André Sesboüé

Finite monogenic distributive systems

Czechoslovak Mathematical Journal, Vol. 46 (1996), No. 4, 697–719

Persistent URL: http://dml.cz/dmlcz/127328

Czechoslovak Mathematical Journal, 46 (121) 1996, Praha

FINITE MONOGENIC DISTRIBUTIVE SYSTEMS

ANDRÉ SESBOÜÉ, Caen

(Received October 3, 1994)

INTRODUCTION

This paper takes place in the context of non-associative systems. We study left self-distributive structures: this means the ones, called *LD-systems*, consisting of a set equipped with a binary operation satisfying the identity

$$\text{(LD)} \qquad x(yz) = (xy)(xz).$$

The importance of monogenic LD-systems has become apparent only in recent years. The fascinating connection between a free monogenerated LD-system $\mathfrak{a}$ and huge cardinals [10] has initiated an intensive study, which led to the discovery of a faithful realization of $\mathfrak{a}$ within the braid group B_∞ [2].

For any positive integers u and v let $(u)_v$ be the unique integer between 1 and v such that u is congruent to $(u)_v$ modulo v. For every k there exists a finite factor of $\mathfrak{a}$ on $\{1, \ldots, 2^k\}$ determined by $i \cdot 1 = (i+1)_{2^k}$, $1 \leqslant i \leqslant 2^k$. These LD-systems have been invented by Laver and they will be denoted here by $\mathfrak{p}_k$.

For a LD-system $\mathfrak{g}$ and an element x of $\mathfrak{g}$ let us define the sequence $(x_{[k]})_{k \geqslant 1}$ of *left powers* of x by $x_{[1]} = x$ and $x_{[k+1]} = x_{[k]}x$. Then $\mathfrak{p}_k$ happens to be the LD-system generated by the element 1 submitted to the relation $1_{[2^k+1]} = 1$ ([12]). In [4] and [12] it is shown that the LD-system $\mathfrak{p}_k$ has a property of periodicity: for each $1 \leqslant x \leqslant 2^k$ there exists an element $\nu_{2^k}(x)$ such that for all $1 \leqslant y \leqslant 2^k$, $xy = x \cdot (y)_{\nu_{2^k}(x)}$ and $\nu_{2^k}(x)$ divides 2^k.

It is not known whether there exists for any $i \geqslant 1$ a k big enough so that $1 \cdot i \neq 2^k$ in $\mathfrak{p}_k$. Laver [9] gave an affirmative solution assuming the existence of a non-trivial elementary embedding of a rank into itself, a very strong set theoretical assumption, while Dougherty and Jech [3] have shown that there is no proof within primitive recursive arithmetic.

The aim of this paper is to show that using three operators we can build a large family of finite monogenerated LD-systems (the *normal* LD-systems) from the $\mathfrak{p}_k$'s. We prove that these new LD-systems satisfy a similar periodicity property. The normal LD-systems are defined as a sub-family of the *left* LD-systems, which are the ones that are made exactly of all left powers of the generator. The generality of our construction has been made more obvious by the recent result of A. Drápal, who proved, after reading the first draft of this work, that all left LD-systems are normal [7].

This paper is organized as follow. The first three sections introduce the basic notions and results. In Section 4 we define the operators to work with and give examples of the way they behave. Section 5 defines the normal LD-systems and Section 6 is devoted to the main result.

1. LD-systems

For each element x of a finite LD-system the sequence of left powers of x is eventually periodic. More precisely, there exists a unique pair of positive integers (r, p) such that the powers $x, x_{[2]}, \ldots, x_{[r+p-1]}$ are distinct and for all $k \geqslant r+p$, we have $x_{[k]} = x_{[k']}$, where k' is the unique positive integer between r and $r+p-1$ such that $k' \equiv k \bmod(p)$.

Definition 1.1. Suppose that the set of the left powers of x is finite (which is certainly the case if the underlying LD-system is finite). The *return* $\varrho(x)$ is the least positive integer r such that there exists $k \geqslant 0$ satisfying $x_{[r+k]} = x_{[r]}$ and the *period* $\pi(x)$ of x is the least positive integer k satisfying $x_{[\varrho(x)+k]} = x_{[\varrho(x)]}$.

Proposition 1.2. *Let P and Q be two terms in one variable. Let $\mathfrak{g}$ be a monogenic LD-system and g a generator of $\mathfrak{g}$ such that $P(g) = Q(g)$. Then for all x in $\mathfrak{g}$, $P(x) = Q(x)$.*

Proof. By induction on the complexity of a one variable term T, it is easy to show that left distributivity implies that $xT(u)$ is $T(xu)$. Let X be the set of all x in $\mathfrak{g}$ such that $P(x) = Q(x)$. Then for all x, y in X we get $P(xy) = xP(y) = xQ(y) = Q(xy)$, so xy is still in X. The set X is a sub-LD-system of $\mathfrak{g}$. Moreover, g is in X, so X equals $\mathfrak{g}$. $\square$

In particular we deduce that two generators g and h of a monogenic LD-system satisfy the same equations and so there exists an automorphism φ such that $\varphi(g) = h$.

Proposition 1.3. *Let $\mathfrak{g}$ be a finite monogenic LD-system. Let g and h be two generators of $\mathfrak{g}$. Then the positive integers $\varrho(g)$, $\pi(g)$ are respectively equal to $\varrho(h)$, $\pi(h)$.*

So, for a monogenic LD-system we can speak, without any ambiguity, of the *return* and of the *period*.

Lemma 1.4. *Let $\mathfrak{g}$ be a finite monogenic LD-system and let g be a generator. If there exist a and b in $\mathfrak{g}$ such that $ab = g$ then the mapping L_a defined by $L_a(x) = ax$ is an automorphism of $\mathfrak{g}$.*

Proof. For each $x \in \mathfrak{g}$ the mapping L_x is an endomorphism by the left distributivity identity. Now, L_a is onto since for each x in $\mathfrak{g}$ there exists a term in one variable P such that x is $P(g)$. Therefore, we get $x = P(g) = P(ab) = aP(b)$. Since $\mathfrak{g}$ is finite, L_a is bijective. □

Definition 1.5. A *left* LD-system $\mathfrak{g}$ is a monogenic LD-system with generator g such that for each x in $\mathfrak{g}$ there exists $k \geqslant 1$ such that $x = g_{[k]}$.

When we look at the multiplication table of a left LD-system $\mathfrak{g}$ with the generator g as the first element of the table, left powers in g are the elements on the first column. If $\mathfrak{g}$ is a monogenic LD-system, saying that $\mathfrak{g}$ is a left LD-system is equivalent to saying that each element but perhaps the generator appears on the first column of the table of $\mathfrak{g}$. If $\mathfrak{g}$ has n elements then the elements of $\mathfrak{g}$ are exactly g, $g_{[2]}, \dots, g_{[n]}$.

Here are two examples of left LD-systems. They are defined on the set $\{1, \dots, 4\}$, 1 is a generator and the product is such that $x \cdot 1 = x + 1$ for $1 \leqslant x < 4$.

	1	2	3	4
1	2	2	2	2
2	3	2	3	2
3	4	2	2	2
4	3	2	3	2

Table 1

	1	2	3	4
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

Table 2

In Table 1 the return is 3 and in Table 2 the return is 1. In fact the second table is the table of the LD-system $\mathfrak{p}_2$.

2. Constant and stable elements

From now on we will use the following conventions: the underlying set of a left LD-system $\mathfrak{g}$ with cardinality n will be $\{1, \dots, n\}$, 1 will be a generator and $1_{[x]}$ will be equal to x for $1 \leqslant x \leqslant n$. Then the value of the return is $r = n \cdot 1$ and for all $x \in \{1, \dots, n - 1\}$ we have $x \cdot 1 = x + 1$.

Definition 2.1. Let $\mathfrak{g}$ be an LD-system. An element x of $\mathfrak{g}$ is *constant* if for each element y in $\mathfrak{g}$ we have $yx = xx$. If in addition x is idempotent then x is called *stable*.

On the table of an LD-system a constant element c corresponds to a constant column. In Table 1 the constant elements are 2 and 4 and 2 is stable. In Table 2 there is a unique constant 4 and it is also stable.

In [1], P. Dehornoy proves the following lemma.

Lemma 2.2. *Let $\mathfrak{g}$ be an LD-system and x, y, z be three elements of $\mathfrak{g}$. If y and z are elements of the sub-LD-system generated by x then there exists a positive integer r such that $yx^{[r]} = zx^{[r]}$.*

Using this lemma one can prove that each finite monogenic LD-system has at least one constant element. Notice that a generator cannot be a constant element (unless we are in the trivial cases of LD-systems with one or two elements). Considering the left LD-systems we have the following result.

Proposition 2.3. *A finite left LD-system $\mathfrak{g}$ with cardinality $n \geqslant 3$ has a unique stable element d and for each constant element c we have*

$$\begin{cases} xc = xd & \text{for all } x, \\ cx = dx & \text{for all } x \text{ distinct from } 1, \\ cx \neq 1 & \text{for all } x \text{ in } \{2, \dots, c\}. \end{cases}$$

P r o o f. For all x in $\mathfrak{g}$ let x^- be $x - 1$ if $2 \leqslant x \leqslant n$ and n if $x = 1$. Then we have

$$x^- \cdot 1 = \begin{cases} x & \text{if } 2 \leqslant x \leqslant n, \\ r & \text{if } x = 1. \end{cases}$$

Let us prove $cc = c'c'$ for any distinct constant elements c and c'. Since c and c' are not equal to 1, we have $c^- \cdot 1 = c$ and $c'^- \cdot 1 = c'$. Then we obtain $cc = c'^- c = c'^-(c^- \cdot 1) = c'^- c^- \cdot (c'^- \cdot 1) = c'^- c^- \cdot c' = c'c'$. Let d be cc. We claim that d is constant. For all x in $\mathfrak{g}$ we have $xd = x \cdot cc = xc \cdot xc = cc \cdot cc = dd$. From the preceding equality, the product dd must be equal to cc since c and d are two constant elements. So we have $dd = cc = d$. The element d is a constant element and idempotent, hence it is stable. Assume there exists an other stable element d'. Then d' is constant and we have $d' = d'd' = dd = d$. Now, if x is in $\mathfrak{g} \setminus \{1\}$ then there exist two elements u and v of $\mathfrak{g}$ such that $x = uv$. Then, we get

$$\begin{aligned} cx &= c \cdot uv = cu \cdot cv = (cu \cdot c)(cu \cdot v) = d(cu \cdot v) = (d \cdot cu) \cdot dv \\ &= (dc \cdot du) \cdot dv = (dd \cdot du) \cdot dv = d(du \cdot v) = (du \cdot d)(du \cdot v) \\ &= du \cdot dv = d \cdot uv = dx. \end{aligned}$$

To prove the last assertion we will suppose that there exists a u in $\{2, \ldots, c\}$ satisfying $cu = 1$ and show this leads to a contradiction. Under this hypothesis the morphism L_c is bijective by Lemma 1.4, therefore. u is a generator of $\mathfrak{g}$. Moreover, c is the unique constant, hence stable, element of $\mathfrak{g}$ (otherwise if c' were another constant element not equal to c we would have $cc = cc'$, which contradicts the fact that L_c is one to one). If u is equal to c then we have $1 = cc = c$ since c is stable and thus is idempotent. This is impossible since the LD-system $\mathfrak{g}$ has at least two elements. Now, assume $u < c$ and compute $c(u \cdot 1)$: $c(u \cdot 1) = cu \cdot (c \cdot 1) = 1(c \cdot 1) = (1 \cdot c)(1 \cdot 1) = c(1 \cdot 1) = c \cdot 2$. Since L_c is one to one, we get $u \cdot 1 = 2$, which implies either $u = n$ or $u = 1$. The two cases lead to a contradiction since if u is n then we have $n < c \leqslant n$ and if u is 1 then u does not belong to $\{2, \ldots, c\}$. $\square$

The last result of this section is the proof of the periodicity for constant elements.

Lemma 2.4. *Let c be the least constant of a left LD-system $\mathfrak{g}$ with cardinality $n \geqslant 3$. Then for each constant element c' and for each integer x satisfying $c \leqslant c+x \leqslant n$ we have*

$$c'(c + x) = \begin{cases} c'(x)_c & \text{if } (x)_c \neq 1, \\ c'(c \cdot 1) & \text{if } (x)_c = 1. \end{cases}$$

Proof. By the preceding proposition we have $cy = c'y$ for all $y \geqslant 2$. Since c is at least 2, it is enough to prove the lemma for c. Let d be the stable element of $\mathfrak{g}$. For $x = 0$ there is nothing to do since $(0)_c = c$. If we have $x = 1$ and $c + 1 \leqslant n$ then we obtain $(1)_c = 1$ and $c + 1 = c \cdot 1$. So, we obtain $c(c + 1) = c(c \cdot 1)$. Now, we proceed by an increasing induction on x. For $x = 2$ we have

$$\begin{aligned} c(c+2) &= d(c+2) = d((c \cdot 1) \cdot 1) = ((c \cdot 1) \cdot d) \cdot ((c \cdot 1) \cdot 1) \\ &= ((c \cdot 1) \cdot c) \cdot ((c \cdot 1) \cdot 1) = (c \cdot 1) \cdot (c \cdot 1) = c \cdot (1 \bullet 1) = c \cdot 2 = c(2)_c. \end{aligned}$$

Assume that the hypothesis is true for all $y \leqslant x < n - c$. We have $c(c + x + 1) = c((c + x) \cdot 1) = (c \cdot (c + x)) \cdot (c \cdot 1)$. If $(x)_c$ is strictly greater than 1 then we have $c(c + x + 1) = (c(x)_c) \cdot (c \cdot 1) = c((x)_c \cdot 1)$. If $(x)_c$ is c then $(x + 1)_c$ is 1 and we have $c(c + x + 1) = c(c \cdot 1)$. If $(x)_c$ is strictly between 1 and c then $(x)_c + 1$ equals $(x + 1)_c$ and we get $c(c + x + 1) = c((x)_c \cdot 1) = c((x)_c + 1) = c(x + 1)_c$. Now, for the case $(x)_c = 1$ we have $(x + 1)_c = 2$, therefore, $c(c + x + 1) = (c \cdot (c \cdot 1)) \cdot (c \cdot 1) = c((c \cdot 1) \cdot 1) = c(c + 2) = c(x + 1)_c$. $\square$

3. The congruence $\approx_{\mathfrak{g}}$

From Proposition 2.3 we have for all constant elements c and c' of a left LD-system $\mathfrak{g}$

$$\begin{cases} xc = xc' & \text{for all } x \text{ in } \mathfrak{g}, \\ cx = c'x & \text{for all } x \text{ in } \mathfrak{g} \setminus \{g\}, \end{cases}$$

where g is a generator of $\mathfrak{g}$. We define a relation which associates two elements of $\mathfrak{g}$ having the above property.

Definition 3.1. Let $\mathfrak{g}$ be a monogenic LD-system and g a generator of $\mathfrak{g}$. The relation $\approx_{\mathfrak{g}}$ is defined by

$$x \approx_{\mathfrak{g}} y \iff \begin{cases} kx = ky & \text{for all } k \text{ in } \mathfrak{g}, \\ xk = yk & \text{for all } k \text{ in } \mathfrak{g} \setminus \{g\}. \end{cases}$$

One can prove easily that this relation is an equivalence relation. Consider the two examples of section 1: in Table 1 the equivalence classes are $\{1\}$, $\{2, 4\}$ and $\{3\}$; in Table 2 all equivalence classes have a single element and the the relation $\approx_{\mathfrak{p}_2}$ is trivial. We will see that in the case of a left LD-system $\mathfrak{g}$ the relation $\approx_{\mathfrak{g}}$ is a congruence.

Definition 3.2. Let $\mathfrak{g}$ be a LD-system. For each x and y in $\mathfrak{g}$ for each integer $k \geqslant 0$ the *k-th left iterated product* of y by x, denoted by $\mathrm{L}^k(x, y)$, is defined by

$$\begin{cases} \mathrm{L}^0(x, y) = x, \\ \mathrm{L}^1(x, y) = xy, \\ \mathrm{L}^{k+1}(x, y) = \mathrm{L}^k(x, y)y. \end{cases}$$

Lemma 3.3. *Let $\mathfrak{g}$ be a left LD-system with cardinality $n \geqslant 3$. Let c be the least constant element of $\mathfrak{g}$.*

i) *If there exists an element $a \neq 1$ such that $a \approx_{\mathfrak{g}} 1$ then necessarily we have $a = n$, $n \cdot 1 = 2$ and $\{1, n\}$ is the unique non-trivial pair of the relation $\approx_{\mathfrak{g}}$.*

ii) *If we have $a \approx_{\mathfrak{g}} b$ and $a < b$ then we necessarily have $c \leqslant b$.*

P r o o f. i) Assume there exists an element $x \in \mathfrak{g} \setminus \{1\}$ such that $1 \approx_{\mathfrak{g}} x$. Let a be the least of those elements. We have the equalities $2 = 1 \cdot 1 = 1 \cdot a = aa = a \cdot 1$. Either a is n and the return of $\mathfrak{g}$ is equal to 2 or a is 1. This last case is impossible since by hypothesis a is distinct from 1. Let u and v be two elements in $\mathfrak{g}$ not equal to 1 and n such that $u \approx_{\mathfrak{g}} v$. We obtain $u \cdot 1 = un = vn = v \cdot 1$. The mapping which maps all elements x in $\mathfrak{g}$ onto $x \cdot 1$ is one-to-one on the subset $\{1, \ldots, n-1\}$, thus we have $u = v$.

ii) One can assume a, b minimal in their equivalence class with respect to $\approx_{\mathfrak{g}}$. Assume $a < b < c$. From Definition 3.2 it follows that $\mathrm{L}^k(x, 1)$ is the k-th successor of x (with respect to the order $<$). For all x we have $xa = xb$. Therefore, for all integers $k \geqslant 0$ we get $x\,\mathrm{L}^k(a, 1) = \mathrm{L}^k(xa, x \cdot 1) = \mathrm{L}^k(xb, x \cdot 1) = x\,\mathrm{L}^k(b, 1)$. We can pick k such that $\mathrm{L}^k(b, 1)$ equals c. Then for all x we have $x\,\mathrm{L}^k(a, 1) = xc$ and $\mathrm{L}^k(a, 1) < c$. So, $\mathrm{L}^k(a, 1)$ is a constant element of $\mathfrak{g}$ which contradicts the fact that c is the least such. □

Theorem 3.4. *Let $\mathfrak{g}$ be a finite left LD-system. Then the relation $\approx_{\mathfrak{g}}$ is a congruence.*

Proof. For $n \leqslant 2$ a direct computation from the table of $\mathfrak{g}$ gives the result. Assume $n \geqslant 3$. Let a, b, a', b' be elements of $\mathfrak{g}$ such that $a \approx_{\mathfrak{g}} b$ and $a' \approx_{\mathfrak{g}} b'$. For all $x \in \mathfrak{g}$ we have $x \cdot aa' = xa \cdot xa' = xb \cdot xb' = x \cdot a'b'$. If (a', b') is not equal to $(1, 1)$ then we have $aa' = ba' = bb'$. It remains to prove that $(a \cdot 1)x = (b \cdot 1)x$ for all $x \neq 1$. We show this by an increasing induction on x, assuming without loss of generality $a < b$. We get for $x = 2$

$$\begin{aligned}(a \cdot 1)2 &= (a \cdot 1)(1 \cdot 1) = (a \cdot 1)1 \cdot (a \cdot 1)1 = \mathrm{L}^2(a, 1) \cdot (a \cdot 1)1 \\ &= (\mathrm{L}^2(a, 1)a \cdot \mathrm{L}^2(a, 1)1) \cdot \mathrm{L}^2(a, 1)1 = (\mathrm{L}^2(a, 1)b \cdot \mathrm{L}^2(a, 1)1) \cdot \mathrm{L}^2(a, 1)1 \\ &= \mathrm{L}^2(a, 1) \cdot (b \cdot 1)1.\end{aligned}$$

From the preceding lemma we have $c \leqslant b$, where c is the least constant of $\mathfrak{g}$. There exists an integer h such that b is $\mathrm{L}^h(c, 1)$. We get

$$\begin{aligned}(a \cdot 1)2 &= \mathrm{L}^2(a, 1)(\mathrm{L}^h(c, 1)1 \cdot 1) = \mathrm{L}^2(a, 1)\,\mathrm{L}^{h+2}(c, 1) \\ &= \mathrm{L}^{h+2}\left(\mathrm{L}^2(a, 1)c, \mathrm{L}^2(a, 1)1\right) = \mathrm{L}^{h+2}\left(\mathrm{L}^2(a, 1)c, \mathrm{L}^3(a, 1)\right) \\ &= \mathrm{L}^{h+2}\left(\mathrm{L}^2(b, 1)c, \mathrm{L}^3(a, 1)\right).\end{aligned}$$

Since we have $xa = xb$ for all x for all integers $k \geqslant 0$ we get

$$x\,\mathrm{L}^k(a, 1) = \mathrm{L}^k(xa, x \cdot 1) = \mathrm{L}^k(xb, x \cdot 1) = x\,\mathrm{L}^k(b, 1).$$

We obtain

$$\begin{aligned}(a \cdot 1)2 &= \mathrm{L}^{h+2}\left(\mathrm{L}^2(b, 1)c, \mathrm{L}^3(b, 1)\right) = \mathrm{L}^{h+2}\left(\mathrm{L}^2(b, 1)c, \mathrm{L}^2(b, 1)1\right) \\ &= \mathrm{L}^2(b, 1)\,\mathrm{L}^{h+2}(c, 1) = \mathrm{L}^2(b, 1)(\mathrm{L}^h(c, 1)1 \cdot 1) \\ &= (b \cdot 1)1 \cdot (b \cdot 1)1 = (b \cdot 1)(1 \cdot 1) = (b \cdot 1)2.\end{aligned}$$

Assume $(a \cdot 1)x = (b \cdot 1)x$ and consider $(a \cdot 1)(x \cdot 1)$. We have

$$\begin{aligned}(a \cdot 1)(x \cdot 1) &= (a \cdot 1)x \cdot (a \cdot 1)1 = (b \cdot 1)x \cdot (a \cdot 1)1 \\ &= \Big(\big((b \cdot 1)x \cdot a\big) \cdot \big((b \cdot 1)x \cdot 1\big)\Big) \cdot \big((b \cdot 1)x \cdot 1\big) \\ &= \Big(\big((b \cdot 1)x \cdot b\big) \cdot \big((b \cdot 1)x \cdot 1\big)\Big) \cdot \big((b \cdot 1)x \cdot 1\big) \\ &= (b \cdot 1)x \cdot (b \cdot 1)1 = (b \cdot 1)(x \cdot 1).\end{aligned}$$

This shows $a \cdot 1 \approx_{\mathfrak{g}} b \cdot 1$, hence the relation $\approx_{\mathfrak{g}}$ is a congruence. □

4. The operators B, R, S

This section consist of technical results. We begin to define methods which are used to obtain new LD-systems from an LD-system $\mathfrak{g}$. From these methods we define the operators B, R and S and prove that they transform a left LD-system into another left LD-system. Throughout this section n will be a fixed integer at least equal to 2.

The first method, called the repetition method, consists in adding a new element to $\mathfrak{g}$. More precisely it consists in adding the new element $n+1$ in the table of $\mathfrak{g}$ by copying the row and the column number $p \cdot 1$ at the row and column number $n+1$ as well as replacing the value $p \cdot 1$ by the new value $n+1$.

Definition 4.1. For all p between 2 and n, the *p-repetition* of $\mathfrak{g}$ is the structure $E_p(\mathfrak{g})$ of underlying set $\{1, \ldots, n+1\}$ with the product defined by

$$x * y = \begin{cases} \varphi_p(x)\varphi_p(y) & \text{if } (x, y) \neq (p, 1) \\ n+1 & \text{if } (x, y) = (p, 1) \end{cases}$$

where $\varphi_p(x)$ is x for $x \leqslant n$ and $\varphi_p(n+1)$ is $p \cdot 1$.

Lemma 4.2. *If the LD-system $\mathfrak{g}$ satisfies $1 \notin \mathfrak{g} \cdot \mathfrak{g}$ then all p-repetitions of $\mathfrak{g}$ are LD-systems.*

P r o o f. The mapping φ_p is clearly an homomorphism from $E_p(\mathfrak{g})$ to $\mathfrak{g}$. Its kernel contains only one non-trivial class, namely $\{p \cdot 1, n+1\}$. As $(p, 1)$ is the only pair (x, y) with $x * y = n+1$ and as 1 is never of the form $x * y$ we see that $n+1$ equals neither $x * (y * z)$ nor $(x * y) * (x * z)$ for any x, y, $z \in E_p(\mathfrak{g})$. □

The next method will change a value on the first column.

Definition 4.3. Let $a \neq 1$, $b \neq 1$, $e \neq 1$ be elements of $\mathfrak{g}$ such that $e \cdot 1 = a$ and $a \approx_{\mathfrak{g}} b$. We denote by $M_{a,b,e}(\mathfrak{g})$ the structure consisting of the set $\{1, \ldots, n\}$ and the product defined by

$$x * y = \begin{cases} xy & \text{if } (x,y) \neq (e,1), \\ b & \text{if } (x,y) = (e,1). \end{cases}$$

Lemma 4.4. *If in the LD-system $\mathfrak{g}$ we have $1 \notin \mathfrak{g} \cdot \mathfrak{g}$ then the structure $M_{a,b,e}(\mathfrak{g})$ is an LD-system.*

Proof. In $M_{a,b,e}(\mathfrak{g})$ the element 1 is never of the form $x * y$, as a consequence, the products $x * (y * z)$ or $(x * y) * (x * z)$ are never of the form $u * 1$. Using this fact, by checking all cases when one or more of the couples (x, y), (x, z), (y, z) equals $(e, 1)$, one can see that in $M_{a,b,e}(\mathfrak{g})$ $x * (y * z) = (x * y) * (x * z)$ holds. □

The last method will change the value of all products xy for $y \neq 1$.

Definition 4.5. Let $a \neq 1$ and b be elements of $\mathfrak{g}$ such that $a \approx_{\mathfrak{g}} b$. We denote by $M'_{a,b}(\mathfrak{g})$ the structure consisting of the set $\{1, \ldots, n\}$ and the product defined by

$$x * y = \begin{cases} \psi_{a,b}(xy) & \text{if } y \neq 1, \\ xy & \text{if } y = 1, \end{cases}$$

where $\psi_{a,b}(x)$ is x if x is not a and $\psi_{a,b}(a)$ is b.

Lemma 4.6. *If in the LD-system $\mathfrak{g}$ we have $1 \notin \mathfrak{g} \cdot \mathfrak{g}$ then the structure $M'_{a,b}(\mathfrak{g})$ is an LD-system.*

Proof. If a product uv equals a then for all $w \in \mathfrak{g}$ we get $w\psi_{a,b}(uv) = w \cdot uv$ and for all $w' \neq 1$ we get $\psi_{a,b}(uv)w' = uv \cdot w'$. Using this and computing the products $x * (y * z)$ and $(x * y) * (x * z)$, when y or z is 1, one can see that in $M'_{a,b}(\mathfrak{g})$ we have $x * (y * z) = (x * y) * (x * z)$. □

Starting with a monogenic LD-system and applying these three different methods we do not necessarily obtain a monogenic LD-system. But, if we consider the left LD-systems and particular values of these parameters (*e.g* in $E_p(g)$ take $p = n$) we do obtain left LD-systems.

Definition 4.7. Let $\mathfrak{g}$ be a left LD-system. Assume $\mathfrak{g}$ satisfies $1 \notin \mathfrak{g} \cdot (\mathfrak{g} \setminus \{1\})$. For $r \neq 1$, we define $B(\mathfrak{g})$ by $B(\mathfrak{g}) = M'_{r,n+1}(E_n(\mathfrak{g}))$. For $r = 1$, $B(\mathfrak{g})$ is the structure consisting of the set $\{1, \ldots, n+1\}$ with the product defined by

$$x * y = \begin{cases} \varphi_n(x)\varphi_n(y) & \text{if } (x,y) \notin \{(n,1),(n,n+1)\}, \\ n+1 & \text{if } (x,y) \in \{(n,1),(n,n+1)\}, \end{cases}$$

where φ_n is the same mapping as in Definition 4.1.

In fact the operator B adds the new element $n+1$ to $\mathfrak{g}$, copies the value of the column and the row $r = n \cdot 1$ to the column and row $n+1$. It also gives the new value $n+1$ to the product $n \cdot 1$ and changes the value of the products xy, $y \neq 1$, equal to r, to the new value $n+1$. As an example assume $\mathfrak{g}$ is like in Table 1. In $\mathfrak{g}$, n is 4 and r is 3. We add the new element 5. We copy the column and the row 3 to the column and the row 5. We change the value of $4 \cdot 1$ equal to 3 in 5 and we change all products xy, $y \neq 1$, equal to 3 in 5. So, we obtain the structure $B(\mathfrak{g})$ of table

	1	2	3	4	5
1	2	2	2	2	2
2	3	2	5	2	5
3	4	2	2	2	2
4	5	2	5	2	5
5	4	2	2	2	2

Table 3

Lemma 4.8. *Assume $\mathfrak{g}$ is a left LD-system, with cardinality n, satisfying $1 \notin \mathfrak{g} \cdot (\mathfrak{g} \setminus \{1\})$. The structure $B(\mathfrak{g})$ is a left LD-system with cardinality $n+1$ and it has return $r+1$ if $r < n$ or r if $r = n$.*

Proof. In both cases, if $B(\mathfrak{g})$ is a LD-system then it is a left one since we added a new element $n+1$ such that $n * 1 = n+1$ and for each x between 1 and $n-1$ we have $x * 1 = x \cdot 1 = x+1$. Also by construction, the return will be $r+1$ if r is not n and equals to n otherwise. If r is not 1 we have $1 \notin \mathfrak{g} \cdot \mathfrak{g}$. Then Lemmas 4.2 and 4.6 imply that $B(\mathfrak{g})$ is a LD-system since by construction we have $r \approx_{E_n(\mathfrak{g})} n+1$. Now if r equals 1, $\mathfrak{g}$ is the LD-system $\mathfrak{p}_k$ for an integer k. By construction we have $1 \approx_{B(\mathfrak{p}_k)} n+1$ and $1 \notin B(\mathfrak{p}_k) * B(\mathfrak{p}_k)$. The mapping φ_n is an homomorphism from $B(\mathfrak{p}_k)$ to $\mathfrak{p}_k$ of kernel $\{1, n+1\}$. The only possibility that a product $x * (y * z)$ equals $n+1$ is when we have $x = n$, $y * z = n+1$. For a product $(x * y) * (x * z)$, the only possibility it equals 1, is when we have $x * y = n$, $x * z = n+1$. Checking the different cases we obtain that $B(\mathfrak{p}_k)$ satisfies the LD-law. $\square$

Definition 4.9. Let $\mathfrak{g}$ be a left LD-system. For all s such that $s \approx_{\mathfrak{g}} r$, $R_s(\mathfrak{g})$ is the LD-system $M_{r,s,n}(\mathfrak{g})$.

In this LD-system the only change made by the operator R is the value of the return, which from r becomes s where s is in the equivalence class of r with respect to the relation $\approx_{\mathfrak{g}}$. Taking the previous LD-system $B(\mathfrak{g})$ (i.e. Table 3), the return is 4 and its equivalence class with respect to the relation $\approx_{B(\mathfrak{g})}$ is $\{2, 4\}$. Then taking $s = 2$ we obtain the new structure $R_2(B(\mathfrak{g}))$ in which the only change is the value of the return which now equals 2.

	1	2	3	4	5
1	2	2	2	2	2
2	3	2	5	2	5
3	4	2	2	2	2
4	5	2	5	2	5
5	2	2	2	2	2

Table 4

Lemma 4.10. *Assume $\mathfrak{g}$ satisfies $1 \notin \mathfrak{g} \cdot \mathfrak{g}$. The structure $R_s(\mathfrak{g})$ is a left LD-system with return s.*

Proof. The structure $R_s(\mathfrak{g})$ is a LD-system by Lemma 4.4 and it is a left one since by construction we have $x * 1 = x \cdot 1 = x + 1$ for each $1 \leqslant x < n$. Also by construction $n * 1 = s$, hence the return of $R_s(\mathfrak{g})$ is s. $\square$

Definition 4.11. Let $\mathfrak{g}$ be a left LD-system with cardinality n.

i) A *selector* for the congruence $\approx_{\mathfrak{g}}$ is a set P such that for each $x \in \mathfrak{g}$ there exists a unique $y \in \overline{x}$ such that $\overline{x} \cap P = \{y\}$, where $\overline{x}$ denotes the equivalence class of x.

ii) For P a selector for $\approx_{\mathfrak{g}}$, the structure $S_P(\mathfrak{g})$ is the successive application of the modification M'_{a,b_a} where a is in $\mathfrak{g}$ and $\overline{a} \cap P = \{b_a\}$, thus we have

$$S_P(\mathfrak{g}) = \left(\prod_{a \in \mathfrak{g}} M'_{a,b_a} \right) (\mathfrak{g})$$

(the product used here denotes the successive use of the modification M').

This operator replaces the value of all products xy, $y \neq 1$, by a new value that is equivalent with respect to $\approx_{\mathfrak{g}}$. In the table of the LD-system $R_2(B(\mathfrak{g}))$ (i.e. Table 4) the equivalence classes are $\{1\}$, $\{2, 4\}$ and $\{3, 5\}$. If we take the selector $P = \{1, 4, 3\}$ then we obtain a new structure $S_P(R_2(B(\mathfrak{g})))$ in which the value of the products xy, $y \neq 1$, has been changed.

	1	2	3	4	5
1	2	4	4	4	4
2	3	4	3	4	3
3	4	4	4	4	4
4	5	4	3	4	3
5	2	4	4	4	4

Table 5

Lemma 4.12. *Assume that $\mathfrak{g}$ satisfies $1 \notin \mathfrak{g} \cdot \mathfrak{g}$. The operator S_P does not depend on the choice of the order to enumerate the selector P.*

Proof. If a belongs to P then $M'_{a,a}(\mathfrak{g})$ is $\mathfrak{g}$ since $\psi_{a,a}$ is the identity. The modification $M'_{a,u}$, with $a \approx_{\mathfrak{g}} u$, changes only the products xy, $y \neq 1$, which equal a. Let a, b be in $\mathfrak{g}$ and u, v be in P such that $a \approx_{\mathfrak{g}} u$ and $b \approx_{\mathfrak{g}} v$. If we have $a \neq v$ and $b \neq u$ then for all x, y in $M'_{a,u}\left(M'_{b,v}(\mathfrak{g})\right)$ we get

$$x * y = \begin{cases} xy & \text{if } y = 1 \text{ or } xy \neq b \text{ or } xy \neq a, \\ v & \text{if } xy = b, \\ u & \text{if } xy = a, \end{cases}$$

and for all x, y in $M'_{b,v}\left(M'_{a,u}(\mathfrak{g})\right)$ we get

$$x \bullet y = \begin{cases} xy & \text{if } y = 1 \text{ or } xy \neq a \text{ or } xy \neq b, \\ u & \text{if } xy = a, \\ v & \text{if } xy = b. \end{cases}$$

Then we have $M'_{a,u} \circ M'_{b,v} = M'_{b,v} \circ M'_{a,u}$. If we have $a = v$ or $b = u$ then u equals v. We get $M'_{a,u}\left(M'_{b,v}(\mathfrak{g})\right) = M'_{a,u}\left(M'_{u,u}(\mathfrak{g})\right) = M'_{a,v}(\mathfrak{g})$ and $M'_{a,u}\left(M'_{b,v}(\mathfrak{g})\right) = M'_{v,v}\left(M'_{b,v}(\mathfrak{g})\right) = M'_{b,v}(\mathfrak{g})$. ☐

Lemma 4.13. *For every selector P of $\approx_{\mathfrak{g}}$, the structure $S_P(\mathfrak{g})$ is a left LD-system with the same underlying set and the same return as $\mathfrak{g}$*

Proof. Lemma 4.6. implies that $S_P(\mathfrak{g})$ is a LD-system. Moreover it is a left LD-system since by construction the first column does not change. ☐

Remark 4.14. If we have $1 \approx_{\mathfrak{g}} n$, then Lemma 3.3 implies that $\{1, n\}$ is the only non-trivial pair of $\approx_{\mathfrak{g}}$. If P is $\{1, 2, \dots, n-1\}$ then all equivalence classes of $\approx_{S_P(\mathfrak{g})}$ are trivial since the generator 1 belongs to the image of one of the endomorphisms L_x, which is, therefore, an automorphism.

5. The normal LD-systems

We now introduce the family of LD-systems to be used in the sequel. This family is a subfamily of the left LD-systems defined using the constant elements and the congruence $\approx_{\mathfrak{g}}$. Let $\mathfrak{g}$ be a monogenic LD-system of underlying set $\{1, \dots, n\}$ with 1 as a generator. For $a \in \mathfrak{g}$, denote the kernel of L_a by $\approx_a$. It is straightforward that $x \approx_{\mathfrak{g}} y$ implies $x \approx_a y$ for all a in $\mathfrak{g}$. The experimental study of left LD-systems of small cardinality ($\leqslant 7$) shows some periodicity phenomenons. In these examples the least constant c is a power of 2 and either there is a unique constant c satisfying $c(c \cdot 1) = 1$ (1 is a generator) or there are some constant elements such that one of them c' satisfies $c'(c' \cdot 1) = c' \cdot 1$. Moreover, the congruences $\approx_c$ and $\approx_{\mathfrak{g}}$ are either identical or they coincide only on the subset $\{2, \dots, n\}$ of $\mathfrak{g}$. This leads to the following definition.

Definition 5.1. A left LD-system $\mathfrak{g}$ with cardinality n is *normal* if

i) there exists a constant element c' such that $c'(c' \cdot 1)$ is either $c' \cdot 1$ or 1 and

ii) the congruence $\approx_{\mathfrak{g}}$ coincides with the congruence $\approx_c$ on the subset $\{2, \dots, n\}$, i.e. for all x, y in $\{2, \dots, n\}$ $x \approx_c y$ is equivalent to $x \approx_{\mathfrak{g}} y$, where c is the least constant element of $\mathfrak{g}$.

It is easy to see that the LD-systems $\mathfrak{p}_k$ are normal as well as the three monogenic LD-systems of cardinality 2 which are

$\mathfrak{p}_1$	1	2
1	2	2
2	1	2

$\mathfrak{t}$	1	2
1	2	2
2	2	2

$\mathfrak{t}'$	1	2
1	2	1
2	2	1

We now give some properties of the normal LD-systems and prove that there exist only four kinds of normal LD-systems.

Lemma 5.2. *Let $\mathfrak{g}$ be a normal LD-system with cardinality $n \geqslant 3$. Let c be the least constant of $\mathfrak{g}$. Then for all $2 \leqslant z < z' \leqslant c$ we have $cz \neq cz'$.*

P r o o f. Assume $cz = cz'$, we have $z \approx_c z'$ and, since $\mathfrak{g}$ is normal, $z \approx_{\mathfrak{g}} z'$. By Lemma 3.3, we get $c \leqslant z'$. So, we obtain $c = z'$ and hence $z \approx_{\mathfrak{g}} c$. This implies $xz = xc = cc$ for all x in $\mathfrak{g}$. Thus, z is a constant element strictly less than c, which contradicts the fact that c is the least constant. $\square$

Lemma 5.3. *Let $\mathfrak{g}$ be a left LD-system with cardinality $n \geqslant 3$. If in $\mathfrak{g}$ a constant c satisfies $c(c \cdot 1) = 1$ then $\mathfrak{g}$ is a normal LD-system, c is unique and either $c \cdot 1 = 1$ or $c \cdot 1 = n$ holds.*

P r o o f. In this case the mapping L_c is one to one by Lemma 1.4. Therefore, c is the unique constant, hence it is stable, and the congruence $\approx_{\mathfrak{g}}$ is trivial. The two congruences $\approx_{\mathfrak{g}}$ and $\approx_c$ are identical. Compute $c((c\cdot 1)1)$: $c((c\cdot 1)1) = c(c\cdot 1)\cdot(c\cdot 1) = 1(c\cdot 1) = (1\cdot c)(1\cdot 1) = c(1\cdot 1)$. The injectivity of L_c gives $(c\cdot 1)1 = 1\cdot 1$. Therefore, either $c \cdot 1 = 1$ or $c \cdot 1 = n$. $\square$

Remark 5.4. If for some element x of $\mathfrak{g}$ we have $x \cdot 1 = 1$ then, from [4] and [12], $\mathfrak{g}$ is a LD-system $\mathfrak{p}_m$ for some integer m. If we have $c(c \cdot 1) = 1$ and $c \cdot 1 = n$ then the return of $\mathfrak{g}$ is 2.

Lemma 5.5. *Let $\mathfrak{g}$ be a normal LD-system with cardinality $n \geqslant 3$. Let c be the least constant of $\mathfrak{g}$. If c is n then $\mathfrak{g}$ is the LD-system $\mathfrak{p}_m$ for some integer m.*

Proof. If c is n, with $n \geqslant 3$, necessarily it is the unique constant element, hence it is stable. The mapping L_n is one-to-one on $\mathfrak{g} \setminus \{1\}$. We have $n \cdot 2 = n(1 \cdot 1) = (n \cdot 1)(n \cdot 1) = (n \cdot 1)n \cdot (n \cdot 1)1 = n \cdot (n \cdot 1)1$. Thus $(n \cdot 1)1 = 1 \cdot 1$ which implies either $n \cdot 1 = 1$ or $n \cdot 1 = n$. In the first case $\mathfrak{g}$ is a LD-system $\mathfrak{p}_m$ for an integer m. In the second case we obtain $2 = (n \cdot 1)1 = n \cdot 1 = n$, so the cardinality of $\mathfrak{g}$ is 2 which is impossible. □

Proposition 5.6. *Each normal LD-system $\mathfrak{g}$ is of one and only one of the following types:*

- *type 1: either the least constant c satisfies $c \cdot 1 = 1$ or we have $c(c \cdot 1) = 1$ and $c \cdot 1 = n$;*
- *type 2: c is the unique constant (thus stable) element, satisfies $c \cdot 1 = n$ and we have $c(c \cdot 1) \neq 1$;*
- *type 3: c is the unique constant (thus stable) element and we have $1 < c \cdot 1 < n$;*
- *type 4: there exists at least one other constant c' not equal to c.*

Proof. Since the four types cover all different values of $c \cdot 1$, each normal LD-system is of one of the four types. Let n be the cardinality of $\mathfrak{g}$. For $n = 2$ we see that the LD-systems $\mathfrak{p}_1$ and $\mathfrak{t}'$ are of type 1 and the LD-system $\mathfrak{t}$ is of type 4. Now, assume that n is greater than 2. If $c(c \cdot 1) = 1$, using Lemma 5.3, c is the unique constant. So, in type 1, 2 and 3 there is a unique constant, thus they are distinct from type 4. Now, one can see easily that type 1, 2 and 3 are distinct. □

Proposition 5.7. *Let $\mathfrak{g}$ be a normal LD-system of cardinality n. Let c be the least constant of $\mathfrak{g}$.*

i) *If $\mathfrak{g}$ has type 2 then the congruences $\approx_{\mathfrak{g}}$ and $\approx_c$ coincide.*

ii) *If $\mathfrak{g}$ has type 3 the class of 1 with respect to the congruence $\approx_{\mathfrak{g}}$ is $\{1\}$.*

iii) *If $\mathfrak{g}$ has type 4 then the congruence $\approx_{\mathfrak{g}}$ coincides with the congruence $\approx_{c'}$ for all constant element c' such that $c'(c' \cdot 1) \neq c' \cdot 1$, except for the LD-system $\mathfrak{t}$ where $\approx_{\mathfrak{t}}$, $\approx_1$ and $\approx_2$ are identical.*

Proof. i) Since none of the LD-systems of cardinality 2 has type 2, we can assume $n \geqslant 3$. By definition c is unique, thus stable, and we have $c = n$ or $c = n - 1$ We cannot have $c = n$ by Lemma 5.5. So, let $c = n - 1$ By definition the congruences $\approx_{\mathfrak{g}}$ and $\approx_c$ coincide on the subset $\{2, \ldots, n\}$ and the mapping L_c is one-to-one on the subset $\{2, \ldots, c\}$ (Lemma 5.2). Thus for all $1 < x < y < n$, we have $cx \neq cy$ hence $x \not\approx_{\mathfrak{g}} y$. Since we have $c \cdot 1 = n$ and $c \cdot 1 = c(c \cdot 1)$ we only need to prove that $1 \approx_c n$ implies $1 \approx_{\mathfrak{g}} n$, the converse beeing true by definition of $\approx_{\mathfrak{g}}$. Let us prove that the return $r = n \cdot 1$ is 2. It cannot be 1 otherwise, using Remark 5.4, $\mathfrak{g}$ would be of type 1. We have $c \cdot 2 = c(1 \cdot 1) = (c \cdot 1)(c \cdot 1) = (c \cdot 1)c \cdot (c \cdot 1)1 = c \cdot (c \cdot 1)1 = c(n \cdot 1) = cr$. If $r = n$ we have $c \cdot 2 = cn = c(c \cdot 1) = c \cdot 1 = n$. Since $r = n \cdot 1$ we have $n \cdot 1 = n$ and we obtain $n \cdot 2 = n(1 \cdot 1) = (n \cdot 1)(n \cdot 1) = nn = (c \cdot 1)(c \cdot 1) = c(1 \cdot 1) = c \cdot 2 = n$. An easy computation shows that $nx = n$ for all x in $\mathfrak{g}$ and we obtain $nc = c = n - 1$, which is a contradiction. Therefore, r is always 2 and this implies for all x in $\mathfrak{g}$ that $1 \cdot x = nx$. Using Proposition 2.3, for all x in $\{2, \dots, c\}$ we have $cx \neq 1$. We now prove that for all $2 \leqslant x \leqslant c$ we have $cx \neq n$. Assume the converse is true, then x is not equal to c since $cc = c \notin \{1, n\}$. We have $x \cdot 1 = x + 1 > 2$ and $c(x \cdot 1) = cx \cdot (c \cdot 1) = n(c \cdot 1) = (c \cdot 1)(c \cdot 1) = c(1 \cdot 1) = c \cdot 2$. The injectivity of L_c on $\{2, \dots, c\}$ gives $x \cdot 1 = 2$ which is a contradiction. Now, a decreasing induction on x, taken between c and 2, shows that $cx = x$. We now prove that $x \cdot 1 = xn$ for all x in $\mathfrak{g}$. We get $xn = x(c \cdot 1) = xc \cdot (x \cdot 1) = c(x \cdot 1)$ thus

$$xn = \begin{cases} x \cdot 1 & \text{if } x < c, \\ c(c \cdot 1) = c \cdot 1 & \text{if } x = c, \\ c(n \cdot 1) = c(1 \cdot 1) = 1 \cdot 1 & \text{if } x = n. \end{cases}$$

ii) Here we can also assume $n \geqslant 3$. Assume there exists an element $x \neq 1$ satisfying $1 \approx_{\mathfrak{g}} x$. Using Lemma 3.3, $x = n$ and this is the only non-trivial pair of $\approx_{\mathfrak{g}}$. This implies that the LD-system $\mathfrak{g}$ has a unique constant (thus stable) c. By definition the congruences $\approx_c$ and $\approx_{\mathfrak{g}}$ coincide on $\{2, \dots, n\}$. If c is n then we have $n \cdot 1 = nn = n$. So, $\mathfrak{g}$ has type 2. If $c \leqslant n - 2$, since $c \cdot 1$ is strictly less than n, we have $(c \cdot 1)1 = c+2 \leqslant n$. We obtain $c \cdot 2 = c(1 \cdot 1) = (c \cdot 1)(c \cdot 1) = (c \cdot 1)c \cdot (c \cdot 1)1 = c \cdot (c \cdot 1)1 = c(c+2)$, then $2 \approx_c c + 2$ which also gives $2 \approx_{\mathfrak{g}} c + 2$ and this is a contradiction. Now, if c is $n - 1$ then we get $c \cdot 1 = c + 1 = n$ and $\mathfrak{g}$ has type 2.

iii) Assume $n \geqslant 3$. If $\mathfrak{g}$ has type 4 the equivalence class of 1 with respect to $\approx_{\mathfrak{g}}$ is trivial, otherwise using Lemma 3.3 there is a unique constant. Let d be the stable of $\mathfrak{g}$. We show that $c'k \neq c' \cdot 1$ for all $k \geqslant 2$. Assume it is not true, then, using Lemma 2.4, pick k between 2 and $c + 1$. If k is $c + 1$ then k is $c \cdot 1$ and we have $c'(c \cdot 1) = c'c \cdot (c' \cdot 1) = c'c' \cdot (c' \cdot 1) = c'(c' \cdot 1)$ wich is a contradiction. If k is c then we have $c' \cdot 1 = c'c = c'c' = d$ and $c'(c' \cdot 1) = c'c' \cdot (c' \cdot 1) = (c' \cdot 1)(c' \cdot 1) = dd = d = c' \cdot 1$ which is also a contradiction. Now if k is in $\{2, \dots, c - 1\}$ then we get $2 < k \cdot 1 \leqslant c$ and $c'(k \cdot 1) = c'k \cdot (c' \cdot 1) = (c' \cdot 1)(c' \cdot 1) = c'(1 \cdot 1) = c' \cdot 2$. Since $c' \approx_{\mathfrak{g}} c$ we also have $c(k \cdot 1) = c \cdot 2$, which contradicts the injectivity of L_c on $\{2, \dots, c\}$. This proves that the equivalence class of 1 for $\approx_{c'}$ is trivial. Now, since all constant elements are in the same equivalence class for $\approx_{\mathfrak{g}}$, the congruences $\approx_{\mathfrak{g}}$ and $\approx_{c'}$ coincide on $\mathfrak{g} \setminus \{1\}$. Therefore, they coincide everywhere. $\square$

The aim of this section is to prove the following:

Theorem 6.1. i) *The normal LD-systems of type 1 are exactly the LD-systems $\mathfrak{p}_n$ and the LD-systems $S_P(B(\mathfrak{p}_n))$ with $P = \{1, 2, \dots, 2^n - 1\}$.*

ii) *The normal LD-systems of type 2 are exactly the LD-systems $B(\mathfrak{p}_n)$.*

iii) *The normal LD-systems of type 3 are exactly the LD-systems $R_r\big(S_P\big(B^d(\mathfrak{p}_n)\big)\big)$ with $d < 2^n$, P a selector for $\approx_{B^d(\mathfrak{p}_n)}$ and r in the equivalence class of the return of $B^d(\mathfrak{p}_n)$.*

iv) *The normal LD-systems of type 4 with cardinality greater than 2 are exactly the LD-systems $R_r\big(S_P\big(B^d(\mathfrak{p}_n)\big)\big)$ with $d \geqslant 2^n$, P a selector for $\approx_{B^d(\mathfrak{p}_n)}$ and r in the equivalence class of the return of $B^d(\mathfrak{p}_n)$. For cardinality 2, $\mathfrak{t}$ is the only possible LD-system (i.e. $\mathfrak{t} = B(\mathfrak{p}_0)$).*

In each case the values of r, P and d are uniquely determined.

We first study the congruence $\approx_{\mathfrak{g}}$ in the LD-systems $B(\mathfrak{g})$, $R_s(\mathfrak{g})$ and $S_P(\mathfrak{g})$.

Lemma 6.2. *Let $\mathfrak{g}$ be a left LD-system with cardinality $n \geqslant 2$. If in $\mathfrak{g}$ we have $1 \approx_{\mathfrak{g}} n$ or $r = 1$ then in $B(\mathfrak{g})$, $\{r, n+1\}$ is the only non-trivial pair of $\approx_{B(g)}$, otherwise $a \approx_{\mathfrak{g}} b$ implies $a \approx_{B(\mathfrak{g})} b$ and we have $r \approx_{B(\mathfrak{g})} n+1$.*

Proof. Let $\mathfrak{g}' = B(\mathfrak{g})$. We use the notation of Section 4. By construction we have $r \approx_{\mathfrak{g}'} n+1$. Let us consider the other elements of $\mathfrak{g}'$. Assume first $1 \not\approx_{\mathfrak{g}} n$ and $r \neq 1$. Let a, b be two elements of $\mathfrak{g}'$ satisfying $a \approx_{\mathfrak{g}} b$ and both neither equal to 1 nor to $n+1$. Let x in $\mathfrak{g}'$, we have $x * a = \psi_{r,n}(\varphi_n(x)\varphi_n(a)) = \psi_{r,n}(xa) = \psi_{r,n}(xb) = \psi_{r,n}(\varphi_n(x)\varphi_n(b)) = x * b$. Let x in $\mathfrak{g}' \setminus \{1\}$, we have $a * x = \psi_{r,n}(\varphi_n(a)\varphi_n(x)) = \psi_{r,n}(ax) = \psi_{r,n}(bx) = \psi_{r,n}(\varphi_n(b)\varphi_n(x)) = b * x$. Thus, $a \approx_{\mathfrak{g}'} b$. Now, if $\{1, n\}$ is the only non-trivial pair of $\approx_{\mathfrak{g}}$ then let a, b be such that $\{a, b\} \cap \{1, n\} = \emptyset$. We have $a = b$ and $a \approx_{\mathfrak{g}'} b$. For the equivalence class of 1, we get by construction $n * 1 = n+1$ and $n * n = n$. Thus, we have two distinct equivalent classes $\overline{1} = \{1\}$ and $\overline{n} = \{n\}$. If r is 1 then all the equivalence classes of $\approx_{\mathfrak{g}}$ are trivial and if $a \approx_{\mathfrak{g}} b$ we have $a = b$ so $a \approx_{\mathfrak{g}'} b$. □

Lemma 6.3. *Let $\mathfrak{g}$ be a left LD-system with cardinality n and return not equal to 1.*

i) *If $\mathfrak{g}$ is different from $\mathfrak{t}$ the congruences $\approx_{\mathfrak{g}}$ and $\approx_{R_s(\mathfrak{g})}$ coincide. If $\mathfrak{g}$ is $\mathfrak{t}$ then $\approx_{R_1(\mathfrak{t})}$ is trivial.*

ii) *If $1 \approx_{\mathfrak{g}} n$ holds and P is $\{1, \dots, n-1\}$ the equivalence classes of $\approx_{S_P(\mathfrak{g})}$ are trivial. Otherwise, the congruences $\approx_{\mathfrak{g}}$ and $\approx_{S_P(\mathfrak{g})}$ coincide.*

P r o o f. This comes from the definition of the operators. They only act on elements of the same equivalence class. Let $\mathfrak{g}' = R_s(\mathfrak{g})$ and $\mathfrak{g}'' = S_P(\mathfrak{g})$. Denote by $*$ the product of $\mathfrak{g}'$ and $\bullet$ the one of $\mathfrak{g}''$. We use the notation of Section 4.

i) If $\mathfrak{g}$ is $\mathfrak{t}$ then $R_1(\mathfrak{t})$ is $\mathfrak{p}_1$ and $\approx_{\mathfrak{p}_1}$ is trivial. Now let n be greater than 2. The LD-systems $\mathfrak{g}'$ and $\mathfrak{g}$ only differ from the value of the return. This return was substituted with an element of its equivalence class with respect to $\approx_{\mathfrak{g}}$. Let x and y satisfying $x \approx_{\mathfrak{g}} y$. For all $z \neq 1$ we have $x * z = xz = yz = y * z$. If $z \neq n$ we have $z * x = zx = zy = z * y$ and if neither x nor y is 1 we get for n, $n * x = nx = ny = n * y$. If x is 1 then there are two cases. Either y is also 1 and we get $n * x = n * 1 = n * y$ or (Lemma 3.3) y is n and the only non-trivial pair of $\approx_{\mathfrak{g}}$ is $\{1, n\}$. The return r is 2, hence its equivalence class for $\approx_{\mathfrak{g}}$ is $\{2\}$ and the LD-system $\mathfrak{g}'$ is $\mathfrak{g}$. In each case the equivalence classes of $\approx_{\mathfrak{g}}$ and $\approx_{\mathfrak{g}'}$ are equal.

ii) For $\mathfrak{g}''$, if $1 \not\approx_{\mathfrak{g}} n$ for all x, y such that $x \approx_{\mathfrak{g}} y$ and for all $z \neq 1$ we have $x \bullet z = \psi_{xz,u}(xz) = \psi_{yz,u}(yz) = y \bullet z$ and if neither x nor y is 1, for all z we have $z \bullet x = \psi_{zx,v}(zx) = \psi_{zy,v}(zy) = z \bullet y$. If $1 \approx_{\mathfrak{g}} n$ and $P \neq \{1, \dots, n-1\}$ then the LD-system $\mathfrak{g}''$ is $\mathfrak{g}$. In these two cases the congruences $\approx_{\mathfrak{g}''}$ and $\approx_{\mathfrak{g}}$ coincide. Now, if $1 \approx_{\mathfrak{g}} n$ and $P = \{1, \dots, n-1\}$ it is straightforward that the equivalence classes for $\approx_{\mathfrak{g}''}$ are trivial. □

Proposition 6.4. *The set of normal LD-systems is stable under the action of the operators B, R and S.*

P r o o f. Let $\mathfrak{g}$ be a normal LD-system with cardinality n. We can assume $n \geqslant 2$ since the operators R and S cannot act on $\mathfrak{p}_0$ and $B(\mathfrak{p}_0) = \mathfrak{t}$ has type 4. Let c be the least constant of $\mathfrak{g}$. By definition, to apply B we must have $xy \neq 1$ for all $y \neq 1$. Then $\mathfrak{g}$ cannot be of type 1 with $c \cdot 1 = n$. Let $\mathfrak{g}' = B(\mathfrak{g})$. Assume $\mathfrak{g}$ is normal of type 1 with $c \cdot 1 = 1$ then $\mathfrak{g}$ is a LD-system $\mathfrak{p}_h$. Therefore, c is $n = 2^h$ and, from Lemma 6.2, the only non-trivial pair of $\approx_{\mathfrak{g}'}$ is $\{1, 2^h\}$. The construction of $\mathfrak{g}'$ gives $2^h * x = 2^h x = x$, for all $x \in \{2, \dots, 2^h\}$, and $2^h * (2^h * 1) = 2^h * (2^h + 1) = 2^h + 1$. Thus, in $\mathfrak{g}'$ the only non-trivial pair for $\approx_c$ is $\{1, 2^h + 1\}$, so $\approx_{\mathfrak{g}'}$ coincides with $\approx_c$. The LD-system $\mathfrak{g}'$ is normal of type 2. Now, if $\mathfrak{g}$ is normal of type 2 then $\mathfrak{g}'$ is normal of type 3 since by construction we have, for all $x \in \{2, \dots, c\}$, $c * x \neq 1$, $c * x = cx = x$ and $c * (c * 1) = c * 1 = n < n + 1$. For the case where $\mathfrak{g}$ is normal of type 3 or 4, using Lemma 6.2, the only new pair is $\{r, n+1\}$ then $c * r$ is equal to $c * (n+1)$. Thus, $\mathfrak{g}'$ is normal of type 3 or 4.

The operator R only changes the return of the former LD-system. Therefore, $R_s(\mathfrak{g})$ is of the same type as $\mathfrak{g}$ unless $\mathfrak{g}$ is equal to $\mathfrak{t}$ and in this case $R_1(\mathfrak{t})$ is $\mathfrak{p}_1$, which has type 1.

The operator S only exchanges values belonging to the same equivalence class. If $\mathfrak{g}$ has type 2, by definition and using the Proposition 5.7, we have $1 \approx_{\mathfrak{g}} n$ and $c \cdot 1 = n$.

If P is $\{1, \dots, n-1\}$ we have in $S_P(\mathfrak{g})$, $c * 1 = n$ and $c * (c * 1) = c * n = 1$. Hence, $S_P(\mathfrak{g})$ has type 1. In all other cases $S_P(\mathfrak{g})$ is of the same type as $\mathfrak{g}$. □

In the sequel we will prove the converse of the previous proposition. Let us begin with some preliminary results.

Lemma 6.5. *If $\mathfrak{g}$ is a left LD-system, with cardinality $n \geqslant 2$, such that the only non-trivial pair of $\approx_{\mathfrak{g}}$ is $\{1, n\}$ then there exists an integer h such that $\mathfrak{g}$ is $B(\mathfrak{p}_h)$.*

Proof. If n equals 2 then $\mathfrak{g}$ is $\mathfrak{t}$ and we have $\mathfrak{t} = B(\mathfrak{p}_0)$. Now assume $n \geqslant 3$. Denote by $\overline{x}$ the equivalence class of x for $\approx_{\mathfrak{g}}$. In $\mathfrak{g}/\approx_{\mathfrak{g}}$ we get $\overline{(n-1)}\overline{1} = \overline{(n-1)1} = \overline{n} = \overline{1}$. Therefore, $\mathfrak{g}/\approx_{\mathfrak{g}}$ is a left LD-system with return 1. It is a LD-system $\mathfrak{p}_h$ for an integer h. Moreover, the number of equivalence classes is $n-1$ thus $n = 2^h + 1$. Let $\mathfrak{g}' = B(\mathfrak{p}_h)$. The cardinality of $\mathfrak{g}'$ is $2^h + 1 = n$. From Lemma 6.2, the only non-trivial pair of $\approx_{\mathfrak{g}'}$ is $\{1, n'\}$. The congruences $\approx_{\mathfrak{g}}$ and $\approx_{\mathfrak{g}'}$ coincide. For all x we have $x \cdot 1 = x * 1$, then $xn = x * n$. We must check that $xy = x * y$ for the other values of y. Let $xy = z$ and $x * y = z'$. Since $\mathfrak{g}$ and $\mathfrak{g}'$ have the same quotient for $\approx$, we must have $\overline{xy} = \overline{x * y} = \overline{z'}$. From the congruences $\approx_{\mathfrak{g}}$ and $\approx_{\mathfrak{g}'}$ we have $z = z'$ or $\{z, z'\} \subseteq \{1, n\}$. Assume $\{z, z'\} \subseteq \{1, n\}$ and $z = 1$, $z' = n$. We have $xy = z = 1$ which implies that all the pairs for $\approx_{\mathfrak{g}}$ are trivial. This contradicts the hypothesis, so $\mathfrak{g}$ is $\mathfrak{g}'$. □

Proposition 6.6. *Let $\mathfrak{g}$ be a normal LD-system with cardinality n. Let c be its least constant element.*

i) *If $\mathfrak{g}$ has type 2 then there exists an integer h such that $\mathfrak{g}$ is $B(\mathfrak{p}_h)$.*

ii) *If $\mathfrak{g}$ has type 1 and $c \cdot 1 = n$ there exist an integer h and a selector P such that $\mathfrak{g}$ is $S_P(B(\mathfrak{p}_h))$.*

Proof. i) We can assume $n \geqslant 3$. The only non-trivial pair of $\approx_c$ in $\mathfrak{g}$ is $\{1, n\}$. Since $\approx_c$ is $\approx_{\mathfrak{g}}$, $\{1, n\}$ is the only non-trivial pair of $\approx_{\mathfrak{g}}$ too. Applying the preceding lemma we obtain $\mathfrak{g} = B(\mathfrak{p}_h)$.

ii) For $n = 2$, it is easy to see that $\mathfrak{t}'$ is $S_{\{1\}}(B(\mathfrak{p}_0))$. Let n be greater than 2. Since $c(c \cdot 1) = 1$, L_c is an automorphism of $\mathfrak{g}$ and c is the unique constant of $\mathfrak{g}$ thus stable. Let us show first that L_c is the transposition $\tau_{(1,n)}$. We have $c \cdot 1 = n$, $c(c \cdot 1) = 1$ and $cc = c$. Since L_c is one-to-one, using the notations of the Proposition 2.3, we have, for all $x \in \{2, \dots, c^-\}$, $cx \in \{2, \dots, c^-\}$. In addition, for all x in $\mathfrak{g}$, we have $x \cdot 1 = x \cdot c(c \cdot 1) = xc \cdot x(c \cdot 1) = c \cdot x(c \cdot 1) = cx \cdot c(c \cdot 1) = cx \cdot 1$. But, we have $x \cdot 1 = x + 1$ for x in $\{2, \dots, c^-\}$. Therefore, we get $x \cdot 1 = x + 1 = cx \cdot 1 = cx + 1$, so $cx = x$ and $L_c = \tau_{(1,n)}$. The return of $\mathfrak{g}$ is 2 since $n \cdot 1 = (c \cdot 1)1 = (c \cdot 1) \cdot c(c \cdot 1) = (c \cdot 1)c \cdot (c \cdot 1)(c \cdot 1) = c \cdot c(1 \cdot 1) = c(c \cdot 2) = c \cdot 2 = 2$. Now, define a relation $\equiv$ on

$\{1, \dots, n\}$ by

$$x \equiv y \iff \begin{cases} x = y, \\ \text{or } \{x, y\} \subseteq \{1, n\} \end{cases}$$

and show it is a congruence. The relation $\equiv$ is an equivalence relation since it is a partition of $\{1, \dots, n\}$. We have to show it is compatible with the product. Fix a, b in $\mathfrak{g}$ satisfying $a \equiv b$. For all x in $\mathfrak{g}$

- if $a = b$ we have $xa = xb$, $ax = bx$ then $xa \equiv xb$ and $ax \equiv bx$,
- if $\{a, b\} \subset \{1, n\}$ and $a \neq b$
  if $x < c$ we have $xn = x(c \cdot 1) = xc \cdot (x \cdot 1) = c(x \cdot 1) = x \cdot 1$, since L_c is $\tau_{(1,n)}$, then $x \cdot 1 \equiv xn$,
  if $x = c$ we have $cn = c(c \cdot 1) = 1$ and $c \cdot 1 = n$ then $\{cn, c \cdot 1\} \subset \{1, n\}$ so $c \cdot 1 \equiv cn$,
  if $x = n = c \cdot 1$ we have $nn = (c \cdot 1)(c \cdot 1) = c(1 \cdot 1) = c \cdot 2 = 2 = 1 \cdot 1 = n \cdot 1$, since the return is 2, then $n \cdot 1 \equiv nn$,
  since the return is 2, we have $n \cdot 1 = 1 \cdot 1$ which implies $nx = 1 \cdot x$ for all $x \neq 1$ so $nx \equiv 1 \cdot x$.

This proves that $\equiv$ is a congruence. Moreover, the only non-trivial pair is $\{1, n\}$, thus there is $n - 1$ equivalence classes for $\equiv$. In $\mathfrak{g}/\equiv$ we have $\overline{c} \cdot \overline{1} = \overline{c \cdot 1} = \overline{n} = \overline{1}$. Therefore, $\mathfrak{g}/\equiv$ admits 1 as return. Thus, $\mathfrak{g}/\equiv$ is a LD-system $\mathfrak{p}_h$ for an integer h. In addition, n is equal to $2^h + 1$. Let $\mathfrak{g}' = B(\mathfrak{p}_h)$. From Lemma 6.2, the only non-trivial pair of $\approx_{\mathfrak{g}'}$ is $\{1, n\}$. By construction the return of $\mathfrak{g}'$ is 2, there is a unique constant $c = n - 1$ and we have

$$c * x = \begin{cases} n & \text{if } x = 1 \text{ or } x = n, \\ x & \text{if } 1 < x < n. \end{cases}$$

Thus, in $\mathfrak{g}'$ the relations $\approx_{\mathfrak{g}'}$, $\approx_c$ and $\equiv$ coincide. Moreover, $\mathfrak{g}'$ satisfies the definition of the normal LD-systems of type 2. Apply the operator S to $\mathfrak{g}'$ with $P = \{1, \dots, n-1\}$. The only change between the table of $\mathfrak{g}'$ and the table of $S_P(\mathfrak{g}')$ is the value of $c * (c * 1)$ which becomes 1. This proves $S_P(\mathfrak{g}') = \mathfrak{g}$. □

Lemma 6.7. *Let $\mathfrak{g}$ be a normal LD-system of type 3 or 4 with cardinality $n \geqslant 3$. There exists an integer h such that $\mathfrak{g}/\approx_{\mathfrak{g}} = B(\mathfrak{p}_h)$.*

Proof. Let c be the least constant of $\mathfrak{g}$. From Lemma 5.3, $c'(c' \cdot 1) \neq 1$ for all constant c', otherwise $\mathfrak{g}$ cannot be of type 3 or 4. Assume $\mathfrak{g}$ has type 3 and let $\mathfrak{h} = \mathfrak{g}/\approx_{\mathfrak{g}}$. The LD-system $\mathfrak{h}$ is a left LD-system since it is a quotient of $\mathfrak{g}$. From Lemmas 2.4, 3.3, 5.2 and the hypothesis, one can see that the number of equivalence classes for $\approx_{\mathfrak{g}}$ is $c \cdot 1 = c + 1 \geqslant 3$, the only constant of $\mathfrak{h}$ is $\overline{c}$ and $\overline{c}(\overline{c} \cdot \overline{1}) = \overline{c(c \cdot 1)} = \overline{c \cdot 1} = \overline{c} \cdot \overline{1}$. Moreover, we have $\overline{c \cdot 1} = \{c \cdot 1\}$. Then the cardinality of $\mathfrak{h}$ is $\overline{c\cdot 1} = \bar{c}\cdot\bar{1}$. Since we have $\bar{c}(\bar{c}\cdot\bar{1}) \neq \bar{1}$ $\mathfrak{h}$ is normal of type 2, and using Proposition 6.6, $\mathfrak{h}$ is $B(\mathfrak{p}_h)$ for an integer h.

Now, if $\mathfrak{g}$ has type 4 and if there is an $x > 1$ which is not a constant element, using the same argument as above, we can prove that $\mathfrak{h}$ is $B(\mathfrak{p}_h)$ for an integer h. If all $x > 1$ are constant then $\mathfrak{h}$ is $\mathfrak{t}$ which is $B(\mathfrak{p}_0)$. ☐

Proof of Theorem 6.1. Let $\mathfrak{g}$ be a normal LD-system with underlying set $\{1,\ldots,n\}$, 1 as a generator and return $r = n\cdot 1$. Let c be its least constant. If $\mathfrak{g}$ has type 1 or 2 the Proposition 6.6 gives the result. If it has type 3 or 4 we can assume $n \geqslant 3$ since $t = B(\mathfrak{p}_0)$. Then using Lemma 6.7, $\mathfrak{g}/\approx_{\mathfrak{g}} = B(\mathfrak{p}_h)$ for an integer h. We have to rebuilt $\mathfrak{g}$ from $B(\mathfrak{p}_h)$. The case of type 3 or 4 is similar. From the injectivity of L_c and Lemma 2.4, for all x, y in $\{2,\ldots,n\}$ we have $x \approx_{\mathfrak{g}} y \iff |x-y| = kc$, with $k = 0$ or $k = 1$ if $\mathfrak{g}$ has type 3 and k satisfies $kc < n$ if $\mathfrak{g}$ has type 4. Since $\approx_{\mathfrak{g}}$ and $\approx_c$ coincide on $\{2,\ldots,n\}$ from the Proposition 5.7, the equivalence classes of $\approx_{\mathfrak{g}}$ are given by

$$\bar{x} = \begin{cases} \{1\} & \text{if } x = 1, \\ \{c\cdot 1\} & \text{if } x = c\cdot 1, \\ \{y \in \mathfrak{g};\ y \geqslant x,\ y - x = kc\} & \text{if } x \in \{2,\ldots,c\}, \end{cases}$$

where $k = 0$ or $k = 1$ if $\mathfrak{g}$ has type 3 and k satisfies $kc < n$ if $\mathfrak{g}$ has type 4. Let $d = \mathrm{card}(\mathfrak{g}) - \mathrm{card}(\mathfrak{p}_h)$ and $\mathfrak{g}' = B^d(\mathfrak{p}_h)$ (i.e. apply d times the operator B to $\mathfrak{p}_h$). Let $*$ denote the product of $\mathfrak{g}'$. Since the normal LD-systems are stable under B, $\mathfrak{g}'$ is normal of same cardinality as $\mathfrak{g}$. From the construction of $\mathfrak{g}'$ and Lemma 6.2, we deduce that

i) if $\mathfrak{g}$ has type 3 then there is a unique constant c, we have $c*(c*1) = c*1$ and $c*1 \notin \{1,n\}$, thus, $\mathfrak{g}'$ has type 3,

ii) if $\mathfrak{g}$ has type 4 then there is a constant c' such that $c'*(c'*1) = c'*1$, if c is the least constant of $\mathfrak{g}'$ then $c \notin \{1,n\}$, thus, $\mathfrak{g}'$ has type 4,

iii) the equivalence classes of $\approx_{\mathfrak{g}'}$ are given by

$$\bar{x} = \begin{cases} \{1\} & \text{if } x = 1, \\ \{c*1\} & \text{if } x = c*1, \\ \{y \in \mathfrak{g};\ y \geqslant x,\ y - x = kc\} & \text{if } x \in \{2,\ldots,c\}, \end{cases}$$

where $k = 0$ or $k = 1$ if $\mathfrak{g}$ has type 3 and k satisfies $kc < n$ if $\mathfrak{g}$ has type 4.

Therefore, $\approx_{\mathfrak{g}}$ and $\approx_{\mathfrak{g}'}$ coincide. If $xy \neq x*y$ then the two values belong to the same equivalence class. We can pick a selector P such that xy represents its equivalence class. Let $\mathfrak{s} = S_P(\mathfrak{g}')$ and denote its product by $\bullet$. The return of $\mathfrak{s}$ is r', return of $\mathfrak{g}'$, and for all couple (x,y) of $\mathfrak{s}^2$ such that $(x,y) \neq (n,1)$ we have $x\bullet y = xy$. Let $\mathfrak{r} = R_r(\mathfrak{s})$ and denote its product by $\circ$. The LD-system $\mathfrak{r}$ is a left LD-system with return r such that, for all couple $(x, y) \neq (n, 1)$, we have $x \circ y = xy$. Then $\mathfrak{r}$ coincides with $\mathfrak{g}$ and we obtain $\mathfrak{g} = R_r(S_P(\mathrm{B}^d(\mathfrak{p}_h)))$.

To prove the unicity, assume that we try to construct a normal LD-system $\mathfrak{g}$ of cardinality n from the LD-system $\mathfrak{p}_m$ with $2^m \leqslant n$. Then the value of d is determined by the equation $2^m + d = n$ and, therefore, it is unique. Each selector P determines all the values of the table but those in the first column. Therefore, to each selector corresponds a family $\mathcal{F}$ of tables which only differ by the first column. The values from 1 to $n-1$ are fixed since a normal LD-system is a left LD-system. Hence, the tables of $\mathcal{F}$ only differ by the value of the return which is the value of $n \cdot 1$. Therefore, the choice of a return r determines a unique table of this family. Then the choice of the three parameters d, r and P determines a unique table. □

Let us consider the following tables.

	1	2	3	4	5	6
1	2	4	4	4	4	4
2	3	4	3	4	3	4
3	4	4	4	4	4	4
4	5	4	3	4	3	4
5	6	4	4	4	4	4
6	3	4	3	4	3	4

Table 6

	1	2	3
1	2	2	2
2	3	2	3
3	2	2	2

Table 7

	1	2	3	4	5	6
1	2	6	6	6	6	6
2	3	6	5	6	5	6
3	4	6	6	6	6	6
4	5	6	5	6	5	6
5	6	6	6	6	6	6
6	5	6	5	6	5	6

Table 8

	1	2	3	4	5	6
1	2	4	4	4	4	4
2	3	4	3	4	3	4
3	4	4	4	4	4	4
4	5	4	3	4	3	4
5	6	4	4	4	4	4
6	5	4	3	4	3	4

Table 9

Let $\mathfrak{g}$ be the normal LD-system of Table 6. This is a normal LD system of type 4, the cardinality is 6, the return is 3, the least constant is 2 (the constant column of least indice) and the equivalence classes of the congruence $\approx_{\mathfrak{g}}$ are $\{1\}$, $\{2, 4, 6\}$, $\{3, 5\}$. The table of $\mathfrak{g}/\approx_{\mathfrak{g}}$ is Table 7, which is the normal LD-system $B(\mathfrak{p}_1)$. We apply successively 3 times the operator B and we obtain the normal LD-system $B^4(\mathfrak{p}_1)$ of Table 8. In this LD-system the equivalence classes of the congruence $\approx_{B^4(\mathfrak{p}_1)}$ are $\{1\}$, $\{2, 4, 6\}$, $\{3, 5\}$. They are identical to equivalence classes of the congruence $\approx_{\mathfrak{g}}$. Taking P equal to $\{1, 3, 4\}$, we obtain the LD-system $S_P(B^4(\mathfrak{p}_1))$ of Table 9. Now, taking s equal to 3, we obtain the LD-system $R_3(S_P(B^4(\mathfrak{p}_1)))$ of Table 6, which coincides with $\mathfrak{g}$.

To finish we prove, now, the periodicity phenomenon for normal LD-systems.

Lemma 6.8. *Let $\mathfrak{g}$ be a normal LD-system with cardinality $n \geqslant 3$ and return $r \geqslant 2$. Assume $\mathfrak{g} = R_r(S_P(\mathrm{B}^d(\mathfrak{p}_m)))$ for suitable d, P, r and m. Then the least constant of $\mathfrak{g}$ is 2^m and we have for all $1 \leqslant x \leqslant 2^m$ and integer k, $0 \leqslant k \leqslant 2^m - \nu_{2^m}(x)$,*

$$x(\nu_{2^m}(x) + k) = \begin{cases} x(k)_{\nu_{2^m}(x)} & \text{if } (k)_{\nu_{2^m}(x)} \neq 1, \\ x \cdot \nu_{2^m}(x)1 & \text{if } (k)_{\nu_{2^m}(x)} = 1. \end{cases}$$

Proof. For $k = 0$ there is nothing to do since $(0)_{\nu_{2^m}(x)}$ is $\nu_{2^m}(x)$. Then let $k \geqslant 1$. By construction the cardinality of $\mathfrak{g}/\approx_{\mathfrak{g}}$ is $c+1 = c+1 = 2^m+1$ where c is the least constant element of $\mathfrak{g}$. Hence, we have $c = 2^m$. Moreover, since $\nu_{2^m}(2^m)$ is 2^m, Lemma 2.4 gives the result for $c = 2^m$. Now, let x be between 1 and $2^m - 1$. Consider the case of a LD-system $B^d(\mathfrak{p}_m)$. Let $*$ denote the product of $\mathfrak{p}_m$. Assume we have $\nu_{2^m}(x) + k \leqslant 2^m$. If neither $(k)_{\nu_{2^m}(x)}$ nor $\nu_{2^m}(x)$ is 1 then in $\mathfrak{p}_m$ we have $x * (\nu_{2^m}(x) + k) = x * (k)_{\nu_{2^m}(x)}$ and this still holds in $B^d(\mathfrak{p}_m)$ by construction. If $\nu_{2^m}(x)$ is 1 then $(k)_{\nu_{2^m}(x)}$ is 1 for all k and in $\mathfrak{p}_m$ we have $x * y = x * z$ for all $1 \leqslant y \leqslant z \leqslant 2^m$. Therefore by contruction, in $B^d(\mathfrak{p}_m)$ we have $x \cdot 2 = xu$ for all $u \geqslant 2$. In particular $\nu_{2^m}(x) + k$ is at least 2. Thus, we have $x(\nu_{2^m}(x) + k) = x \cdot 2 = x(1+1) = x(\nu_{2^m}(x) \cdot 1)$. Now if we have $(k)_{\nu_{2^m}(x)} = 1$ and $\nu_{2^m}(x) \neq 1$ then we have either $k = 1$ or $k = u\nu_{2^m}(x) + 1 \geqslant 2$. In the first case we have $x(\nu_{2^m}(x) + 1) = x(\nu_{2^m}(x) + 1)$ since $\nu_{2^m}(x)$ is less than $2^m + d$, the cardinality of $B^d(\mathfrak{p}_m)$. For the second case, in $\mathfrak{p}_m$ we have $x * (u\nu_{2^m}(x) + 1) = x * (\nu_{2^m}(x) + 1)$ and $\nu_{2^m}(x) + 1 \geqslant 2$. Then still by contruction, in $B^d(\mathfrak{p}_m)$ we have $x(\nu_{2^m}(x) + k) = x(\nu_{2^m}(x) + 1)$, hence, we have $x(\nu_{2^m}(x) + k) = x(\nu_{2^m}(x) + 1) = x(\nu_{2^m}(x) \cdot 1)$. For $\nu_{2^m}(x) + k > 2^m$, by construction there exists a unique $2 \leqslant y \leqslant 2^m$ satisfying $xy = x(\nu_{2^m}(x) + k)$ and such that $y - (\nu_{2^m}(x) + k)$ is a multiple of 2^m. Let $y = \nu_{2^m}(x) + h$, we have $\nu_{2^m}(x) + k = u2^m + \nu_{2^m}(x) + h$. Since $\nu_{2^m}(x)$ divides 2^m, we have $(k)_{\nu_{2^m}(x)} = (\nu_{2^m}(x) + k)_{\nu_{2^m}(x)} = (u2^m + \nu_{2^m}(x) + h)_{\nu_{2^m}(x)} = (h)_{\nu_{2^m}(x)}$. So, we obtain $x(\nu_{2^m}(x) + k) = x(\nu_{2^m}(x) + h)$ and, from the preceding, the result follows.

Now if we apply S, all equalities of the type $xy = xz$, $1 < y \leqslant z$, in $B^d(\mathfrak{p}_m)$ still hold in $S_P(B^d(\mathfrak{p}_m))$. If k is 0 then we have the result since $(0)_{\nu_{2^m}(x)} = \nu_{2^m}(x)$. If k is at least 1 then we have $\nu_{2^m}(x) + k > 1$ and $\nu_{2^m}(x) \cdot 1 > 1$. Therefore, we can conclude. For the operator R we have the result since it only changes the return, thus, none of the products xy, $y > 1$. □

Proposition 6.9. *Let $\mathfrak{g}$ be a normal LD-system with cardinality $n \geqslant 3$ and return $r \geqslant 2$. Assume $\mathfrak{g} = R_r(S_P(\mathrm{B}^d(\mathfrak{p}_m)))$ for suitable d, P, r and m. The values of r and of the products xy, for x in $\{1, \dots, 2^m\}$ and y in $\{2, \dots, \nu_{2^m}(x) + 1\}$, completely determine the table of $\mathfrak{g}$.*

Proof. Since $\mathfrak{g}$ is a left LD-system, all values in the first column but the one of the return are determined. The previous lemma proves that for all x in $\{1, \dots, 2^m\}$ the values of the products xy are determined by the values of the products xy with y in $\{2, \dots, \nu_{2^m}(x) + 1\}$. Now, by construction for all $y > 2^m$ there exists a unique $x \leqslant 2^m$ such that $yz = xz$ holds for all $z > 1$. □

Conclusion

The normal LD-systems have the same periodic behaviour as the LD-systems $\mathfrak{p}_k$. Moreover, the least constant element of a normal LD-system $\mathfrak{g}$ is a power of 2, which is the cardinality of the LD-system $\mathfrak{p}_k$ from which $\mathfrak{g}$ is built. Thus, the normal LD-systems are "natural" extensions of the LD-systems $\mathfrak{p}_k$.

To mention some natural open questions, we would mention the conjecture that the relation $\approx_{\mathfrak{g}}$ is a congruence for any monogenic LD-system (and not only for the left ones), an assertion that has been verified for all LD-systems with cardinality $\leqslant 6$ (there are 1221 non isomorphic such systems), and the more informal conjecture that all monogenic LD-systems can be constructed from the $\mathfrak{p}_k$ in some sense (see [7] and [8] for further result on this question).

Acknowledgement

I would like to thank Patrick Dehornoy for his help during the preparation of this paper.

References

[1] *P. Dehornoy*: Sur la structure des gerbes libres. C. R. Acad. Sci. Paris *309* (1989), 143–148.

[2] *P. Dehornoy*: Braid Group and Left Distributive Operations. Trans. Amer. Math. Soc *345-1* (1994), 115–151.

[3] *R. Dougherty and Th. Jech*: Finite left-distributive algebras and embeddings algebras. To appear in Advances in Math.

[4] *A. Drápal*: Homomorphisms of Primitive Left Distributive Groupoids. Communications in Algebra *22(7)* (1994), 2579–2592.

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

[6] *A. Drápal*: Persistence of Left Distributive Algebras. To appear in J. Pure Appl. Algebra.

[7] *A. Drápal*: Finite Left Distributive Algebras with One Generator. To appear in J. Pure Appl. Algebra.

[8] *A. Drápal*: Finite Left Distributive Grupoids with One Generator. To appear in Int. J. Algebra & Computation.

[9] *R. Laver*: The left distributive law and the freeness of an algebra of elementary embeddings. Advances in Mathematics *91* (1992), 209–231.

[10] *R. Laver*: On the algebra of elementary embeddings of a rank into itself. Advances in Mathematics *110* (1995), 334–346.

[11] *A. Sesboüé*: Algèbres distributives finies monogènes. Thèse de doctorat, Université de Caen, (1993).

[12] *F. Wehrung*: Gerbes primitives. C. R. Acad. Sci. Paris *313* (1991), 357–362.

Author's address: André Sesboüé, Département de Mathématiques, Université de Caen, Esplanade de la Paix, 14032 Caen Cedex, France, e-mail: `sesboue@math.unicaen.fr`.