ such that, for all p,q, with $q<N$[1]

$$p\star 1 = p+1 \mod (N) \tag{2.1}$$

$$p\star(q\star 1) = (p\star q)\star(p\star 1) \tag{2.2}$$

Indeed property (2.1) implies

$$N\star 1 = 1.$$

Using (2.2) we get

$$N\star 2 = N\star(1\star 1) = (N\star 1)\star(N\star 1) = 1\star 1 = 2.$$

By induction on q we have

$$N\star q = N\star((q-1)\star 1) = (N\star(q-1))\star(N\star 1) = (q-1)\star 1 = q.$$

Starting from $(N-1)\star 1 = N$ and the relation

$$p\star(q+1) = p\star(q\star 1) = (p\star q)\star(p+1) \tag{2.3}$$

we can use induction, descending on p and ascending on q, to prove that $p\star q$ is well defined and satisfies $N\geq p\star q>p$.

[1] In Dehornoy's book [1] it is stated that (2.2) holds for all p,q however if N is not a power of 2 this is not true. I would like to thank Arkadiusz Lewandowski for pointing this out to me.

2.2. **The Laver tables.** It turns out that the binary operation $\star$, defined above, is left distributive if and only if $N = 2^n$ for some $n \geq 0$. Left distributivity is the property that, for all p, q, r we have

$$p \star (q \star r) = (p \star q) \star (p \star r). \tag{2.4}$$

Note that (2.4) is (2.2) with 1 replaced by any $r \in [1, N]$. The proof of this result is elementary, but non-trivial, and can be found for example in the books [1, 2] or in the survey by Drápal [9]. In the sequel I will denote by $\star_n$ the operation on $[1, 2^n]$ thus obtained. Here is the Laver table giving the values of $p \star_n q$, for $N = 4$:

$\star$	**1**	**2**	**3**	**4**
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

and for $N = 8$:

$\star$	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	2	4	6	8	2	4	6	8
2	3	4	7	8	3	4	7	8
3	4	8	4	8	4	8	4	8
4	5	6	7	8	5	6	7	8
5	6	8	6	8	6	8	6	8
6	7	8	7	8	7	8	7	8
7	8	8	8	8	8	8	8	8
8	1	2	3	4	5	6	7	8

The p's are in the first column and the q's in the first row.

2.3. **Left distributive operations.** Before going further into a combinatorial exploration of the Laver tables, I will make some general remarks on left distributive operations. A thorough study of these, with many examples and applications, notably to knots and braids, can be found in the monograph by Dehornoy [1]. A binary operation $\star : S \times S \to S$ on a set S is said to be *left distributive* if it satisfies (2.4) for all $p, q, r \in S$. A good way to think about property (2.4) is to notice that the left multiplication operator by some element s, denoted by λ_s i.e., $\lambda_s(t) = s \star t$, is a homomorphism of the structure: for all p, q, r we have

$$\lambda_p(q \star r) = \lambda_p(q) \star \lambda_p(r). \tag{2.5}$$

Thus λ gives a map $S \to \mathrm{Hom}(S, \star)$. However, in general, $\lambda_{p \star q}$ does not have an obvious relation to λ_p and λ_q, in particular it is not equal to $\lambda_p \circ \lambda_q$! A motivation for considering such a property comes from the study of the set of maps of a set to itself. Composition of maps gives a semigroup structure on this set. Identifying a function $f : X \to X$ with its graph $G_f = \{(x, f(x)), x \in X\}$, the graph of the composition $f \circ g$ is

$$(\mathrm{Id} \times f)(G_g) = \{(x, f(g(x))) : x \in X\}.$$

It is also possible to "apply" the function f to the graph G_g to produce the set

$$(f \times f)(G_g) = \{(f(x), f(g(x)) : x \in X\}.$$

In general this is not the graph of a function, unless f is a bijection, in which case it is the graph of the function $f \circ g \circ f^{-1}$. It turns out that the operation $f \star g = f \circ g \circ f^{-1}$ is left distributive in the following sense: if f and g are invertible then $f \star (g \star h) = (f \star g) \star (f \star h)$. Actually, a trivial computation shows that, in any group, the conjugation operation $f \star g = fgf^{-1}$ is left distributive. It is interesting however, for reasons which will appear later, to enlarge the previous example in the following way: for a set X let I_X be the set of partially defined injections $f : D_f \subset X \to X$, where D_f is the domain of definition of f, containing in particular "the injection with empty domain". The set I_X is a semigroup for the natural notion of composition (which may result in an injection with empty domain). Each such injection can be described by its graph $\{(x, f(x)) : x \in D_f\} \subset X \times X$. If $g \in I_X$ then $(g \times g)(G_f)$ is the graph of a partially defined injection $g \star f$ and again it is easy to see that the operation $\star$ is left distributive and that $\lambda_f \lambda_g = \lambda_{f \circ g}$, where $f \circ g$ denotes the composition of partially defined injections. Observe that we have

$$(f \star g)(f(x)) = f(g(x)) \tag{2.6}$$

whenever the two members of this equality are defined. This serves as a substitute for the formula $f \star g = f \circ g \circ f^{-1}$. At this stage, a natural question is whether one can find a family I (not reduced to the identity) of *increasing, everywhere defined* injections of $\mathbf{N}$ into itself, endowed with a binary left distributive operation $\star : I \times I \to I$, such that, for any $\iota, \eta \in I$ and $x \in \mathbf{N}$ we have $\iota \star \eta(\iota(x)) = \iota(\eta(x))$, as in (2.6). It turns out that this is a highly non-trivial question to which, as we shall see in Section 7, the Laver tables give a surprising answer.

3. Basic properties of the Laver tables

We now come back to the Laver tables constructed in Section 2 and describe some of their elementary properties.

3.1. Periods and projective limits. The following properties of the operation $\star_n$ are easily established by induction, see e.g. [1] (as above we put $N = 2^n$).

- For all $p \in [1, N]$ we have $N \star_n p = p$ and $p \star_n N = N$.
- For every $p \in [1, N]$ the sequence $p \star_n q$, $q = 1, 2, \ldots$, is periodic, with period $\pi_n(p)$, a power of 2, and the sequence $p \star_n q$, $q = 1, 2, \ldots, \pi(p)$, is strictly increasing from $p \star_n 1 = p + 1$ to $p \star_n \pi(p) = N$.
- The projection $\Pi_N : [1, 2N] \to [1, N]$ modulo N is a homomorphism.
- For all p, q we have

$$p \star_n q = (p + 1)^{(q)}, \tag{3.1}$$

where the *left powers*[2] $x^{(k)}$ are defined by $x^{(1)} = x$, $x^{(k+1)} = x^{(k)} \star_n x$. This follows at once from (2.3).

In order to illustrate these properties let us display again the Laver table of size 8. In the last column we show the period of each row and we divide the table into four squares. It is immediate to check that each of these squares is equal, modulo 4, to the table of order 4.

$\star$	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	π
1	2	4	6	8	2	4	6	8	4
2	3	4	7	8	3	4	7	8	4
3	4	8	4	8	4	8	4	8	2
4	5	6	7	8	5	6	7	8	4
5	6	8	6	8	6	8	6	8	2
6	7	8	7	8	7	8	7	8	2
7	8	8	8	8	8	8	8	8	1
8	1	2	3	4	5	6	7	8	8

It is possible to take a projective limit of the Laver tables with respect to the natural projections $\Pi_{n,m} : [1, 2^n] \to [1, 2^m],\ n > m$ and obtain a left distributive operation on the set of 2-adic integers. This left distributive system is generated by 1.

3.2. **Generators and relations.** Consider the free system with one generator for the left distributive operation (2.4), namely, denoting the generator by 1, it consists of all well parenthesized expressions in $1, \star$, like $1, 1\star 1, (1\star 1)\star 1, 1\star(1\star 1)$, etc. equipped with the operation $\star$, modulo the congruence induced by the relation (2.4). The Laver table of order 2^n, as a left distributive system with one generator, satisfies supplementary relations, for example we have

$$1^{(2^n+1)} = 1. \tag{3.2}$$

In fact one can show that the Laver table of order 2^n is exactly the left distributive system with one generator 1 and the relation (3.2), see e.g. [1, 16]. A very deep question is whether the projective limit of Laver tables is a free system. We will say more about this in Section 7.

3.3. **Homomorphisms and semigroup structure.** As we have remarked, for any p the left multiplication by p is a homomorphism for the operation $\star_n$. More generally, if $p \in [1, 2^n]$ has period $\pi_n(p) \leq 2^m$ then the map $q \mapsto p \star_n q$ is a homomorphism from $[1, 2^m]$ to $[1, 2^n]$ (with respect to their respective operations $\star_m, \star_n$). Conversely, for any homomorphism $\varphi : [1, 2^m] \to [1, 2^n]$ we have, using (3.1),

$$\varphi(q) = \varphi(1^{(q)}) = (\varphi(1))^{(q)} = p \star_n q$$

with $p = \varphi(1) - 1 \mod 2^n$ so that φ is given by left multiplication by p. Since composition of homomorphisms is a homomorphism, for any $p, q \in [1, N]$, there exists a unique

[2] One can similarly define right powers but we will not use them.

s, denoted $p \circ_n q$, such that $\lambda_s = \lambda_p \circ \lambda_q$ or, equivalently,

$$p \star_n (q \star_n r) = s \star_n r \quad \text{for all } r. \tag{3.3}$$

Using Equation (3.3) for $r = 1$ we see that $p \circ_n q$ is characterized by the relation

$$(p \circ_n q) + 1 = p \star_n (q + 1) \mod N \tag{3.4}$$

which relates $\star_n$ and $\circ_n$. The product $\circ_n$ is associative and gives a semigroup structure on $[1, N]$. In fact the map λ gives an isomorphism $([1, N], \circ_n) \sim \mathrm{End}([1, N], \star_n)$. One can check that $\star_n$ and $\circ_n$ satisfy the properties

$$p \star_n (q \circ_n r) = (p \star_n q) \circ_n (p \star_n r) \tag{3.5}$$

$$(p \circ_n q) \star_n r = p \star_n (q \star_n r) \tag{3.6}$$

$$(p \star_n q) \circ_n p = p \circ_n q. \tag{3.7}$$

These relations might seem less strange if one observes that they are also satisfied by any pair $\circ, \star$, where $\circ$ is a group operation and $\star$ the associated conjugation operation, $a \star b = a \circ b \circ a^{-1}$, as in Section 2.3.

3.4. **Backwards notation.** We have seen that the natural projection

$$\Pi_N : [1, 2N] \to [1, N]$$

is a homomorphism. The embedding:

$$\iota_N : ([1, N], \star_n) \to ([1, 2N], \star_{n+1})$$
$$p \mapsto p + N = N \star_{n+1} p$$

is also a homomorphism. This implies that, for nonnegative integers p, q, the value of

$$p * q := N - (N - p) \star_n (N - q) \tag{3.8}$$

does not depend on N, as long as $p, q < N = 2^n$. One can therefore take an inductive limit with respect to the embeddings ι_N and build an infinite table giving the values of $p * q$ for nonnegative integers p and q. The set of nonnegative integers is thus endowed with a left distributive operation $*$. The properties of $\star_n$ immediately translate into the following properties of $*$:

- $0 * p = p$ and $p * 0 = 0$ for all $p \geq 0$.
- For every $p > 0$ the sequence $p * q$, $q = 0, 1, 2 \ldots$, is periodic, with period $\pi(p)$, a power of 2.
- $p * q$, $q = 0, 1, 2, \ldots, \pi(p) - 1$, is strictly increasing and $p * (\pi(p) - 1) = p - 1$.
- For all p, q, r, n, we have

$$p * (q * r) = (p * q) * (p * r) \tag{3.9}$$

$$(p \mod 2^n) * (q \mod 2^n) = p * q \mod 2^n \tag{3.10}$$

- The formula $p \circ q = p * (q - 1) + 1$ defines a semigroup structure on the set of positive integers.
- We have

$$p * (2^n - q) = (p - 1)^{(q)} \qquad \text{for } 2^n \geq \pi(p) \tag{3.11}$$

  (where the left powers $(p - 1)^{(q)}$ for $*$ have a definition analogous to that for $\star$ below (3.1)).

Equations (3.5)–(3.7) also hold for $*$ and $\circ$. It follows in particular that for every m the interval $[0, m]$ is closed under $*$ and $[1, m]$ is closed under $\circ$. Since the operations $\star_n$ and $*$ are related by the map $p \mapsto N - p$ they are equivalent but, depending on the aspects of Laver tables one wants to consider, often one of them turns out to be more convenient than the other.

3.5. **Computation of the Laver table.** We saw in Section 2 how to compute the products $p \star_n q$ by induction. For the convenience of the reader I will illustrate here the computation of the operation $*$, which gives the inductive structure and which, of course, is equivalent to the computation of the operations $\star_n$. The Laver table recording the $p * q$ can be constructed by induction on the rows. If one knows the rows from 0 to $p-1$, the row of p is obtained as follows: for n large enough (i.e., $2^n > p$) we have

$$p * (2^n - 1) = p - 1 \tag{3.12}$$

and

$$p*(2^n-2) = p*((2^n-1)*(2^n-1)) = (p*(2^n-1))*(p*(2^n-1)) = (p-1)*(p-1). \tag{3.13}$$

By induction on k, using $2^n - k - 1 = (2^n - k) * (2^n - 1)$ and (2.4):

$$p * (2^n - k - 1) = (p * (2^n - k)) * (p - 1). \tag{3.14}$$

By the periodicity properties of the Laver tables, we have $p * (2^n - 2^m) = 0$ for some $m < n$ so that the period of the sequence $p * q$, $q = 0, 1, 2, \ldots$, is 2^m. Once this value is reached, the row is completed by periodicity. As an example we compute the row of 7 assuming the rows from 0 to 6 have already been computed (all rows between 1 and 6 have period ≤ 4):

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
0	0	1	2	3	4	5	6	7	8
1	0	0	0	0	0	0	0	0	0
2	0	1	0	1	0	1	$\boxed{0}$	1	0
3	0	2	0	2	0	2	0	2	0
4	0	1	2	3	0	1	$\boxed{2}$	3	0
5	0	4	0	4	0	4	0	4	0
6	0	1	4	5	0	1	$\boxed{4}$	5	0
7	0	2	4	6	$\boxed{0}$	$\boxed{2}$	$\boxed{4}$	$\boxed{6}$	0

In order to get row 7 we take $n = 3$ so that $2^n - 1 = 7$ and by (3.12) we have $7 * 7 = 6$. Application of (3.13) gives $7 * 6 = 6 * 6 = 4$ and by repeatedly applying (3.14) we get $7 * 5 = 4 * 6 = 2$, $7 * 4 = 2 * 6 = 0$. The rest of the row follows by periodicity. The relevant values are shown in boxes in the above table.

It is easy to make a computer program which performs these computations for larger values of p and q, however one encounters quickly memory size problems. We will see in Section 5.2 how to encode the Laver tables in a more compact form. A simple formula expressing $p * q$ in terms of p and q is known for some classes of p's (for example if p is a power of 2, see Section 6 below) but no formula is known in the general case. Any such formula, if it exists, is probably very complicated: in Section 7.2 below we will see that, if a certain large cardinal axiom is true, then a formula for $p*q$ would involve non primitive recursive functions.

4. Where do Laver tables come from?

The Laver tables are finite combinatorial objects with a very simple and elementary definition, however they were discovered in the context of the theory of large cardinals, a part of mathematics which seems quite far from finite combinatorics. Although logic and set theory are not in my domain of expertise, I will try to convey some idea of the set theoretical objects involved in this construction, without giving complete definitions, and refer to the books [1, 2] for a thorough discussion. I assume here only a very basic knowledge of ordinals.

Recall that a set X is infinite if there exists an injection $j : X \to X$ which is not surjective. The typical example is the map $j : x \to x+1$ on the set $\mathbf{N}$ of natural numbers. We will need also the notion of an elementary embedding of a structure X into itself, which is an injective map $j : X \to X$ such that any formula in the language of X is true if and only if its image by j is true. We consider now ordinals. Recall that ordinals are totally ordered

$$0 < 1 < 2 < \cdots < \omega < \omega+1 < \cdots .$$

Any ordinal λ has a successor $\lambda+1$, but some ordinals, like ω, the first infinite ordinal, are not the successor of any ordinal. They are called *limit ordinals*. To ordinals we can associate *ranks* V_λ which are sets defined by induction starting with $V_0 = \emptyset$ and satisfying $V_{\lambda+1} = 2^{V_\lambda}$ and $V_\lambda = \bigcup_{\mu<\lambda} V_\mu$ if λ is a limit ordinal. The rank V_λ is equipped with the language of first order set theoretic formulas. Laver postulated the existence of a limit ordinal λ and a non-trivial elementary embedding j of V_λ into itself. Consideration of such an object is a natural extension of the idea of an infinite set: a set is infinite if it is "isomorphic" to one of its subsets without being equal to it, except that here the notion of "isomorphic" is taken in a very strict sense, that of "satisfying the same first order properties", which is much stronger than just "being in bijection with".

The image by j of any formula which is true in V_λ remains true. It follows that all "ordinary sets" i.e., the ones which can be constructed from the empty set by using the the von Neumann construction of taking subsets, power sets, unions, etc., which form the universe in which almost all ordinary mathematics is done, are invariant under j, and moreover j is monotonous. Since j is assumed to be non-trivial there must exist a smallest ordinal $\kappa < \lambda$ such that $j(\kappa) > \kappa$, this ordinal is called the *critical ordinal* of j. By elaborating on the remark above one can see that κ has to be inaccessible, so that, for example, for every ordinal $\mu < \kappa$ we have $2^\mu < \kappa$. The ordinals κ and λ have therefore to be very large. The existence of such an object cannot be proved in the usual axiomatic system of ZFC, it has to be introduced by adding a new axiom. Once the existence of j is granted by this new axiom, one can construct new elementary embeddings: an obvious way is to compose j with itself, but the structure of set theory allows also another construction, reminiscent of what we saw in Section 2.3: given an elementary embedding l of V_λ, its restriction to some V_μ with $\mu < \lambda$ is itself a set in V_λ (it can be identified with its graph as a function) and one can apply another elementary embedding k to this set. Taking inductive limits over $\mu < \lambda$ one gets an elementary embedding $k \star l$. This gives a new operation on elementary embeddings. One can prove that this operation is left distributive (essentially for the reason explained in Section 2.3). Take now J to be the set of all elementary embeddings obtained from j by using $\star$ (e.g. $j, j \star j, (j \star j) \star j, etc$). Every such elementary embedding is non-trivial and has a critical ordinal. One can prove that these ordinals form an increasing sequence $\kappa_0 < \kappa_1 < \kappa_2 < \cdots$. Moreover one can define a notion of equivalence modulo κ_n on elementary embeddings so that the Laver table of order 2^n is obtained from J by taking the quotient with respect to this equivalence relation, with j corresponding to 1 and $\star$ giving $\star_n$. The composition of elementary embeddings gives another operation, which yields $\circ_n$ by passing to the quotient. The details are somewhat technical and can be found in [1]. Thus we see that Laver tables, which are finite combinatorial objects, have been discovered from quite elaborate considerations, involving logic and set theory of large cardinals!

5. Some further properties of Laver tables

We now describe some more involved properties of Laver tables. Other results of this kind can be found in the papers of Drápal and Dougherty mentioned in the bibliography. Here we use the operation $*$, for which many of the properties are more easily stated, but of course equivalent properties can be stated for the operations $\star_n$. We will use the following notation: if p is a positive integer we denote $\nu_i(p)$ (with $\nu_1 < \nu_2 < \cdots$) the powers of 2 arising in the binary expansion of p, i.e., $p = \sum_{i=1}^{r} 2^{\nu_i(p)}$.

5.1. **Adding a power of 2.** For all p, q, n with $0 < p < 2^n$ it follows from (3.10) that $(p + 2^n) * q = p * q$ or $p * q + 2^n$.

Proposition 5.1. *Let p be such that $0 < p < 2^m < 2^n$ and q a nonnegative integer. Then*

$$(p + 2^m) * q = p * q + 2^m \text{ if and only if } (p + 2^n) * q = p * q + 2^n. \tag{5.1}$$

Proof. It is easy to prove the statement for $p = 1$, indeed we have $(1 + 2^n) * q = 0$ if q is even and $= 2^n$ if q is odd, see Section 6.2 below. Let now $\bar{p} = p + 2^m$ with $0 \leq p < 2^m$. We have $\pi(\bar{p}) \leq 2^m$ therefore, for l large enough we have, using (3.14),

$$\bar{p} * (2^l - k) = (\bar{p} * (2^l - k + 1)) * (p - 1)$$

and similarly for $\tilde{p} = p + 2^n$:

$$\tilde{p} * (2^l - k) = (\tilde{p} * (2^l - k + 1)) * (p - 1).$$

The relation is deduced by a double induction on p and k, noting that we have always $u * v < u$. □

In particular one can define, for every p, its "coperiod" by $\bar{\pi}(p) = \pi(p + 2^n)$, which does not depend on n if n is large enough. One has $\bar{\pi}(p)/\pi(p) = 1$ or 2. One can go further and note that, for $p < 2^m < 2^n$, we have

$$(p + 2^m + 2^n) * q = p * q + i2^m + j2^n$$

for some $i, j \in \{0, 1\}$. By an argument analogous to the one in the above proof we easily get

Proposition 5.2. *Let p, q, m, n, s, t be integers such that $p < 2^{m-1}$, $m < n$ and $p < 2^{s-1}$, $s < t$. Then for $i, j \in \{0, 1\}$ we have*

$$(p+2^m+2^n)*q = p*q+i2^m+j2^n \text{ if and only if } (p+2^s+2^t)*q = p*q+i2^s+j2^t. \tag{5.2}$$

Note that the conditions $p < 2^{m-1}$ and $p < 2^{s-1}$ are necessary. In general one can prove the following assertion, using similar arguments.

Proposition 5.3. *If $1 \le p < 2^m < 2^{n-1}$ then*

$$\pi(p + 2^{m+1} + 2^n) \le \pi(p + 2^m + 2^n) \le 2\pi(p + 2^{m+1} + 2^n). \tag{5.3}$$

However one may have $\pi(p + 2^m + 2^n) = 2\pi(p + 2^{m+1} + 2^n)$, for example taking $p = 5, m = 3, n = 5$ we have $\pi(45) = 8$, $\pi(53) = 4$.

5.2. **The threshold.** Let p be a nonnegative integer. Consider the increasing sequence $p * 1, p * 2, \ldots, p * (\pi(p) - 1)$. If $p \le 2^n$ and $q = p + 2^n$ then there are two possibilities for $q * 1, \ldots, q * (\pi(q) - 1)$:

- either $\pi(q) = 2\pi(p)$ and
$$q * r = p * r \quad \text{for } r < \pi(p),$$
$$q * r = p * (r - \pi(p)) + 2^n \quad \text{for } \pi(p) \le r < 2\pi(p);$$
- or $\pi(q) = \pi(p)$ and there exists some integer $\theta(q) \ge 1$ such that
$$q * r = p * r \quad \text{for } r < \pi(p) - \theta(p),$$
$$q * r = p * r + 2^n \quad \text{for } \pi(p) - \theta(p) \le r < \pi(p).$$

We define $\theta(q) = \pi(p)$ in the first case. The integer $\theta(q)$ is called the threshold of q. In order to build a row of the Laver table $p*q$; $q = 0, 1, \ldots$, for some integer p, it is enough to know the thresholds of the numbers $p_j = \sum_{i=1}^{j} 2^{\nu_i(p)}$, $j = 1, 2, \ldots$. In particular, knowing the sequence of numbers $\theta(p)$; $p = 2, 3, \ldots$, allows one to reconstruct the whole Laver table. This is especially useful for doing computer experiments since, instead of storing all products of the Laver table, one can just store the sequence of thresholds, which saves a lot of memory space. As an example we illustrate how to compute the row $p*q$ for $p = 494 = 2^1 + 2^2 + 2^3 + 2^5 + 2^6 + 2^7 + 2^8$ (the sequence $\nu_i(p)$ is $1, 2, 3, 5, 6, 7, 8$). The table below gives the numbers p_i in the first column, their thresholds in the second column and, in the last column, the row $p_i * q$; $q = 0, 1, 2, \ldots$, up to the period, with the last $\theta(p)$ numbers underlined in bold characters.

p_i	θ	$p_i * q$
2	1	$0, \underline{\mathbf{1}}$
6	2	$0, 1, \underline{\mathbf{4}}, \underline{\mathbf{5}}$
14	1	$0, 1, 4, \underline{\mathbf{13}}$
46	4	$0, 1, 4, 13, \underline{\mathbf{32}}, \underline{\mathbf{33}}, \underline{\mathbf{36}}, \underline{\mathbf{45}}$
110	3	$0, 1, 4, 13, 32, \underline{\mathbf{97}}, \underline{\mathbf{100}}, \underline{\mathbf{109}}$
238	3	$0, 1, 4, 13, 32, \underline{\mathbf{225}}, \underline{\mathbf{228}}, \underline{\mathbf{237}}$
494	8	$0, 1, 4, 13, 32, 225, 228, 237, \underline{\mathbf{256}}, \underline{\mathbf{257}}, \underline{\mathbf{260}}, \underline{\mathbf{269}}, \underline{\mathbf{288}}, \underline{\mathbf{481}}, \underline{\mathbf{484}}, \underline{\mathbf{493}}$

Proposition 5.4. *If $p < 2^m$ and $m < n$ then $\theta(p + 2^m) = \theta(p + 2^n)$.*

Proof. This follows from Proposition 5.1. ☐

This implies the existence of a "cothreshold" $\bar{\theta}(p) = \theta(p + 2^n)$ with $p < 2^n$ which does not depend on n. Here is the sequence of periods and thresholds for small values of p.

p	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\pi(p)$	1	2	2	4	2	4	4	8	2	4	4	8	4	4	4	16	2	4
$\theta(p)$	-	1	1	2	1	2	2	4	1	2	2	4	2	1	1	8	1	2

Looking at this table we see that, in this range, $\theta(p) \leq \pi(p)/2$. Actually this is always true, as follows from the following results, due to Drápal [7, 8, 9].

Proposition 5.5. *For $p \geq 1$ we have $p * p = 0$ if and only if p is a power of 2.*

Proof. It is easy to see that $2^n * 2^n = 0$ for all n. If $p = 2^m + 2^n$ with $m < n$ then $p * p = 2^m \neq 0$ by Proposition 6.1. In general, if $p = \sum_i 2^{\nu_i(p)}$ we can reduce modulo $2^{\nu_2(p)+1}$, and use the preceding case to prove that $p * p \neq 0$. ☐

Since $q \mapsto p * q$ is a homomorphism for $*$, it must map elements with square zero to elements with square zero. Therefore we get the following result.

Corollary 5.6. *For any p and $2^k < \pi(p)$ there exists $l \geq k$ with $p * 2^k = 2^l$.*

Finally we get the following estimate on tresholds.

Proposition 5.7. *Let p be a positive integer with $p < 2^n$ and $q = p + 2^n$. Then*

- *either $\theta(q) = \pi(p)$ and $\pi(q) = 2\pi(p)$*
- *or $\theta(q) < \pi(p)/2$ and $\pi(q) = \pi(p)$.*

Proof. Assume that $\pi(q) = \pi(p) = 2^m$ and $\theta(q) > 2^{m-1}$, we have $q * 2^{m-1} = p * 2^{m-1} + 2^n$ with $0 < p * 2^{m-1} < 2^n$, which is impossible in view of Corollary 5.6. ☐

The values of the thresholds in the table above are all powers of 2. This is not true generally but here is the repartition of pairs $(\theta(p), \pi(p))$ for p between 1 and 2^{12}, (for example there are 761 numbers $1 \leq p \leq 2^{12}$ with period 16 and threshold 4):

	2	**4**	**8**	**16**	**32**	**64**	**128**	**256**	**512**	**1024**	**2048**	**4096**
1	12	2103										
2		66		30								
3			398	213								
4			58	761								
7				63								
8				121								
16					12	110						
32						34						
48							19	6				
64							22	26				
112								1				
128								25				
256									4	2		
512										6		
1024											2	
2048												1

The data above seem to indicate that $\theta(p)$ only takes values of the form $2^i - 2^j$. Indeed the values of thresholds in this table are, apart from powers of 2:

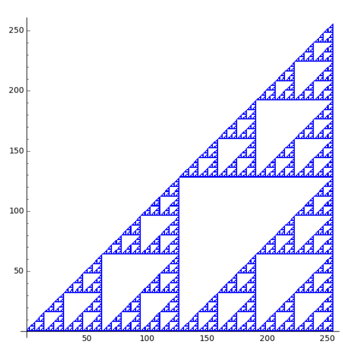
$$3 = 2^2 - 2^0,\ 7 = 2^3 - 2^0,\ 15 = 2^4 - 2^0,\ 48 = 2^6 - 2^4,\ 112 = 2^7 - 2^4,$$

(in the table above only values smaller than 2^{12} are considered, in fact I pushed the computations to 2^{31} and the claim still holds). I do not know whether this property holds for all thresholds.

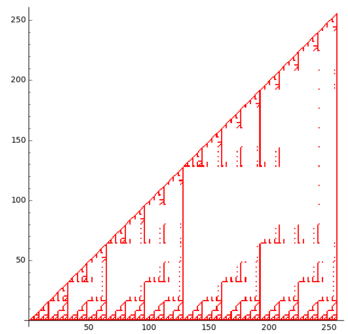
5.3. **Binary expansion.** Any nonnegative integer can be identified with a finite subset of $\mathbf{N}$ by its binary expansion. The inclusion relation of subsets of $\mathbf{N}$ induces an order relation $p \sqsubset q$ on the nonnegative integers, thus $p \sqsubset q$ if and only if the digits of the binary expansion of p are not larger than the corresponding ones of q. The existence of the threshold implies that, for any p, q we have

$$p * q \sqsubset p - 1. \tag{5.4}$$

Here is a graph of the order relation $\sqsubset$, for $p \leq 256$, which is essentially a Sierpiński triangle:



The Laver table can be represented as a subset of this graph, (shifted by 1 to take into account the $p-1$ in (5.4)): drawing the points $p*q$ above p for each p, we get the following picture



As is clear on this graph, the Laver tables become much sparser than the Sierpiński triangle as n increases. More on this in Sections 8 and 9.

6. Some rows of the Laver tables

In this section I explain how to compute the row of p for some particular values of p.

6.1. **The row of 2^n.** It is easy to see, by reverse induction on q, that $2^n*q = q \mod 2^n$ and $\pi(2^n) = 2^n$. Moreover $\theta(2^n) = 2^{n-1}$ since the period doubles between 2^{n-1} and 2^n.

6.2. **The row of $p = 2^m + 2^n$.**

Proposition 6.1. *Let $n > m \geq 0$ and $p = 2^m + 2^n$. Then $\pi(p) = 2^{m+1}$. Moreover if $q < 2^m$ then $p*q = q$ and $p*(q+2^m) = q+2^n$.*

Proof. If $2^n < r < 2^m + 2^n$ then $r = 2^n + s$ with $s < 2^m$ therefore $\pi(s) < 2^m$ and $\pi(r) \leq 2^m$. On the other hand, by (3.14), we have

$$p*(2^l - k - 1) = (p*(2^l - k))*(p-1)$$

therefore by induction on $k \leq 2^m$ we have $p*(2^l - k) = p - k$ since

$$(p*(2^l-k))*(p-1) = (p*(2^l-k))*(2^m-1) = (p*(2^l-k)) - 1.$$

Finally $p*(2^l - 2^m) = 2^n$ and $\pi(2^n + 2^m) > \pi(2^m)$. The proposition follows from that. □

6.3. **The row of $p = 2^l + 2^m + 2^n$.** This case is more involved than the preceding ones. Observe that $\pi(2^l + 2^m) = 2^{l+1}$ by Proposition 6.1, therefore $\pi(p) = 2^{l+1}$ or 2^{l+2}. We will prove the following result, by induction on n.

Proposition 6.2. *Let n be a positive integer.*

1. *For $0 \leq l < m < n$ and $p = 2^l + 2^m + 2^n$ we have $\pi(p) = 2^{l+2}$ if l is even and $\pi(p) = 2^{l+1}$ if l is odd. Moreover $\theta(p) = 2^{l-1}$ in this last case.*
2. *For any $p < 2^{n+1}$ we have $\pi(p) \leq 2^n$ with equality exactly in the following cases:*

$$p = 2^n$$
$$p = 2^n + 2^{n-1}$$
$$p = 2^n + 2^{n-1} + 2^{n-2} \quad \textit{if } n \textit{ is even.}$$

Proof. The statements are easy to check for small values of n. Let $r > 0$ and assume that Proposition 6.2 holds for all values $l < m < n \leq r$. We will prove that it holds for all $l < m < n = r + 1$. The proof is divided into several cases.

I. r is odd.

We start with proving (1). If $m < r$ then the lines of $p = 2^l + 2^m + 2^{r+1}$ and $p_- = 2^l + 2^m + 2^r$ can be deduced from one another by Proposition 5.1 therefore we conclude by induction. Similarly, if $l < r - 2$ and $m = r$ we can apply Proposition 5.2 to conclude.

It remains to consider the cases $l = r - 2$ and $l = r - 1$.

a) Let $l = r - 2$ so that $p = 2^{r+1} + 2^r + 2^{r-2}$. Take some t large enough (e.g. $t = r + 2$), we have $p - 1 = p * (2^t - 1)$ and, by (3.14),

$$p * (2^t - k) = (p * (2^t - (k - 1)) * (p - 1). \tag{6.1}$$

Let u be the smallest $s \geq 1$ such that $\pi(p-s) \geq 2^{r-1}$. Since $p - 2^{r-3} = 2^{r+1} + 2^r + 2^{r-3}$ we have, by what we just saw, that $\pi(p - 2^{r-3}) = 2^{r-1}$ therefore $u \leq 2^{r-3}$. Applying (6.1) and noting that $p - 1 = 2^{r-2} - 1 \mod 2^{r-2}$ we see, by induction on s, that $p * (2^t - s) = p - s$ for all $s \leq u$. Suppose that $u < 2^{r-3}$. Then $p - u = 2^{r+1} + 2^r + 2^{r-2} - u = 2^{r+1} + 2^r + v$ with $2^{r-3} < v < 2^{r-2}$. In order that $\pi(p-u) \geq 2^{r-1}$ we must have $\pi(v) \geq 2^{r-3}$ therefore, by induction hypothesis, either $v = 2^{r-3} + 2^{r-4}$ or $v = 2^{r-3} + 2^{r-4} + 2^{r-5}$. However, by Proposition 5.2, we have $\pi(2^{r+1} + 2^r + v) = \pi(2^r + 2^{r-1} + v)$ and we can use the induction hypothesis to see that in these two cases $\pi(2^r + 2^{r-1} + v) \leq 2^{r-2}$. It follows that $s = 2^{r-3}$ and $p * (2^t - 2^{r-3}) = 2^{r+1} + 2^r + 2^{r-3} := w$ with $\pi(w) = 2^{r-1}$ as we have seen. We can now compute

$$p * (2^l - 2^{r-3} - 1) = w * (p - 1) = w * (2^{r-2} - 1) = 2^{r-3} + 2^r - 1 < 2^{r+1}.$$

It follows that $\theta(p) = 2^{r-3}$ and $\pi(p) = 2^{r-2}$, as claimed.

b) Let $l = r - 1$. A similar reasoning as in case a) shows that $p * (2^l - k) = p - k$ for $k = 1, \dots, 2^{r-2}$, in particular

$$p * (2^l - 2^{r-2}) = p - 2^{r-2} = 2^{r+1} + 2^r + 2^{r-2}.$$

We can now apply case a) and compute

$$p * (2^l - 2^{r-2} - 1) = (2^{r+1} + 2^r + 2^{r-2}) * (p - 1) = (2^{r+1} + 2^r + 2^{r-2} - 1).$$

Using now that all q with $2^{r+1} + 2^r < q \leq 2^{r+1} + 2^r + 2^{r-2} - 1$ have period at most 2^{r-1} we obtain $p * (2^l - 2^{r-1}) = 2^{r+1} + 2^r$. We know that $\pi(2^{r+1} + 2^r) = 2^{r+1}$ and we can compute $(2^{r+1} + 2^r) * (p - 1) = 2^{r+1} + 2^{r-1} - 1$. Since all $q < 2^{r+1} + 2^{r-1}$ have period at most 2^{r-1} it follows that $p * (2^l - 2^r) = 2^{r+1}$ and $\pi(p) = 2^{r+1}$.

Let us now prove (2). We have already checked that the periods of $p = 2^{r+1}, 2^{r+1} + 2^r$ and $2^{r+1} + 2^r + 2^{r-1}$ are equal to 2^{r+1}. Suppose that some other $p < 2^{r+2}$ satisfies $\pi(p) = 2^{r+1}$. Then we have $p > 2^{r+1}$. Moreover if $p = 2^{r+1} + q$ with $q < 2^{r+1}$ then $\pi(q) = 2^r$. Therefore, by induction hypothesis, we have either $q = 2^r$ or $q = 2^r + 2^{r-1}$.

II. r is even.

The argument when r is even is similar. We start with (1). The cases $m < r$ and $m = r$, $l < r - 2$ are identical with the odd case.

Suppose now $p = 2^{r+1} + 2^r + 2^{r-2}$. Again we prove that $p * (2^l - k) = p - k$ for $k = 1, \dots, 2^{r-3}$, in particular $p * (2^l - 2^{r-3}) = 2^{r+1} + 2^r + 2^{r-3}$. This time we have $\pi(2^{r+1} + 2^r + 2^{r-3}) = 2^{r-2}$ and we can argue as in b) of case I to show that $\pi(p) = 2^r$.

Assume that $p = 2^{r+1} + 2^r + 2^{r-1}$, now $p * (2^l - k) = p - k$ for $k = 1, \dots, 2^{r-2}$, in particular $p * (2^l - 2^{r-2}) = 2^{r+1} + 2^r + 2^{r-2}$ with $\pi(2^{r+1} + 2^r + 2^{r-2}) = 2^r$ as we have just seen and an argument similar as in case I above shows that $\pi(p) = 2^r$ and $\theta(p) = 2^{r-2}$.

For the proof of (2), we have already checked that the periods of 2^{r+1} and of $2^{r+1} + 2^r$ are 2^{r+1}. Suppose that some other $p < 2^{r+1}$ satisfies $\pi(p) = 2^{r+1}$. Then we have $p > 2^{r+1}$. Moreover if $p = 2^{r+1} + q$ with $q < 2^{r+1}$ then $\pi(q) \geq 2^r$ therefore by induction hypothesis we have either $q = 2^r$ or $q = 2^r + 2^{r-1}$ or $q = 2^r + 2^{r-1} + 2^{r-2}$. It remains to prove that $\pi(2^{r+1} + 2^r + 2^{r-1} + 2^{r-2}) = 2^r < 2^{r+1}$. The argument is similar as above: if we have $\pi(2^{r+1} + 2^r + 2^{r-1} + 2^{r-2}) = 2^{r+1}$ we would have $(2^{r+1} + 2^r + 2^{r-1} + 2^{r-2}) * (2^l - 2^{r-2}) = 2^{r+1} + 2^r + 2^{r-1}$ but by what we have seen above $\pi(2^{r+1} + 2^r + 2^{r-1}) = 2^r$ therefore $\pi(2^{r+1} + 2^r + 2^{r-2}) * (p-1) < 2^{r+1} + 2^r + 2^{r-2} - 1$. $\square$

Remark 6.3. It would be also possible to prove the preceding proposition using results of Dougherty [5] or Drápal [10]. We provided the proof above in order to give a glimpse of the kind of arguments used in these computations.

7. Why are Laver tables interesting?

7.1. **Structure of the Laver tables.** In view of their very elementary definition and of their connection with basic operations such as the composition of functions, it is clear that Laver tables are fundamental objects in mathematics. They are also very recursive objects. This can be seen from the relation (2.2) defining self-distributivity, in which the number of symbols on both sides is not the same. This implies that the computation of a product $p * q$ using rules (2.2) and (2.1) makes one go through long recursions. As I wrote in the introduction, in some respect these objects are reminiscent of the Mandelbrot or Julia sets which also have a very simple recursive definition, yet display very complex features[3]. As such, they pose challenging problems which are quite different from the ones one encounters usually in algebraic combinatorics. The most obvious question is whether there exists a simple formula for computing $p * q$ for arbitrary p and q, i.e., one which involves the computation of as few intermediate values as possible. Also we would like to find formulas for $\pi(p)$ or $\theta(p)$. As we shall see below, it is unlikely that such general formulas exist, however we might find large classes of elements for which the computation is easy. Some examples were described above in Section 6 and I will describe further results in this direction in Section 9. Examination of numerical values of the Laver tables reveals a lot of non-obvious structure. As an example, here are the periods $\pi(p)$ of all $p \in [1, 256]$, with the p arranged in increasing order, in 16 rows of 16.

[3]Incidentally the combinatorics of powers of 2 also plays a role in the study of the Mandelbrot set, cf. [13].

1	2	2	4	2	4	4	8	2	4	4	8	4	4	4	16
2	4	4	8	4	4	4	16	4	4	4	16	8	8	8	32
2	4	4	8	4	4	4	16	4	4	4	16	8	8	8	32
4	4	4	16	4	4	4	16	4	4	4	16	16	8	8	64
2	4	4	8	4	4	4	16	4	4	4	16	8	8	8	32
4	4	4	16	4	4	4	16	4	4	4	16	16	8	8	64
4	4	4	16	4	4	4	16	4	4	4	16	16	8	8	64
8	4	4	16	4	4	4	16	4	4	4	16	16	16	8	128
2	4	4	8	4	4	4	16	4	4	4	16	8	8	8	32
4	4	4	16	4	4	4	16	4	4	4	16	16	8	8	64
4	4	4	16	4	4	4	16	4	4	4	16	16	8	8	64
8	4	4	16	4	4	4	16	4	4	4	16	16	16	8	128
4	4	4	16	4	4	4	16	4	4	4	16	16	8	8	64
4	4	4	16	4	4	4	16	4	4	4	16	16	8	8	64
4	4	4	16	4	4	4	16	4	4	4	16	16	8	8	64
16	4	4	16	4	4	4	16	4	4	4	16	16	16	8	256

A cursory look at this table suggests that there are many patterns here. For example several lines coincide and some of these coincidences can be easily explained using Proposition 5.1 or 5.2. More subtle is the fact that the first row is equal to the first column and multiplying it by 16 gives the last column. This remark can be explained by the following results.

Proposition 7.1 (Drápal [7, Theorem 3.6])**.** *Let $\sigma_d : ([1,2^n],\star_n) \to ([1,2^{n+d}],\star_{n+d})$ be given by $\sigma_d(p) = 2^d p$. Then σ_d is a homomorphism if and only $n \leq 2^{r+1}$, where 2^r is the largest power of 2 dividing d. Similarly σ_d is a homomorphism for $*$.*

Applying Proposition 7.1 for $d = 4$ and $n = 4$ we see that the map $p \mapsto 16p$ is a homomorphism from $[1,16]$ to $[1,256]$ therefore the period of $256 - 16q$ in the Laver table of size 256 is 16 times the period of $16 - q$ in the Laver table of size 16. This gives an explanation for the fact that the first row multiplied by 16 is equal to the last column. A corollary of Proposition 7.1 is the following.

Corollary 7.2. *For any integers $r \in [0, 2^{2^n}[$ and $q \geq 0$ we have*

$$2^{2^n}((1+r)*q) = (1 + r2^{2^n}) * q.$$

Proof. Applying (3.11) and Proposition 7.1 we get

$$(1 + r2^{2^n}) * q = (r2^{2^n})^{(q)} = 2^{2^n}\left(r^{(q)}\right) = 2^{2^n}((1+r)*q). \quad \square$$

It follows from this corollary that the first row and the first column of the table above coincide. These results can be further generalized and several more sophisticated explicit homomorphisms have been constructed by Drápal (see e.g. [8, 10]) and Dougherty (see [5], we will use one of these results in Section 9). Looking for more homomorphisms could be of use for solving the questions we are going to expose in the next section.

7.2. **Asymptotic properties of Laver tables.** For any $p \geq 1$, the sequence of periods $\pi_n(p)$ (which is defined for n large enough) satisfies $\pi_{n+1}(p) = \pi_n(p)$ or $2\pi_n(p)$, in particular it is nondecreasing. It is therefore natural to ask whether it remains bounded as n goes to infinity. From the work of Laver [11, 12], Dougherty and Jech [6] we know that this is equivalent to the freeness of the projective limit of Laver tables, more precisely, $\pi_n(1) \to \infty$ if and only if $\pi_n(p) \to \infty$ for all p, if and only if the projective limit of the Laver tables is the free left distributive system generated by 1. Moreover, if we assume the existence of a limit ordinal λ and a non-trivial elementary embedding from V_λ into itself, then all these equivalent statements hold. No direct proof of this (i.e., not using the Laver axiom) has been found and by [6] such a proof does not exist in primitive recursive arithmetic. In fact the function which maps m to the smallest n such that $\pi_n(1) = 2^m$ grows faster than any primitive recursive function. For example, it is easy to compute the first values of $\pi_n(1)$ and see that $\pi_9(1) = 16$, however Dougherty [4] has given an amazing lower bound: he proved that, if there exists an n such that $\pi_n(1) = 32$ then $n > f_9(f_8(f_8(254)))$, where $f_x(y)$ is a variant of the Ackermann function. This number, if it exists, is thus incredibly large. However it is not known whether the existence of such an n can be proved without Laver's axiom. Finding proofs of these statements from a combinatorial approach is a very challenging task. Some interesting attempts have been made by Drápal [8] and Dougherty [5] but for the moment a full proof seems out of reach. The considerations above give an answer to a question we raised in Section 2.3. There we mentioned the problem of constructing a family I (not reduced to the identity) of injections of a set X into itself, endowed with a binary left distributive operation $\star : I \times I \to I$, such that, for any $\iota, \eta \in I$ and $x \in X$ we have $(\iota \star \eta)(\iota(x)) = \iota(\eta(x))$, as in (2.6). As shown by Dougherty and Jech [6], assuming that the projective limit of Laver tables is free, we can construct such a family in the following way. Let W be the free left distributive system with one generator. For any $w \in W$ we can look at its image in the Laver table of order 2^m. Let $e_w(n)$ be the largest integer m such that $w \star_m 2^n = 2^m$ in the Laver table of order 2^m. Since the period $\pi_m(2^n)$ goes to infinity as $m \to \infty$ (by Laver's result) this is well defined and gives a family $(e_w; w \in W)$ of embeddings of $\mathbf{N}$ into itself. This family is endowed with a left distributive operation inherited from W. Dougherty and Jech have proved that for any pair of such embeddings the property $(\iota \star \eta)(\iota(n)) = \iota(\eta(n))$ is satisfied. Actually they prove much more properties of these objects, see [6].

Another natural question that one can ask is whether one can say something about Laver tables seen from very far, i.e., do the Laver tables satisfy some interesting statistical properties for large n? A first result in this direction is the subject of the next section.

8. Asymptotic frequencies

For $n \geq k$ let $N_k(n)$ be the number of $p \in [1, 2^n]$ whose period is 2^k and $\omega_k(n) = N_k(n)/2^n$ be the frequency of the period 2^k in the Laver table of order 2^n. Thus $\sum_{k=0}^{n} \omega_k(n) = 1$.

Proposition 8.1. *For any k the limit $\omega_k = \lim_{n\to\infty} \omega_k(n)$ exists.*

Proof. Let $P_k(n)$ be the number of $p \in [1, 2^{n-1}]$ such that $\pi(p) = 2^{k-1}$ and $\pi(p+2^{n-1}) = 2^k$. Since $\pi(p + 2^{n-1}) = \pi(p)$ or $2\pi(p)$ we have

$$N_k(n) = 2N_k(n-1) + P_k(n) - P_{k+1}(n)$$

and

$$\omega_k(n) = \omega_k(n-1) + (P_k(n) - P_{k+1}(n))/2^n.$$

The only p with $\pi(p) = 1$ is $p = 1$ and the only p with $\pi(p) = 2$ are the numbers $p = 1 + 2^k$; $k = 0, 1, 2, \ldots$. It follows that $N_0(n) = 1$ and $N_1(n) = n$. Looking at the table of order 4 we see that $\omega_2(2) = 1/4$. Moreover from Proposition 6.1 we see that $P_2(n) = N_1(n-1) = n-1$ for $n \geq 3$ therefore

$$\begin{aligned}
\omega_0(n) &= \tfrac{1}{2^n} \to \omega_0 = 0 \quad \text{as } n \to \infty \\
\omega_1(n) &= \tfrac{n-1}{2^n} \to \omega_1 = 0 \quad \text{as } n \to \infty \\
\omega_2(n) &= 1/4 + \textstyle\sum_{m=3}^n \tfrac{m-1}{2^m} - \tfrac{P_3(m)}{2^m}.
\end{aligned}$$

Since $\omega_2(n) \geq 0$ we have

$$\sum_{m=2}^{n} \frac{P_3(m)}{2^m} \leq 1/4 + \sum_{m=3}^{n} \frac{m-1}{2^m} < 1/4 + \sum_{m=3}^{\infty} \frac{m-1}{2^m} = 1$$

therefore the series $\sum \frac{P_3(m)}{2^m}$ converges and

$$\omega_2(n) \to \omega_2 = 1 - \sum_{m=3}^{\infty} \frac{P_3(m)}{2^m} \quad \text{as } n \to \infty$$

We have also

$$\omega_3(n) = 1/8 + \sum_{m=4}^{n} \frac{P_3(m)}{2^m} - \frac{P_4(m)}{2^m}$$

therefore

$$\sum_{m=4}^{n} \frac{P_4(m)}{2^m} \leq 1/8 + \sum_{m=4}^{\infty} \frac{P_3(m)}{2^m}$$

and the series $\sum_{m=4}^{\infty} \frac{P_4(m)}{2^m}$ converges. It follows that

$$\omega_3(n) \to 1/8 + \sum_{m=4}^{\infty} \frac{P_3(m)}{2^m} - \frac{P_4(m)}{2^m} \quad \text{as } n \to \infty.$$

An obvious induction now yields the result for all k as well as the explicit expressions

$$\omega_k = 2^{-k} + \sum_{m=k+1}^{\infty} \frac{P_k(m)}{2^m} - \frac{P_{k+1}(m)}{2^m},$$

where all series $\sum_m \frac{P_k(m)}{2^m}$ converge. $\square$

Note that, by the same argument, we can also obtain the convergence of frequencies $\omega_{k,l,m}$ of the set of $p \leq 2^n$, with period 2^k satisfying, $p = m \mod 2^l$ for some fixed l

and $m \in [1, 2^l]$. The argument above is very simple. Moreover we can also derive upper bounds on the values of the asymptotic frequencies from it. For example we have

$$\sum_{k=1}^{l} \omega_k = 1 - \sum_{m=l+1}^{\infty} \frac{P_{l+1}(m)}{2^m} \leq \sum_{k=1}^{l} \omega_k(n)$$

so that knowing the values of the $\omega_k(n)$ for some n gives upper bounds on the asymptotic frequencies. Unfortunately this proof does not give any useful lower bounds on the asymptotic frequencies. Indeed, at this point, we cannot exclude that all ω_k may be zero. Here are some numerical values of the frequencies (expressed as percentages to gain readability) for $n = 22$ and $n = 31$:

π_n	2	4	8	16	32
$n = 22$	0.000572	52.936697	10.196733	30.197978	0.002623
$n = 31$	0.000002	52.936599	10.193012	30.202195	0.001429
π_n	64	128	256	512	1024
$n = 22$	3.550982	0.684047	2.035284	0.000763	0.209165
$n = 31$	3.551050	0.679749	2.040756	0.000003	0.209228

Arguments of Dougherty in [4] show that one can expect the frequencies $\pi_n(p)$ to grow very slowly with n, therefore that the numbers $P_k(n)$ might be small compared to 2^n. This would imply that not only some of the ω_k are nonzero, but also that $\sum_n \omega_n = 1$, therefore they define a probability distribution on the positive integers. Here are some values of $\mathcal{P}(n) = \sum_k P_n(k)$ which is the number of p whose period doubles between A_n and A_{n+1}.

n	4	8	12	16	20	24	28
$\mathcal{P}(n)$	16	58	147	336	650	1201	2249
$2^{4+n/4}$	32	64	128	256	512	1024	2048

On this small sample the formula $2^{n/4+4}$ seems to give a rough approximation of $\mathcal{P}(n)$ which, if it remains valid for large values of n, would be enough for the probability measure to put zero mass at infinity.

The existence of this probability measure, which is canonical, in the sense that it does not depend on any external parameter like a mean or a variance, raises challenging and completely open questions: can one characterize this probability distribution, or give a formula for it? Does it appear in other questions of mathematics or physics?

9. Maximal elements

9.1. **Definition of maximal elements.** Let $bit(n)$ is the number of ones in the binary expansion of an integer n. The set of numbers r satisfying $r \sqsubset n$ has $2^{bit(n)}$ elements. We have seen that for any p the numbers $p * q$ satisfy $p * q \sqsubset p - 1$ therefore

$$\pi(p) \leq 2^{bit(p-1)}. \tag{9.1}$$

Definition 9.1. *A positive integer p is called* maximal *if $\pi(p) = 2^{bit(p-1)}$.*

It follows from Section 6 that, if p has at most two ones in its binary expansion, then p is maximal. If it has three ones in its binary expansion then it is maximal if and only if the largest power of 2 which divides it is of the form 2^{2m} for some integer $m \geq 1$. The purpose of this section is to determine the set of all maximal p's. As a consequence of the description of these elements, we will see that they form a subset stable under the binary operations $*$ and $\circ$. Let p be a maximal element, it follows from the definition that the numbers $p * q$, $q = 0, 1, 2 \ldots, \pi(p) - 1$, are all the integers whose binary expansion is contained in that of $p - 1$, listed in increasing order. This gives a simple algorithm for the computation of $p * q$. As an example, assume p has binary expansion $p = 1010110000111100000001$ (we will see below that p is maximal, thus $\pi(p) = 2^8$) and let q have binary expansion 11000101. The binary expansion of $p * q$ is obtained by writing the binary expansion of q below the 1's of $p - 1$ and keeping only the 1's of $p - 1$ which match a 1 of q, as shown below:

$$\begin{array}{cccccccccccccccccccccccc}
p-1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
q & 1 & & 1 & & 0 & 0 & & & & & 0 & 1 & 0 & 1 & & & & & & & & \\
p*q & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}$$

Note also that, by Proposition 5.1, if p is maximal then all the numbers $p \mod (2^m)$ are maximal. Moreover if we write $p = 2^n + q$ with $q < 2^n$ then for any l such that $2^l > q$ the number $2^l + q$ is also maximal. It follows that it is enough to describe all maximal elements such that $2^{n-1} + 2^{n-2} < p \leq 2^n$ for some n.

9.2. **Characterization of maximal elements.** Recall that a partition of an integer n is a sequence of integers $\lambda_1 \geq \lambda_2 \geq \cdots \geq 0$ such that $n = \sum_i \lambda_i$. A binary partition is a partition in which all λ_i are powers of 2. Since any binary partition of an odd integer must contain a 1, the number of binary partitions of $2n + 1$ is equal to the number of binary partitions of $2n$. The numbers of binary partitions of n form sequence A018819 in OEIS, see [15]. Their first values are $1, 1, 2, 2, 4, 4, 6, 6, 10, 10, 14, 14, 20, 20, \ldots$. These numbers satisfy the recursion

$$a(2m + 1) = a(2m) = a(2m - 1) + a(m).$$

Theorem 9.2. *For any $n \geq 2$ the maximal elements $p \in]2^{n-1}+2^{n-2}, 2^n]$ are in bijection with the binary partitions with sum $n - 1$: if*

$$n - 1 = (b_1 + 1)2^{a_1} + (b_2 + 1)2^{a_2} + \cdots + (b_r + 1)2^{a_r},$$

with $a_1 < a_2 < a_3 < \cdots < a_r$ and $b_i \geq 0$, is a binary partition of sum $n - 1$ (where $b_i + 1$ is the multiplicity of 2^{a_i} in the partition) then the binary word

$$11^{2^{a_1}}0^{b_1 2^{a_1}}1^{2^{a_2}}0^{b_2 2^{a_2}} \cdots 1^{2^{a_r}}0^{b_r 2^{a_r}} \tag{9.2}$$

is the binary expansion of $p - 1$, where p is a maximal element of period 2^m with $m = 1 + 2^{a_1} + \cdots + 2^{a_r}$, and all maximal elements in $]2^{n-2} + 2^{n-1}, 2^n]$ are of this form.

Corollary 9.3. *The set of maximal elements is the set of p such that $p - 1$ has binary expansion of the form*

$$10^{b_0}1^{2^{a_1}}0^{b_1 2^{a_1}}1^{2^{a_2}}0^{b_2 2^{a_2}} \cdots 1^{2^{a_r}}0^{b_r 2^{a_r}}. \tag{9.3}$$

The proof relies on the following results of Dougherty (see Theorem 4.1 and Lemma 4.5 in [5]).

Theorem 9.4.

(1) *If* $p-1 = a2^{2^k} + b$ *with* $a < 2^{2^k}$ *and* $b < 2^{2^k} - 1$ *then* $\pi(p) \leq 2^{2^k}$.
(2) *Let* $p = x + 1 + 2^{mn}y$, *where* $n = 2^k$ *is a power of* 2 *and* $x = z2^{(m+1)n}$ *for some positive integer* z *and* $y < 2^n$. *Let* 2^l *be the period of* $x+1$ *and suppose* $l \leq n$. *Then* p *has the same period as* $2^{l+n} - 2^n + y + 1$. *Moreover* $(2^{l+n} - 2^n + y + 1) * q = 2^n w + y'$ *with* $y' < 2^n$ *if and only if* $p * q = (x+1) * w + 2^{mn}y'$.

From this we deduce the following bound.

Lemma 9.5. *Let* $k \geq 1, m \geq 0$ *and* $p - 1 = (2^{2^k+1} - 1)2^{2^{k-1}+m2^k}$. *Then* $\pi(p) \leq 2^{2^k}$.

Proof. If $m = 0$ apply (i) of Theorem 9.4 with $a = 2^{2^{k-1}+1} - 1$ and $b = 2^{2^k} - 2^{2^{k-1}}$ to get that $\pi(p) \leq 2^{2^k}$. If $m > 0$ we can use (ii) with $x + 1 = (2^{2^{k-1}+1} - 1)2^{(m+1)2^k}$ and $y = 2^{2^k} - 2^{2^{k-1}}$ so that $p = x + y2^{m2^k} + 1$. Since $bit(x) = 2^{k-1} + 1$ we have $\pi(x+1) = 2^l \leq 2^{2^{k-1}+1}$ therefore p has the same period as $2^{l+2^k} - 2^{2^k} + y + 1 = 2^{l+2^k} - 2^{2^{k-1}} + 1$, which is less that 2^{2^k} by the case $m = 0$ that we just proved. □

In particular $p = (2^{2^k+1} - 1)2^{2^{k-1}} + 1$ is not a maximal element.

Proof of Theorem 9.2. We prove by induction on $m = 1 + \sum_i 2^{a_i}$ that, if $p - 1$ has binary expansion (9.2) then it is a maximal element. This is clear if $m = 1$ or 2, by Proposition 6.2. If $m - 1 = 2^a + l$ with $l < 2^a$ then $p - 1$ has binary expansion $1w1^{2^a}0^{b2^a}$ for some binary word w. Moreover if x has binary expansion $1w0^{(b+1)2^a}$ then, by induction hypothesis, $x + 1$ is a maximal element. We can now apply (ii) of Theorem 9.4 with $y = 2^{2^a} - 1$, $n = 2^a$, $m = b$ to see that p is again maximal.

Now we prove the converse: if $p - 1$ is not of the form (9.3) then p is not maximal. The reduction modulo 2^m of a maximal element is again maximal, therefore we may assume that $p - 1 = 2^n + q - 1$, where $q - 1 < 2^n$ and q has the form (9.3), i.e., n is the smallest integer such that $p - 1 \mod 2^{n+1}$ does not have the form (9.3). It is easy to check that $p - 1$ must have a binary expansion of the form

$$10^{b_0}1^{2^{a_1}}0^{b_1 2^{a_1-1}}1^{2^{a_2}}0^{b_2 2^{a_2}} \cdots 1^{2^{a_r}}0^{b_r 2^{a_r}},$$

where

(1) either $r \geq 1,\ 1 \leq a_1 \leq a_2 < a_3 < \cdots < a_r$ and b_1 is odd.
(2) or $r \geq 2,\ 0 \leq a_1 = a_2 < a_3 < \cdots < a_r$ and $b_1 \geq 2$ is even.

Without loss of generality we can assume that $b_0 = 0$ (cf. Proposition 5.1).

We first treat case (1) for $r = 1$, $b_1 = 1$: this follows from Lemma 9.5 with $a_1 = k$. Extension to $b_1 > 1$ is obtained by applying Theorem 9.4. The case $r \geq 2$ follows by induction, again using Theorem 9.4.

Case (2) with $r = 2$: let $a = a_1$ and assume by contradiction that p is maximal, with period $2^{2^{a+1}+1}$. Then

$$p * (2^{2^{a+1}+1} - 2^{2^a} + 1) - 1 = p' - 1$$

can be computed using the algorithm above for maximal elements. We see that $p' - 1$ has binary expansion $11^{2^a}0^{(b_1+1)2^a}1^{b_2 2^a}$ therefore p' is maximal by what we have proved.

We can compute again

$$p * (2^{2^{a+1}+1} - 2^{2^a}) = p' * (p-1) = 2^{(b_1+b_2+1)2^a} - 2^{(b_1+b_2)2^a} < 2^{(b_1+b_2+1)2^a+1}$$

which shows that p is not maximal and also that $\theta(p) \leq 2^{2^a} - 1$. The case of $r > 2$ is treated again by induction. □

9.3. **Stability of maximal elements.** Let $\mathcal{M}$ be the set of maximal elements and $\mathcal{M}^* = \mathcal{M} \cup \{0\}$.

Theorem 9.6. *Let $p, q \in \mathcal{M}^*$. Then $p * q \in \mathcal{M}^*$. If $p, q \in \mathcal{M}$ then $p \circ q \in \mathcal{M}$.*

Proof. Now that we have a complete description of maximal elements and a simple formula for computing $p * q$ and $p \circ q = p * (q-1) + 1$ whenever p is maximal, this amounts just to a verification. This is not difficult but a bit cumbersome due to the boundary effects caused by subtracting 1, so we will only sketch the idea of the proof, leaving the details to the reader. First we note that, if p maximal, then the binary expansion of $p-1$ can be obtained from the following construction. Let w be a binary word and $t = 0^{b2^a}$. Define the insertion of t into w as follows: split w as $w = uv$, where the number of 1's in u is at most 2^{a+1} while the number of 1's in v is a multiple (possibly 0) of 2^{a+1}, then insert t so as to obtain the word utv. The result of the insertion is uniquely defined by w, a, b, but beware that by writing $b2^a = c2^d$ the insertion may give a different result. It is easy to see that the set of maximal elements with period 2^n is exactly the set of p such that the binary expansion of $p-1$ is obtained by a sequence of such insertions, starting from the word 1^n.

Let now p be a maximal element with period 2^n and let $x_0 = 2^n - 1, \ldots, x_s = p-1$ be the sequence of numbers obtained by the successive insertions. Then each $p_i = x_i + 1$ is maximal and for any q, the binary expansion of $p_{i+1} * q - 1$ is obtained from that of $p_i * x$ by an insertion of the same block of zeros as x_{i+1} from x_i. Note that $b2^a$ may be interpreted as $c2^d$ for some $d < a$ in this process. Since q is maximal, $2^n * q$ is maximal and since the insertion process preserves the set of maximal elements we are done. The case of $\circ$ is similar and left to the reader. □

We have thus identified a subset of the integers which forms a stable subset for the two operations $*, \circ$, on which these are given by very simple formulas. This could be the first step in determining a more general formula, valid for much larger sets of integers.

References

[1] P. Dehornoy, *Braids and Self Distributivity.* Progress in Mathematics, vol. 192; Birkhäuser (2000).

[2] P. Dehornoy, *Théorie des ensembles.* Calvage et Mounet, Paris (2017).

[3] P. Dehornoy, *Some aspects of the SD-world.* Nonassociative mathematics and its applications, 69–96, Contemp. Math., vol. 721, Amer. Math. Soc., Providence, R.I., 2019.

[4] R. Dougherty, *Critical points in an algebra of elementary embeddings.* Ann. Pure Appl. Logic 65 (1993), 211–241.

[5] R. Dougherty, *Critical points in an algebra of elementary embeddings, II.* Logic: from foundations to applications (Staffordshire, 1993), 103–136, Oxford Sci. Publ., Oxford Univ. Press, New York, 1996.

[6] R. Dougherty, T. Jech, *Finite left-distributive algebras and embedding algebras.* Adv. Math. 130 (1997), no. 2, 201–241.

[7] A. Drápal, *Homomorphisms of primitive left distributive groupoids.* Commun. Algebra 22 (1994), 2579–2592.

[8] A. Drápal, *Persistence of cyclic left distributive algebras.* J. Pure Appl. Algebra 105 (1995), 137–165.

[9] A. Drápal, *On the semigroup structure of cyclic left distributive algebras.* Semigroup Forum 51 (1995), 23–30.

[10] A. Drápal, *About Laver tables.* Nonassociative mathematics and its applications, 97–113, Contemp. Math., vol. 721, Amer. Math. Soc., Providence, R.I., 2019.

[11] R. Laver, *The left distributive law and the freeness of an algebra of elementary embeddings.* Adv. Math. 91 (1992) 209–231.

[12] R. Laver, *On the algebra of elementary embeddings of a rank into itself.* Adv. Math. 110 (1995), no. 2, 334–346.

[13] J. Milnor, *Periodic orbits, externals rays and the Mandelbrot set: an expository account.* Géométrie complexe et systèmes dynamiques (Orsay, 1995). Astérisque No. 261 (2000), 277–333.

[14] J. Milnor, *Dynamics in one complex variable.* Third edition. Annals of Mathematics Studies, 160. Princeton University Press, Princeton, NJ, 2006.

[15] *The Online Encyclopedia of Integer Sequences.* `https://oeis.org/`.

[16] F. Wehrung, *Gerbes primitives.* C. R. Acad. Sci. Paris Sér. I Math. 313 (1991), no. 6, 357–362.

Email address: `biane@univ-mlv.fr`

Institut Gaspard-Monge, Université Paris-Est Marne-la-Vallée, 5 Boulevard Descartes, Champs-sur-Marne, 77454, Marne-la-Vallée cedex 2, France