SUBDIRECTLY IRREDUCIBLE NON-IDEMPOTENT LEFT DISTRIBUTIVE LEFT QUASIGROUPS

DAVID STANOVSKÝ

Abstract. Left distributive left quasigroups are binary algebras with unique left division satisfying the left distributive identity $x(yz) \approx (xy)(xz)$. In other words, binary algebras where all left translations are automorphisms. We provide a description and examples of non-idempotent subdirectly irreducible algebras in this class.

1. Introduction

A groupoid (it means an algebra with one binary operation, denoted usually multiplicatively) is called *left distributive*, if it satisfies the identity

(LD) $$x(yz) \approx (xy)(xz)$$

and it is called a *left quasigroup*, if

(LQ) for every a, b there is a unique c with $ac = b$.

Such c is usually denoted $a\backslash b$. Equivalently, left distributive left quasigroups are groupoids, where all left translations are automorphisms. (A *left translation* of an element a in a groupoid G is the mapping $L_a : G \to G$, $x \mapsto ax$.) It is thus a very naturally defined class of algebras. We aim for a structural theorem for this class. The first step might be, to describe the structure of its subdirectly irreducible members. We do so in the non-idempotent case.

There are very natural examples of (idempotent) left distributive left quasigroups. On a group G, we define a new operation by

$$x * y = xyx^{-1}.$$

It is very easy to check that the groupoid $G(*)$, called the *conjugation groupoid* of G, is an idempotent left distributive left quasigroup. To get a non-idempotent example, consider, for instance, the operation $x *_a y = xyx^{-1}a$, where a is a fixed central element of the group.

Idempotent selfdistributive structures were studied for a long time, because of natural examples arising in algebra, geometry and topology. The attention to non-idempotent ones was brought in 1980's by P. Dehornoy, R. Laver, T. Jech and others, when a relation between free (non-idempotent) left distributive groupoids and large cardinals was found (see [15], [5]). Later, another source of natural examples appeared in braid groups. For more information, the reader is refered

1991 *Mathematics Subject Classification.* 20N02, 08B20.

Key words and phrases. Groupoid, left distributive, left quasigroup, subdirectly irreducible, group conjugation.

While working on this paper, the author was supported by the Eduard Čech Center for Algebra and Geometry. A partial support by the grant GAČR 201/05/0002 is also acknowledged.

to the excellent book [4] of P. Dehornoy. A purely algebraic approach to non-idempotent selfdistributive groupoids is developed in [13].

Left distributive left quasigroups were studied by several authors, mostly in the idempotent case, under different names, e.g. *left-distributive algebras* [14], *racks* [7] [21], *quandles* [10] [11], *automorphic sets* [2], *pseudo-symmetric sets* [17] [18] [19], etc. These papers contain some theory and applications. We wish to emphasize the famous articles [10] of D. Joyce and [16] of S. V. Matveev, where a left distributive left quasigroup is assigned to every knot (so called *knot quandle*) so that it is invariant with respect to knot homotopy.

The purpose of the present paper is to continue the investigations on non-idempotent left distributive left quasigroups started in [12], [9], [24], [25] and, in particular, to get a better insight into the structure of subdirectly irreducible ones. We generalize most of the results from the paper [9] of Jeřábek, Kepka and the author, where left distributive left quasigroups with left translations of order at most 2 were considered. This is an improved version of what appeared in the author's PhD Thesis [22].

We start with several basic facts about general (not necessarily subdirectly irreducible) non-idempotent left distributive left quasigroups. Section 3 contains a description of subdirectly irreducibles, our main results are Theorems 3.2, 3.4 and 3.9. In Section 4, we show some examples.

For our considerations, it is essential that a non-idempotent element is present in the groupoid. It seems that the classification of *idempotent* subdirectly irreducible left distributive left quasigroups will be very difficult. Even the classification of *simple* ones, made by D. Joyce in [11], is fairly complicated; they are in a tight connection to simple groups (finite ones to finite simple groups) via conjugation groupoids. We also note that idempotent subdirectly irreducible *medial* left quasigroups with left translations of order at most 2 were classified by B. Roszkowska-Lech in [20].

Finally, we note that if one consideres the subclass of those groupoids, where both *left and right* translations are automorphisms (these are called *distributive quasigroups* and are necessarily idempotent), there is a nice description, due to V. D. Belousov [1]: they are just isotopes of commutative Moufang loops, a non-associative generalization of abelian groups.

2. Basic facts

We use a standard terminology and notation of universal algebra, mostly following the book [3]. We recall that a groupoid G is *subdirectly irreducible*, if and only if the intersection of its non-trivial congruences, called the *monolith* and denoted μ_G, is non-trivial.

Left quasigroups are groupoids, where for every a, b there is a unique $a\backslash b$ such that $a(a\backslash b) = b$. In the present paper, we do not regard the left division $\backslash$ as a basic operation. However, it often happens that there is a (multiplicative) term $t(x, y)$ such that $a\backslash b = t(a, b)$ for every a, b. In this case we say that the left quasigroup has *term-definable left division.* We note that left quasigroups do not form a groupoid variety (i.e. they cannot be axiomatized by identities in the language of multiplication). However, they are axiomatized by the identities $x(x\backslash y) \approx y$ and $x\backslash(xy) \approx y$ in the language of multiplication and left division. (We note that in this language the equational theory of idempotent left distributive left quasigroups coincides with that of group conjugation, see [10]. This is not true when restricted to multiplication, see [6], [14] or [23].)

A groupoid G is called *left n-symmetric*, if $(L_a)^n = id$ for every $a \in G$. (Such groupoids are clearly left quasigroups.) Left n-symmetric groupoids do form a variety: they are based by the identity

$$(n\text{-LS}) \qquad \underbrace{x(x(\dots(x}_{n}\, y))) \approx y.$$

(The notion of *left symmetry* is usually used for left 2-symmetry.)

Note that every finite left quasigroup is left n-symmetric for some n and that left n-symmetric groupoids have term definable left division — namely,

$$x\backslash y \approx \underbrace{x(x(\dots(x}_{n-1}\, y))).$$

In further text, we will abbreviate the names of the identities by LD, LS, n-LS, etc.

A subgroupoid of a left quasigroup is not necessarily a left quasigroup (it is indeed left cancellative, but not necessarily left divisible). We will thus use the notion of *left subquasigroup*. Subgroupoids of left quasigroups with term-definable left division are indeed left subquasigroups.

A non-empty subset I of a left quasigroup G is called a *left ideal*, if $a \in G$, $b \in I$ implies $ab \in I$ (in other words, if $GI \subseteq I$). I is called a *strong left ideal*, if $a \in G$, $b \in I$ implies $ab \in I$ and $a\backslash b \in I$. Clearly, if $I \subset G$ is a strong left ideal, then $G \smallsetminus I$ is also a strong left ideal. Ideals of left quasigroups with term-definable left division are always strong.

A subset S of a groupoid G is called *definable* in G if there exists a formula Φ with a single free variable such that $S = \{a \in G : \Phi(a)\}$. A relation α on G is called *definable*, if there exists a formula Φ with two free variables such that $\alpha = \{(a, b) \in G \times G : \Phi(a, b)\}$. A relation α is called *right stable*, if $(a, b) \in \alpha$ implies $(ac, bc) \in \alpha$ for every c.

Lemma 2.1. *Let G be an LD left quasigroup. Then*

(1) *every definable subset in G is either empty, or a strong left ideal;*
(2) *every definable right stable equivalence on G is a congruence of G.*

Proof. Indeed, for every automorphism α, $\Phi(a)$ holds iff $\Phi(\alpha(x))$ holds. Hence the claim follows from the fact that left translations and their inverses are automorphisms. □

Later we will need also the following observation:

Lemma 2.2. *Let G be an LD left quasigroup, $a, b \in G$ and φ an automorphism of G. Then*

$$L_{\varphi(b)} = \varphi L_b \varphi^{-1} \quad \textit{and} \quad L_{ab} = L_a L_b L_a^{-1}.$$

Proof. For every $c \in G$ we have $L_{\varphi(b)}(c) = \varphi(b)c = \varphi(b\varphi^{-1}(c)) = \varphi L_b \varphi^{-1}(c)$. The second claim follows from the first one by setting $\varphi = L_a$. □

Consequently, we have a Cayley-like representation of LD left quasigroups: the mapping $a \mapsto L_a$ is a homomorphism from G into the conjugation groupoid of the symmetric group over the set G. It is not necessarily injective.

We recall that a groupoid is *idempotent*, if it satisfies $xx \approx x$. It is called *left idempotent*, if it satisfies the identity

$$(xx)y \approx xy. \tag{LI}$$

An easy induction shows that left idempotent groupoids satisfy for every $n \geq 1$ the identity $x^n y \approx xy$, where

$$x^n = \underbrace{x(x(\cdots(xx)))}_{n}.$$

Indeed, if $x^{n-1}y \approx xy$, then

$$x^n y = (xx^{n-1})y \approx (x^{n-1}x^{n-1})y \approx x^{n-1}y \approx xy.$$

Consequently, any term t in a single variable x is LI-equivalent to the term x^d, where d is the right depth of t. In particular, in LI groupoids

$$(x^m)^n \approx (x^n)^m \approx x^{m+n-1}$$

holds for every $m, n \geq 1$.

Lemma 2.3. *LD left quasigroups are left idempotent.*

Proof. $xy \approx x(x(x\backslash y)) \approx_{LD} (xx)(x(x\backslash y)) \approx (xx)y$. □

The main feature for investigation of non-idempotent LD left quasigroups is the fact that the smallest congruence with idempotent quotient, denoted by ip_G, has a very nice structure. This was first observed by P. Jedlička in [8], more generally for LDLI groupoids. We will need the following improvement of his result.

Let γ_k be the smallest congruence such that the corresponding factor satisfies the identity $x^{k+1} \approx x$. Indeed, $\gamma_k \subseteq \gamma_\ell$, iff $\ell \mid k$. Particularly, $\gamma_k \subseteq \gamma_1 = ip_G$ for every k.

Proposition 2.4. *Let G be an LDLI groupoid and $k \geq 1$. Then γ_k is the smallest equivalence on the set G containing all pairs (a, a^{k+1}), $a \in G$. Further,*

$$\gamma_k = \{(a,b) \in G \times G : a^m = b^n \text{ for some } m, n \text{ such that } k \text{ divides } m - n\}.$$

Moreover, if $(a,b) \in \gamma_k$, then $ac = bc$ holds for every $c \in G$.

Proof. Clearly γ_k must contain all pairs (a, a^{k+1}), $a \in G$. We prove that the equivalence α generated by these pairs is a congruence. It means that we need to check that $(ab, a^{k+1}b) \in \alpha$ and $(ba, ba^{k+1}) \in \alpha$ for every $a, b \in G$. The first claim follows from left idempotency, since $ab = a^n b$ for every n. For the second claim, using k-times left distributivity we obtain that $ba^{k+1} = (ba)^{k+1}$. Consequently, $\alpha = \gamma_k$.

Next, assume that $(a,b) \in \gamma_k$ and we prove that $a^m = b^n$ for some m, n with $k \mid m - n$. Since γ_k is generated as an equivalence by the set $\{(a, a^{k+1}) : a \in G\}$, there are $c_0, \ldots, c_\ell$ such that $a = c_0$, $b = c_\ell$ and either $c_i = c_{i+1}^{k+1}$, or $c_i^{k+1} = c_{i+1}$ for every $i = 0, \ldots, \ell - 1$. We proceed by induction on ℓ. If $\ell = 0, 1$, it is trivial. So, assume that $a^m = c_{\ell-1}^n$ for some m, n with $k \mid m - n$. If $c_{\ell-1} = b^{k+1}$, then

$$b^{n+k} = (b^{k+1})^n = c_{\ell-1}^n = a^m$$

and $k \mid m - (n+k)$. If $c_{\ell-1}^{k+1} = b$, then

$$a^{m+k} = (a^m)^{k+1} = (c_{\ell-1}^n)^{k+1} = (c_{\ell-1}^{k+1})^n = b^n$$

and, again, $k \mid m + k - n$.

For the other inclusion, assume that $a^m = b^n$ for some m, n with $k \mid m-n$. Then also $a^{m+u} = (a^m)^{u+1} = (b^n)^{u+1} = b^{n+u}$ for every $u \geq 0$. Let us write $m = m'k + q$ and $n = n'k + q$. Since

$$(a, a^{k+1}) \in \gamma_k,\ (a^{k+1}, a^{2k+1}) \in \gamma_k,\ \ldots,\ (a^{m'k+1}, a^{(m'+1)k+1}) \in \gamma_k,$$

we have $(a, a^{m'k+k+1}) \in \gamma_k$ and similarly $(b, b^{n'k+k+1}) \in \gamma_k$. Since

$$a^{m'k+k+1} = a^{m+(k+1-q)} = b^{n+(k+1-q)} = b^{n'k+k+1},$$

we obtain $(a, b) \in \gamma_k$.

Finally, if $(a, b) \in \gamma_k$, then $a^m = b^n$ for some m, n and thus $ac = a^m c = b^n c = bc$ for every $c \in G$ by left idempotency. □

Consequently, every block of ip_G is a subgroupoid of G satisfying the identity $xz \approx yz$ and it is term equivalent to a *connected* monounary algebra; the left translation is the corresponding unary operation.

A groupoid isomorphic to the groupoid C_n, defined on the set $\{0, \ldots, n-1\}$ by $ab = b + 1 \bmod n$, will be called *circle of length* n. A groupoid isomorphic to the groupoid C_∞ of integers with the operation $ab = b + 1$ will be called *infinite path.*

Corollary 2.5. *Let G be an LD left quasigroup. Then every block of ip_G is either a circle, or an infinite path.*
Moreover, if G is n-LS, then every block is a circle of length $k \mid n$.

Note that the congruence lattice of C_n consists of the (pairwise different) congruences γ_k, $k \mid n$. Consequently, we have the following:

Corollary 2.6. *Circles of prime length are the only simple non-idempotent LD left quasigroups.*

We define the *cycle type* of an LD left quasigroup G to be the set of all $k \in \mathbb{N} \cup \{\infty\}$ such that there is an ip_G-block isomorphic to C_k. Indeed, n-LSLD groupoids have only divisors of n in its cycle type. For example, the cycle type contains 1 if and only if G has an idempotent element.

3. Description

Let G be an LD left quasigroup. According to Lemma 2.1, the set Ip_G of idempotent elements of G and its complement $K_G = G \setminus Ip_G$ are either empty, or strong left ideals.

Lemma 3.1. *Let G be a non-idempotent subdirectly irreducible LD left quasigroup. Then K_G contains no proper strong left ideal. Consequently, it contains no definable proper subset.*

Proof. Let $I \subset K_G$ be a proper strong left ideal in K_G. For any $a \in I$, we have also $a \neq aa \in I$, hence I contains at least two elements. Let ρ_I be the set of all $(a, b) \in ip_G$ such that $a = b$ or $a, b \in I$. This equivalence is a non-trivial congruence of G: non-trivial because we have $(a, aa) \in \rho_I$ for every $a \in I$, right stable by Proposition 2.4 (any equivalence below ip_G is right stable) and $(a, b) \in \rho_I$ implies $(ca, cb) \in \rho_I$, because I is a left ideal. Now, we apply the same to the strong left ideal $J = K_G \setminus I$ and we obtain two non-trivial congruences ρ_I and ρ_J with trivial intersection, contradicting the subdirect irreducibility of G. The second statement follows from Lemma 2.1. □

Theorem 3.2. *Let G be a non-idempotent subdirectly irreducible LD left quasigroup. Then there is a prime p and $r \in \mathbb{N}$ such that G has cycle type $\{p^r\}$ or $\{1, p^r\}$. Consequently, the monolith of G is below $\gamma_{p^{r-1}}$.*
Moreover, if G has term-definable left division, the monolith of G is $\gamma_{p^{r-1}}$.

Proof. First, assume that all non-trivial ip_G-blocks are infinite. Then $\gamma_k \neq \gamma_l$ for every $k \neq l$, and so there is an infinite decreasing sequence

$$\gamma_2 \supset \gamma_4 \supset \cdots \supset \gamma_{2^k} \supset \ldots$$

with trivial intersection. Hence G is not subdirectly ireducible, a contradiction.

So, let n be the least number such that there is a non-trivial ip_G-block which is a circle of length n. Then, according to Lemma 2.1, $K_n = \{a \in G : a^{n+1} = a\}$ is a strong left ideal and thus $K_n = K_G$. It means that all non-trivial blocks are circles of length n. If $n = kl$ for some relatively prime k, l, then γ_k and γ_l are non-trivial congruences with trivial intersection, a contradiction. Hence n is a prime power. Clearly,

$$ip_G = \gamma_1 \supset \gamma_p \supset \cdots \supset \gamma_{p^{r-1}} \supset \gamma_{p^r} = id_G,$$

so $\mu_G \subseteq \gamma_{p^{r-1}}$.

Now, assume that G has term-definable left division and μ_G is a proper subcongruence of $\gamma_{p^{r-1}}$. Then there is a non-trivial ip_G-block B such that μ_G is identical on B and thus the set

$$I = \{a \in G : (a, b) \in \mu_G \text{ for some } b \neq a\}$$

is a proper subset of K_G. However, I is a strong left ideal, contradicting Lemma 3.1. □

Let $\mathrm{Aut}(G)$ denote the automorphism group of a groupoid G and let

$$\mathrm{Aut}_n(G) = \{\varphi \in \mathrm{Aut}(G) : \varphi^n = id\}.$$

It is easy to check that $\mathrm{Aut}_n(G)$ is a left n-symmetric subgroupoid of the conjugation groupoid of $\mathrm{Aut}(G)$.

Lemma 3.3. *Let K be an idempotent-free LD left quasigroup and I be a left subquasigroup of the conjugation groupoid of $\mathrm{Aut}(K)$. Let G be the disjoint union of I and K. Then the following conditions are equivalent.*

1. *The operations of I and K can be extended onto G so that G becomes an LD left quasigroup with*
$$\varphi \cdot u = \varphi(u)$$
for all $\varphi \in I$, $u \in K$.
2. *$L_u^K \varphi (L_u^K)^{-1} \in I$ and $(L_u^K)^{-1} \varphi L_u^K \in I$ for all $\varphi \in I$, $u \in K$; here L_u^K denotes the left translation of u in K.*

If the conditions are satisfied, the operation on G is uniquely determined and

$$u \cdot \varphi = L_u^K \varphi (L_u^K)^{-1} = L_u^K * \varphi$$

for all $\varphi \in I$, $u \in K$.
Moreover, G is n-LS, if and only if K is n-LS and $\varphi^n = id$ for every $\varphi \in I$.

Proof. For every $u \in K$, we need to extend the left translation L_u^K of u in K to a left translation L_u^G of u in G. Left distributivity yields for every $u, v \in K$ and $\varphi \in I$ the identity $u(\varphi v) = (u\varphi)(uv)$. Substituting $u\backslash v$ for v we obtain $u(\varphi(u\backslash v)) = (u\varphi)v$. Consequently, the automorphism $u\varphi$ maps v onto

$$u(\varphi(u\backslash v)) = L_u^K \varphi (L_u^K)^{-1}(v)$$

and thus we must set $u\varphi = L_u^K \varphi (L_u^K)^{-1}$. Of course, this is possible, iff

$$L_u^K \varphi (L_u^K)^{-1} \in I.$$

We check that all left translations in G are permutations. First, consider the translation L_φ^G, $\varphi \in I$. Then $L_\varphi^G|_I$ is a permutation, because I is a left quasigroup and $L_\varphi^G|_K = \varphi$ is indeed a permutation too. Next, consider L_u^G, $u \in K$. Then $L_u^G|_K$ is a permutation, because K is a left quasigroup, so it remains to discuss $L_u^G|_I : \varphi \mapsto L_u^K * \varphi$. This is indeed an injective mapping and it is surjective, iff for each $\varphi \in I$ there is $\psi \in I$ such that $L_u^K \psi (L_u^K)^{-1} = \varphi$, it means iff

$$(L_u^K)^{-1} \varphi L_u^K \in I$$

for every $\varphi \in I$. Note that $(L_\varphi^G)^n = id$ iff $\varphi^n = id$ and $(L_u^G)^n = id$ iff $(L_u^K)^n = id$.

Finally, we prove that G is left distributive. Since I and K are left distributive, there remain six cases of choosing variables x, y, z from I, K. An easy calculation (using Lemma 2.2 several times) shows that for every $\varphi, \psi \in I$ and $u, v \in K$

$$\begin{aligned}
\varphi(\psi u) &= \varphi(\psi(u)) = \varphi\psi\varphi^{-1}\varphi(u) = (\varphi * \psi)(\varphi u);\\
\varphi(u\psi) &= \varphi L_u \psi L_u^{-1} \varphi^{-1} = \varphi L_u \varphi^{-1} \varphi\psi\varphi^{-1} \varphi L_u^{-1} \varphi^{-1} = L_{\varphi(u)} \varphi\psi\varphi^{-1} L_{\varphi(u)}^{-1}\\
&= (\varphi u)(\varphi * \psi);\\
u(\varphi * \psi) &= L_u \varphi\psi\varphi^{-1} L_u^{-1} = (u\varphi)(u\psi);\\
u(v\psi) &= L_u L_v \psi L_v^{-1} L_u^{-1} = L_u L_v L_u^{-1} L_u \psi L_u^{-1} L_u L_v^{-1} L_u^{-1} = L_{uv} L_u \psi L_u^{-1} L_{uv}^{-1}\\
&= (uv)(u\psi);\\
u(\psi v) &= u\psi(v) = L_u \psi(v) = L_u \psi L_u^{-1}(uv) = (u\psi)(uv);\\
\psi(uv) &= \psi(u)\psi(v) = (\psi u)(\psi v).
\end{aligned}$$

□

We will denote the groupoid G constructed in Lemma 3.3 by $I \sqcup K$ and call it the *extension* of K by I. The *full extension* of K is the extension $\mathrm{Full}(K) = \mathrm{Aut}(K) \sqcup K$ and the *full n-extension* of K is $\mathrm{Full}_n(K) = \mathrm{Aut}_n(K) \sqcup K$. The multiplication table of $I \sqcup K$ looks like

$I \sqcup K$	ψ	v
φ	$\varphi\psi\varphi^{-1}$	$\varphi(v)$
u	$L_u^K \psi (L_u^K)^{-1}$	uv

We are ready to prove the main theorem, describing non-idempotent subdirectly irreducible LD left quasigroups.

Theorem 3.4. *Let G be a non-idempotent subdirectly irreducible LD left quasigroup. Then G embeds into $\mathrm{Full}(K_G)$ by an injective homomorphism Φ defined*

$$\Phi(u) = u \text{ for } u \in K_G \quad \text{and} \quad \Phi(a) = L_a|_{K_G} \text{ for } a \in Ip_G.$$

Moreover, if G is n-LS, then it embeds by Φ into $\mathrm{Full}_n(K_G)$.

Proof. First, we show that the mapping Φ is a homomorphism. Let $a, b \in G$, we prove that $\Phi(ab) = \Phi(a)\Phi(b)$. The case $a, b \in K_G$ is trivial. For a, b idempotent, we have $L_{ab} = L_a * L_b$ by Lemma 2.2. For a idempotent and $b \in K_G$, we have $\Phi(a) = L_a|_{K_G}$, $\Phi(b) = b$ and $ab \in K_G$, thus both sides are equal to ab. Finally, for $a \in K_G$ and b idempotent, $\Phi(ab) = L_{ab}|_{K_G}$ and the right side is $aL_b|_{K_G} = L_a|_{K_G} * L_b|_{K_G} = L_{ab}|_{K_G}$ according to Lemma 2.2 again.

To prove injectivity of Φ, we define an equivalence α on G by setting $(a, b) \in \alpha$ iff $a = b$ or a, b are idempotent and $L_a|_{K_G} = L_b|_{K_G}$. We show that α is a congruence of G. Assume that $(a, b) \in \alpha$ and $c \in G$. Since $L_a|_{K_G} = L_b|_{K_G}$ implies both

$$L_a L_c L_a^{-1}|_{K_G} = L_b L_c L_b^{-1}|_{K_G} \quad \text{and} \quad L_c L_a L_c^{-1}|_{K_G} = L_c L_b L_c^{-1}|_{K_G},$$

we obtain $(ac, bc) \in \alpha$ and $(ca, cb) \in \alpha$ by Lemma 2.2. So α is a congruence of G, but the intersection of α and ip_G is trivial. Since ip_G is assumed to be non-trivial, it follows that α is trivial. It means that $L_a|_{K_G} \neq L_b|_{K_G}$ for all idempotent elements $a \neq b$ and thus Φ is injective.

Finally, if G is n-LS, then it embeds into $\mathrm{Full}_n(K_G)$, because $(L_a)^n = id$. □

It follows that every subdirectly irreducible LD left quasigroup is isomorphic to some $I \sqcup K$, where K is an idempotent-free LD left quasigroup and I is a left subquasigroup of the conjugation groupoid of $\mathrm{Aut}(K)$. In further text, we will address this situation just by saying that $G = I \sqcup K$.

We proceed with three auxiliary claims.

Lemma 3.5. *Let $G = I \sqcup K$. If α is a non-trivial congruence of G, then $\alpha \cap K^2$ is a non-trivial congruence of K.*

Proof. Indeed $\alpha \cap K^2$ is a congruence. We prove that it is non-trivial. If there are $\varphi, \psi \in I$ with $(\varphi, \psi) \in \alpha$, then there is $u \in K$ such that $\varphi(u) \neq \psi(u)$ and thus $(\varphi(u), \psi(u))$ is a non-trivial pair in $\alpha \cap K^2$. So assume that $(\varphi, u) \in \alpha$ for some $\varphi \in I$ and $u \in K$. If $\varphi \neq L_u|_K$, again, there is $v \in K$ such that $\varphi(v) \neq uv$ and thus $(\varphi(v), uv)$ is a non-trivial pair in $\alpha \cap K^2$. Otherwise, if $\varphi = L_u|_K$, then $(u\varphi, uu) = (\varphi, uu) \in \alpha$ and so (u, uu) is a non-trivial pair in $\alpha \cap K^2$. □

An equivalence α is called *I-invariant*, if $(a, b) \in \alpha$ implies $(\varphi(a), \varphi(b)) \in \alpha$ for every $\varphi \in I$.

Lemma 3.6. *Let $G = I \sqcup K$ and assume that there is a non-trivial congruence ν of K such that every non-trivial I-invariant congruence of K contains ν. Then G is subdirectly irreducible and its monolith is $\mathrm{Cg}_G(\nu)$, the congruence generated by ν in G.*

Proof. Let α be an arbitrary non-trivial congruence of G. By Lemma 3.5, $\alpha \cap K^2$ is a non-trivial congruence of K and it is I-invariant because of left multiplication by elements of I in G. Consequently, $\nu \subseteq \alpha$ and thus $\mathrm{Cg}_G(\nu) \subseteq \alpha$ too. □

Proposition 3.7. *Let $G = I \sqcup K$, $H = J \sqcup K$ and $J \subseteq I$. If H is subdirectly irreducible, then G is so.*

Proof. Let α be a non-trivial congruence of G. By Lemma 3.5, $\alpha \cap K^2$ is a non-trivial congruence of K and thus $\alpha \cap H^2$ is a non-trivial congruence of H. Consequently, α contains μ_H. Thus G is subdirectly irreducible and its monolith is $\mathrm{Cg}_G(\mu_H)$. □

Let G be an LD left quasigroup and $k \geq 1$. We define a mapping

$$\rho_k : G \to G, \quad \rho_k(a) = a^k.$$

This is an automorphism of G, because $(xy)^k \approx_{LD} xy^k \approx_{LI} x^k y^k$. Moreover, ρ_k commutes with any automorphism φ of G, because $\varphi(a^k) = \varphi(a)^k$ for every $a \in G$. Consequently, $\{\rho_k\}$ is a one-element strong left ideal in $\mathrm{Full}(K)$ for any idempotent-free LD left quasigroup K. If G is a subgroupoid of $\mathrm{Full}(K)$, we will denote G^- the subgroupoid $G \setminus \{\rho_k : k \in \mathbb{N}\}$.

Proposition 3.8. *Let $G = I \sqcup K$. Then G is subdirectly irreducible, if and only if G^- is subdirectly irreducible.*

Proof. The "if" part follows from Proposition 3.7. To prove the other implication, assume that α is a non-trivial congruence of G^-. We show that α contains the congruence $\nu = \mu_G \cap (G^-)^2$ and thus that ν is the monolith of G^-. For this, it is sufficient to prove that $\alpha \cup id$ is a congruence of G — then $\alpha \cup id$ contains μ_G. So let $(a, b) \in \alpha$ and we check that

$$(\rho_k a, \rho_k b) \in \alpha \cup id \quad \text{ and } \quad (a\rho_k, b\rho_k) \in \alpha \cup id$$

for every k. In the latter case, $a\rho_k = \rho_k = b\rho_k$, because $\{\rho_k\}$ is a left ideal, hence $(a\rho_k, b\rho_k) \in id$. In the former case, observe that $\rho_k c = c^k$ for every c (for c idempotent, $\rho_k c = c$ because ρ_k commutes with any automorphism, and for c non-idempotent by definition) and thus $(\rho_k a, \rho_k b) = (a^k, b^k) \in \alpha$, since $(a, b) \in \alpha$. □

The following theorems settle conditions, when an idempotent-free LD left quasigroup possesses a subdirectly irreducible extension.

Theorem 3.9. *Let K be an idempotent-free LD left quasigroup. The following statements are equivalent:*

(1) *There is a subdirectly irreducible LD left quasigroup G with $K_G = K$.*
(2) $\mathrm{Full}(K)$ *is subdirectly irreducible.*
(3) $\mathrm{Full}(K)^-$ *is subdirectly irreducible.*

The three statements are implied by

(4) *There is a congruence ν of K such that every non-trivial* $\mathrm{Aut}(K)$*-invariant congruence of K contains ν.*

Moreover, if K has term-definable left division and cycle type $\{p^r\}$, then each of the four statements is equivalent to

(5) *Every non-trivial* $\mathrm{Aut}(K)$*-invariant congruence of K contains $\gamma_{p^{r-1}}$.*

Theorem 3.10. *Let K be an idempotent-free n-LSLD groupoid of cycle type $\{p^r\}$. The following statements are equivalent:*

(1) *There is a subdirectly irreducible n-LSLD groupoid G with $K_G = K$.*
(2) $\mathrm{Full}_n(K)$ *is subdirectly irreducible.*
(3) $\mathrm{Full}_n(K)^-$ *is subdirectly irreducible.*
(4) *Every non-trivial* $\mathrm{Aut}_n(K)$*-invariant congruence of K contains $\gamma_{p^{r-1}}$.*

We prove the first theorem only. To prove the second one, one can just replace Aut by Aut_n and Full by Full_n.

Proof. The implications (3) ⇒ (1) and (5) ⇒ (4) are trivial, (1) ⇒ (2) follows from Theorem 3.4 and Proposition 3.7, (2) ⇒ (3) follows from Proposition 3.8 and (4) ⇒ (2) follows from Lemma 3.6.

It remains to prove (2) ⇒ (5). Assume that α is a non-trivial $\mathrm{Aut}(K)$-invariant congruence of K. Let β be a union of α and

$$\{(\varphi,\psi)\in\mathrm{Aut}(K)^2:(\varphi(u),\psi(v))\in\alpha \text{ and } (\varphi^{-1}(u),\psi^{-1}(v))\in\alpha \text{ for every } (u,v)\in\alpha\}.$$

It is easy to see that β is an equivalence. We prove that β is a congruence of $\mathrm{Full}(K)$ — in this case, (2) together with Theorem 3.2 yields that $\mu_{\mathrm{Full}(K)}=\gamma_{p^{r-1}}\subseteq\beta$ and thus α contains $\gamma_{p^{r-1}}$ (on K) too.

First, let $(u,v)\in\alpha$. Then for every $w\in K$ and $\varphi\in\mathrm{Aut}(K)$

- $(uw,vw),(wu,wv)\in\beta$, because α is a congruence of K;
- $(\varphi u,\varphi v)\in\beta$, because α is $\mathrm{Aut}(K)$-invariant; and
- $(u\varphi,v\varphi)=(L_u\varphi L_u^{-1},L_v\varphi L_v^{-1})\in\beta$, because from $(x,y)\in\alpha$ follows that $(u\varphi(u\backslash x),v\varphi(v\backslash y))\in\alpha$ and also $(u\varphi^{-1}(u\backslash x),v\varphi^{-1}(v\backslash y))\in\alpha$.

Now, let $(\varphi,\psi)\in\beta\cap\mathrm{Aut}(K)$. Again, for every $u\in K$, $\rho\in\mathrm{Aut}(K)$

- $(\varphi u,\psi u)\in\alpha$ immediately from the definition of β;
- $(\varphi*\rho,\psi*\rho),(\rho*\varphi,\rho*\psi)\in\beta$ follows easily from the definition of β because of $\mathrm{Aut}(K)$-invariancy of α; and
- $(u\varphi,u\psi)$ is a particular case of the previous for $\rho=L_u$.

□

4. Examples

Let k,ℓ be positive integers. We will denote $C(k,\ell)$ the set

$$\{0,\dots,k-1\}\times\{0,\dots,\ell-1\},$$

$P(k,\ell)$ the group of all permutations π on the set $C(k,\ell)$ such that

$$\pi(i,a)=(j,b)\quad\text{implies}\quad\pi(i,a+1)=(j,b+1)$$

(here addition means mod ℓ) and

$$P_n(k,\ell)=\{\pi\in P(k,\ell):\pi^n=id\}.$$

The set $C(k,\ell)$ should be viewed as k cycles of length ℓ and $P(k,\ell)$ as the largest possible group of automorphisms.

Proposition 4.1. *Let G be a non-idempotent subdirectly irreducible LD left quasigroup of cycle type $\{1,p^r\}$ with k non-trivial ip_G-blocks. Then*

$$|G|\le kp^r+|P(k,p^r)|=kp^r+k!(p^r)^k.$$

Moreover, if G is n-LS, then

$$|G|\le kp^r+|P_n(k,p^r)|.$$

Proof. It follows from the embedding established in Theorem 3.4. □

We show that the upper bound on the number of idempotent elements is optimal. For every k and p^r, we construct a subdirectly irreducible LD left quasigroup G of cycle type $\{1,p^r\}$ with k non-trivial ip_G-blocks such that $|G|=kp^r+|P(k,p^r)|$. The bound is optimal also in the case of n-LSLD groupoids, provided n has a proper divisor not greater than k (and indeed $p^r\mid n$, because otherwise there is no such n-LSLD groupoid).

Example 4.2. Let $K = C(k, p^r)$ and put

$$(i, a) \cdot (j, b) = (j, b + 1)$$

for every $0 \leq i, j < k$ and $0 \leq a, b < p^r$. It is easy to see that K is an LD left quasigroup and $\mathrm{Aut}(K) = P(k, p^r)$. Moreover, K is n-LS iff $p^r \mid n$, and $\mathrm{Aut}_n(K) = P_n(k, p^r)$. Thus $|\mathrm{Full}(K)|$ and $|\mathrm{Full}_n(K)|$ attain the upper bound from Proposition 4.1. We prove that $\mathrm{Full}_n(K)$ is subdirectly irreducible whenever n is divisible by p^r and by some number q with $1 < q \leq k$. Consequently, $\mathrm{Full}(K)$ is subdirectly irreducible too, by Proposition 3.7.

We will use Theorem 3.10 and check the condition (4). Let α be a non-trivial $\mathrm{Aut}_n(K)$-invariant congruence of K, we show that it contains $\gamma_{p^{r-1}}$. Assume that $((i, a), (j, b)) \in \alpha$. First, if $i \neq j$, we choose the permutation π fixing all circles except for the i-th one and shifting the i-th circle by one. Indeed $\pi \in \mathrm{Aut}_n(K)$ and thus $\mathrm{Aut}_n(K)$-invariancy yields that $(\pi(i, a), \pi(j, b)) = ((i, a + 1), (j, b)) \in \alpha$ and thus we have $((i, a), (i, a + 1)) \in \alpha$. Consequently, we can assume that $i = j$ and $a \neq b$. In this case, α certainly contains the restriction of $\gamma_{p^{r-1}}$ to the i-th circle and we can use for every $j \neq i$ a permutation that sends the i-th circle onto the j-th one and get $\gamma_{p^{r-1}} \subseteq \alpha$. Indeed, $P_n(k, p^r)$ contains such a permutation whenever n has a proper divisor not greater than k.

The upper bound for n-LSLD groupoids is not necessarily reached when k is too small, i.e. when no $1 < q \leq k$ divides n. For example, we prove that there is no subdirectly irreducible 3-LSLD groupoid (of cycle type {1,3}) with two non-trivial ip-blocks, regardless the number of idempotent elements. First, note that $P_3(2, 3)$ is not transitive and the sets $\{i\} \times \{0, 1, 2\}$, $i = 0, 1$ are its orbits. Second, note that there is only one (up to isomorphism) two-element idempotent LD left quasigroup

T	☺	☹
☺	☺	☹
☹	☺	☹

Consequently, every idempotent-free 3-LSLD groupoid K with two ip_K-blocks contains two proper (strong) left ideals (namely, each of the two ip_K-blocks) and so does $\mathrm{Full}_3(K)$. Hence, according to Lemma 3.1, $\mathrm{Full}_3(K)$ is not subdirectly irreducible.

We also note that the above considerations are not limited to finite groupoids; if k is an infinite cardinal number, then the upper bound on the number of idempotents in a subdirectly irreducible LD left quasigroup with k (finite) blocks is 2^k and this bound is reached by a simple modification of Example 4.2. (The condition "$q \mid n$ for some $1 < q \leq k$" becomes trivial here.)

In the rest of the section, we discuss non-idempotent subdirectly irreducible LD left quasigroups with small number of ip-blocks.

One ip-block. Let G be a subdirectly irreducible LD left quasigroup of cycle type $\{p^r\}$ or $\{1, p^r\}$ with one non-trivial ip-block. Then K_G is isomorphic to C_{p^r}. Since C_{p^r} is subdirectly irreducible, every $I \sqcup C_{p^r}$ is subdirectly irreducible, by Proposition 3.7. It is easy to see that $\mathrm{Aut}(C_{p^r})$ is the cyclic group of order p^r, generated by the mapping $a \mapsto a + 1$. It is abelian, so every idempotent element in $\mathrm{Full}(C_{p^r})$ forms a one-element left ideal. Consequently, $I \sqcup C_{p^r}$ is a subdirectly irreducible LD left quasigroup for every subset I of $\mathrm{Aut}(C_{p^r})$. So *there are (up to* *isomorphism)* 2^{p^r} *subdirectly irreducible LD left quasigroup of cycle type* $\{p^r\}$ *or* $\{1, p^r\}$ *with one non-trivial ip-block.*

Two *ip*-blocks. Let G be a subdirectly irreducible LD left quasigroup of cycle type $\{p^r\}$ or $\{1, p^r\}$ with two non-trivial ip_G-blocks. Let's denote the blocks B_1, B_2 and their elements $B_1 = \{0, 1, \dots, p^r - 1\}$ and $B_2 = \{\overline{0}, \overline{1}, \dots, \overline{p^r - 1}\}$. Indeed both B_1 and B_2 are isomorphic to C_{p^r}, so their only automorphisms are rotations. Since K_G/ip_G is isomorphic to the unique two-element idempotent LD left quasigroup T (see above), there exist some $i, j \in \{0, \dots, p^r - 1\}$ such that K_G has the following multiplication table:

K_G	c	$\overline{d}$
a	$c+1$	$\overline{d+i}$
$\overline{b}$	$c+j$	$\overline{d+1}$

(here a, b, c, d are arbitrary elements of $\{0, \dots, p^r - 1\}$). If $i \neq j \neq 1$, then the set B_1 is definable in K_G by the formula $(\exists y)\ yx \approx x^{j+1}$, and if $i \neq j = 1$, then the set B_1 is definable in K_G by the formula $(\forall y)\ yx \approx x^2$, so both cases contradict Lemma 2.1. Hence $i = j$ and it is easy to see that

$$\mathrm{Aut}(K_G) = P(2, p^r).$$

Since $\gamma_{p^{r-1}}$ should be the monolith, we see that

- for $i = 0$, $I \sqcup K$ is subdirectly irreducible, iff I contains a permutation π such that $\pi(B_1) = B_2$.
- for $i \neq 0$, $I \sqcup K$ is subdirectly irreducible, iff I contains a permutation π such that $\pi(B_1) = B_2$ and some permutations that disallow congruences which intersect trivially with ip_G.

Let us illustrate how it works for $p^r = 2$. Let K_i, $i = 0, 1$ denote the two possibilities for K_G. The multiplication table of $\mathrm{Aut}(K_0)^- = \mathrm{Aut}(K_1)^- = \{a, b, c, d, e, f\}$, where $a = (0\ 1)$, $b = (\overline{0}\ \overline{1})$, $c = (0\ \overline{0})(1\ \overline{1})$, $d = (0\ \overline{1})(1\ \overline{0})$, $e = (0\ \overline{0}\ 1\ \overline{1})$ and $f = (0\ \overline{1}\ 1\ \overline{0})$, is

$*$	a	b	c	d	e	f
a, b	a	b	d	c	f	e
c, d	b	a	c	d	f	e
e, f	b	a	d	c	e	f

Its subgroupoids are singletons, $\{a, b\}$, $\{c, d\}$, $\{e, f\}$ and the unions of the latter three. According to the previous paragraph, the minimal subgorupoids I of $\mathrm{Aut}(K_0)^-$ such that every I-invariant congruence contains γ_1 are $\{d\}$, $\{e\}$ and $\{f\}$. Since I must satisfy also the condition (2) from Lemma 3.3, we have six subdirectly irreducible extensions: by $\{c, d\}$, $\{e, f\}$, $\{a, b, c, d\}$, $\{c, d, e, f\}$, $\{a, b, e, f\}$ and $\mathrm{Full}(K_0)^-$. For the groupoid K_1, the minimal subgroupoids are $\{e\}$, $\{f\}$ and $\{a, b, c, d\}$. Hence there are five subdirectly irreducible extensions: by $\{e, f\}$, $\{a, b, c, d\}$, $\{c, d, e, f\}$, $\{a, b, e, f\}$ and $\mathrm{Full}(K_0)^-$. Now each of these extensions can be further extended by ρ_1, ρ_2, both or none, see Proposition 3.8. Hence *there are altogether (up to isomorphism)* $4 \cdot 6 + 4 \cdot 5 = 44$ *subdirectly irreducible LD left quasigroups of cycle type* $\{1, 2\}$ *with two non-trivial ip-block.*

Three *ip*-blocks. The number of possible K_G's and the size of their automorphism groups grow rapidly. We only note that all subdirectly irreducible 2-LSLD groupoids with at most three non-trivial *ip*-blocks were computed in [9]. The table shows the number of isomorphism classes with a given number of idempotent elements. Rows represent groupoids with 1, 2 and 3 *ip*-blocks, respectively. We note that $|P_2(1,2)| = 2$, $|P_2(2,2)| = 6$ and $|P_2(3,2)| = 20$.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	2	1																		
0	0	1	2	3	4	2														
0	0	0	0	0	0	4	8	4	8	16	8	6	12	6	4	8	4	2	4	2

Summary. Here we summarize the number of isomorphism classes of subdirectly irreducible LD left quasigroups with a given number of non-idempotent elements. The second column displays the structure of K_G by the number of blocks × their type. The third column is the upper bound on the number of idempotents. In the last column one can find the number of those which are left 2-symmetric. (The blank spaces haven't been computed.)

$\|K_G\|$	structure	$\|I_G\| \le$	#	2-LSLD
1			0	0
2	$1 \times C_2$	2	4	4
3	$1 \times C_3$	3	8	0
4	$1 \times C_4$	4	16	0
	$2 \times C_2$	8	44	12
5	$1 \times C_5$	5	32	0
6	$1 \times C_6$	—	0	0
	$2 \times C_3$	18		0
	$3 \times C_2$	48	> 96	96
7	$1 \times C_7$	7	128	0
8	$1 \times C_8$	8	256	0
	$2 \times C_4$	32		0
	$4 \times C_2$	384		

References

[1] V. D. Belousov, *Основы теории квазигрупп и луп (Foundations of theory of quasigroups and loops),* Nauka Moskva, 1967 (Russian).

[2] E. Brieskorn, *Automorphic sets and singularities,* Contemp. Math. 78 (1988), 45–115.

[3] S. Burris, H.P. Sankappanavar, *A course in universal algebra,* GTM 78, Springer, 1981.

[4] P. Dehornoy, *Braids and self-distributivity,* Progress in Math. 192, Birkhäuser Basel, 2000.

[5] R. Dougherty, T. Jech, *Finite left-distributive algebras and embedding algebras,* Adv. Math. 130/2 (1997), 201–241.

[6] A. Drápal, T. Kepka, M. Musílek, *Group conjugation has non-trivial LD-identities,* Comment. Math. Univ. Carolinae, 35/2 (1994), 219–222.

[7] R. Fenn, C. Rourke, *Racks and links in codimension two,* J. Knot Theory Ramifications 1 (1992), 343–406.

[8] P. Jedlička, *On left distributive left idempotent groupoids,* Comment. Math. Univ. Carol., 46/1 (2005) 15–20.

[9] E. Jeřábek, T. Kepka, D. Stanovský, *Subdirectly irreducible non-idempotent left symmetric left distributive groupoids,* to appear in Discussiones Math. – General Algebra and Appl.

[10] D. Joyce, *A classifying invariant of knots, the knot quandle,* J. Pure Appl. Alg. 23 (1982), 37–66.

[11] D. Joyce, *Simple quandles,* J. Alg. 79 (1982), 307–318.

[12] T. Kepka, *Non-idempotent left symmetric left distributive groupoids,* Comment. Math. Univ. Carolinae, 35 (1994), 181-186.

[13] T. Kepka, P. Němec, *Selfdistributive groupoids. A1. Non-indempotent left distributive groupoids,* Acta Univ. Carolin. Math. Phys. 44/1 (2003), 3–94.

[14] D. Larue, *Left-distributive idempotent algebras,* Commun. Alg., 27/5 (1999), 2003–2009.

[15] R. Laver, *The left distributive law and the freeness of an algebra of elementary embeddings,* Adv. Math. 91/2 (1992), 209–231.

[16] S. V. Matveev, *Distributive groupoids in knot theory,* Math. USSR – Sbornik, 47/1 (1984), 73–83. (Mat. Sbornik 119/1 (1982) in Russian)

[17] N. Nobusawa, *Some structure theorems on pseudo-symmetric sets,* Osaka J. Math. 20 (1983), 727–734.

[18] N. Nobusawa, *On a construction of exceptional pseudo-symmetric sets,* Osaka J. Math. 21 (1984), 701–706.

[19] N. Nobusawa, *Jordan-Hölder theorem for pseudo-symmetric sets,* Osaka J. Math. 23 (1986), 853–858.

[20] B. Roszkowska-Lech, *Subdirectly irreducible symmetric idempotent entropic groupoids,* Demonstratio Math. 32/3 (1999), 469–484.

[21] H. Ryder, *The congruence structure of racks,* Commun. Alg. 23 (1995), 4971–4989.

[22] D. Stanovský, *Left distributive left quasigroups,* PhD Thesis, Charles University in Prague, 2004. Available at `http://www.karlin.mff.cuni.cz/~stanovsk/math/disert.pdf`

[23] D. Stanovský, *On equational theory of group conjugation,* Contributions To General Algebra 15 (2004), Proceedings of the Klagenfurt Workshop AAA66, 177–185.

[24] D. Stanovský, *On varieties of left distributive left idempotent groupoids,* Discussiones Math. – General Algebra and Appl. 24/2 (2004), 267–275.

[25] D. Stanovský, *Left symmetric left distributive operations on groups,* Algebra Universalis 54/1 (2005), 97–103.

David Stanovský, Charles University in Prague, Czech Republic
E-mail address: `stanovsk@karlin.mff.cuni.cz`