BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(49), 2005, Pages 153–164
ISSN 1024–7696

Cores of Bol loops and symmetric groupoids [*]

A. Vanžurová

Abstract. The notion of a core was originally invented by R.H. Bruck for Moufang loops, [3], and the construction was generalized by V.D. Belousov for quasigroups in [2] (we will discuss 1-cores here). It is well known that cores of left Bol loops, particularly cores of Moufang loops, or groups, are left distributive, left symmetric, and idempotent, [2]. Among others, our aim is to clarify the relationship between cores and the variety of left symmetric left distributive idempotet groupoids, $\underline{SID}$, or its medial subvariety, $\underline{SIE}$, respectively. The class of cores of left Bol loops is not closed under subalgebras, therefore is no variety (even no quasivariety), and we can ask what variety is generated by cores: the class of left Bol loop cores (even the class of group cores) generates the variety of left distributive left symmetric idempotent groupoids, while cores of abelian groups generate the variety of idempotent left symmetric medial groupoids.

It seems that the variety $\underline{SID}$ of left distributive left symmetric idempotent groupoids (”symmetric groupoids”) aroused attention especially in connection with symmetric spaces in 70' and 80' [15, 16, 18, 19] and the interest continues. Recently, it was treated in [8, 26, 27], and also in [29], from the view-point of hypersubstitutions. The right symmetric idempotent and medial case was investigated e.g. in [1, 21–24].

Mathematics subject classification: 20N05.
Keywords and phrases: Groupoid, variety of algebras, quasigroup, loop, Bol identity, core.

1 Preliminaries

We use the standard notation of universal algebra here, [5–7]. $T_\tau(X)$ denotes the set of all terms of a type τ over a non-empty set X. An algebra with the carrier set A and the sequence $F = (f_i)_{i\in I}$ of operation symbols is denoted by $\mathcal{A} = (A; F)$. The fundamental operation corresponding to the operation symbol f_i in the algebra $\mathcal{A}$ is denoted by ${f_i}^{\mathcal{A}}$. If $\mathcal{A} = (A; F)$ is an algebra and $\tilde{F} = (f_i)_{i\in\tilde{I}}$, $\tilde{I} \subset I$ a subsequence of the sequence F of operation symbols then $\tilde{\mathcal{A}} = (A; \tilde{F})$ is called a *reduct* of $\mathcal{A}$, [20].

If the class V of algebras is defined by identities, i.e. is a variety of algebras (equivalently speaking, is closed under homomorphic images of subalgebras of products), [6], let us denote it by $\underline{V}$, and denote $Id\underline{V}$ the set of all identities valid in $\underline{V}$. If Σ is the defining set of identities of the variety $\underline{V}$ we write $\underline{V} = Mod(\Sigma)$ (Mod means ”models”).

More generally, a class of algebras closed under subalgebras and products is called a *quasivariety.*

[*] Supported by grant No̊201/05/2707 of The Grant Agency of Czech Republic.

2 Symmetric groupoids

2.1 Some identities in groupoids. Under *left* (*right*) *cancellation* we understand the quasi-identity $(C_l) : xy = xy' \Rightarrow y = y'$ (or $(C_r) : xy = x'y \Rightarrow x = x'$, respectively). We will pay attention to the following identities:

(S_l) $x \cdot (x \cdot y) = y$ (left symmetry);
(S_l) $x \cdot (y \cdot z) = (x \cdot y) \cdot (x \cdot z)$ (left self-distributivity);
(I) $x \cdot x = x$ (idempotency);
(E) $(x \cdot y) \cdot (z \cdot u) = (x \cdot z) \cdot (y \cdot u)$ (mediality, or entropy).

Note that the identity (S_l) is also called left keyes identity [10]. Consider the variety of *left symmetric* groupoids $\underline{S} = Mod(S_l)$. Analogously, *right symmetric* groupoids are introduced by the mirror identity (S_r): $(y \cdot x) \cdot x = y$ and form a variety $\underline{RS} = Mod(S_r)$. Evidently, due to the mirror symmetry of both theories, it is sufficient to investigate one of them, we prefer the left one.

Any left symmetric groupoid $\mathcal{A} = (A; \cdot) \in \underline{S}$ is left cancellative, and left translations $L_a : x \mapsto ax$, $a, x \in A$, are permutations of the underlying set. A groupoid is left symmetric if and only if every left translation is an involutive permutation. Any left translation may be decomposed into disjoint cycles of length at most two. Moreover, the algebra $(A; \cdot, \cdot)$ is a left quasigroup (indeed, if $c = a \cdot b$ then $b = a \cdot c$ for $a, b, c \in A$, another speaking, $u = a \cdot b$ is a unique solution in A of the equation $a \cdot u = b$ with $a, b \in A$). Analogously for right translations in the right symmetric case.

A groupoid $(A; \cdot)$ is idempotent iff each singleton $\{a\}$ is a subalgebra. A product of n copies of $a \in A$ is again a, independently of the placement of brackets. Not much can be proved about $\underline{I} = Mod(I)$, but idempotency combined with further identities leads to more interesting structures.

Medial idempotent groupoids are distributive (i.e. left and right distributive).

Mediality of a groupoid $(A; \cdot)$ means that the basic operation yields a homomorphism $(a, b) \mapsto ab$, $(A^2; \cdot) \to (A; \cdot)$. The following consequence of mediality might be of some interest: the set of endomorphisms of a medial groupoid is closed under multiplication (which is not the case for groupoids in general):

Lemma 2.1. *Let $\mathcal{A} = (A; \cdot)$ be a medial groupoid, and $End(\mathcal{A})$ the set of its endomorphisms. Given φ, $\psi \in End(\mathcal{A})$, define $(\varphi \cdot \psi)(x) := \varphi(x) \cdot \psi(x)$. Then $\varphi \cdot \psi \in End(\mathcal{A})$.*

Proof. In fact, given $\mathcal{A}$ medial, φ, $\psi \in End(\mathcal{A})$ and $a, b \in A$ we calculate $(\varphi \cdot \psi)(a \cdot b) = \varphi(a \cdot b) \cdot \psi(a \cdot b) = (\varphi(a) \cdot \varphi(b)) \cdot (\psi(a) \cdot \psi(b)) = (\varphi(a) \cdot \psi(a)) \cdot (\varphi(b) \cdot \psi(b)) = ((\varphi \cdot \psi)(a)) \cdot ((\varphi \cdot \psi)(b))$. □

Let us consider $\underline{SI} = Mod(\{(S_l), (I)\})$, i.e. groupoids which are both idempotent and left symmetric. In $\underline{SI}$ the following holds: $x^n \cdot y^m = x \cdot y$ for $n, m \in \mathbb{N}$,

$\underbrace{x \cdot (x \cdot (\cdots \cdot (x \cdot y) \dots))}_{k\text{-times}} = y$ for k even, $\underbrace{x \cdot (x \cdot (\cdots \cdot (x \cdot y) \dots))}_{k\text{-times}} = x \cdot y$ for k odd,

$$x^m \cdot (x^n \cdot y) = x \cdot y \text{ for } k \text{ even, } x^m \cdot (x^n \cdot y) = y \text{ for } k \text{ odd.}$$

In the variety of left distributive groupoids $\underline{D} = Mod(\{(D_l)\})$, the identities $x(yx) = (xy)(xx)$, $x(xy) = (xx)(xy)$ and $x(xx) = (xx)(xx)$ hold. In $\underline{SD} = Mod(\{(S_l),(D_l)\})$, the identities $x(yz) = (x(y(xz))$, $x(xy{\cdot}xz) = yz$, $y(yx{\cdot}z) = x(yz)$ and $y(yx\cdot y) = x(yy)$ are satisfied. Quasigroups belonging to $\underline{SD}$ are sometimes called *reflection quasigroups* [10] or *left-sided* quasigroups.

Left distributive quasigroups are idempotent:

Lemma 2.2. *Let $(A;\cdot,\backslash,/)$ be a quasigroup*[1] *such that the groupoid $(A;\cdot)$ is left distributive. Then*

(i) $(A;\cdot)$ *is idempotent,*

(ii) for any $a \in A$, if $a\cdot b = b$ then $b = a$.

Proof. Let $a, b \in A$. Then $b\cdot a \underset{(D_l)}{=} b\cdot(b\cdot(b\backslash a)) \underset{(D_l)}{=} (b\cdot b)\cdot(b\cdot(b\backslash a)) = (b\cdot b)\cdot a$, and we use (C_r). Cancelling a, we obtain $b\cdot b = b$, i.e. (i) holds, and (ii) is a consequence. □

In algebra and geometry, examples of algeras belonging to the variety $\underline{SID} = Mod(\{(S_l),(I),(D_l)\})$ of left symmetric left self-distributive idempotent groupoids arise in a natural way. E.g. let us mention cores of left Bol loops, particularly of Moufang loops and groups. Another famous class of (infinite) examples comes from differential geometry, [12]: a symmetric space is in fact an $\underline{SID}$-groupoid defined on a smooth manifold such that the binary operation is a smooth map (with respect to the manifold structure), and a certain local condition is satisfied. If we accept only topological structure we can say that a *symmetric space* $(A;*,\mathcal{T})$ is a groupoid $(A;*) \in \underline{SID}$ together with a topology $\mathcal{T}$ on A such that the binary operation $*$ is continuous and satisfies: each $a \in A$ has a neighborhood $U \subset A$ such that for all $u \in U$, if $a * u = u$ then $u = a$.

$\underline{SID}$-groupoids, or their mirrors, right distributive right symmetric idempotent groupoids (forming the variety $\underline{RSID}$), are known and studied under various names. They were introduced by M. Takasaki in [29] as *kei*, investigated as *symmetric groupoids* in [15, 16], they were also called *symmetric sets* in the finite case, [18] etc. They can be described even in the terminology of quandles (structures with two binary operations, which were used as classifying invariants for knots, [9]): $\underline{RSID}$ may be regarded equivalent with the variety of the so called involutory quandles.

For the sake of brevity, $x_1x_2\ldots x_{n-1}x_n$ stands for $x_1(x_2\ldots(x_{n-1}x_n)\ldots)$, $n \geq 2$; such products will be called *right associated*).

Lemma 2.3. *In $\underline{SID}$, the following identities hold:*

(i) $(xy)z = x(y(xz))$,

(ii) $(y_1y_2\ldots y_{m-1}y_m)\cdot z = y_1y_2\ldots y_{m-1}y_my_{m-1}\ldots y_2y_1z$,

(iii) $(xy)x = x(yx)$.

Proof. First, $x(y(xz)) = (xy)(x(xz)) = (xy)z$ by left distributivity and left symmetry. To prove (ii) we either use (i) $(m-1)$-times, or go by induction on m: for

[1] For the terminology from the theory of quasigroups and loops, e.g. [2, 17].

$m = 2$, the formula follows from (i). Assume that (ii) holds for a natural number $m \geq 2$. Then by (i) and the induction assumption

$$(y_1 y_2 \dots y_m y_{m+1}) \cdot z = (y_1 [y_2 \dots y_m y_{m+1}]) \cdot z \ =$$

$$= y_1([y_2 \dots y_m y_{m+1}](y_1 z)) = y_1(y_2(\dots(y_m(y_{m+1}(y_m(\dots(y_2(y_1 z)\dots).$$

Hence the statement holds for $m+1$, and therefore for all $m \geq 2$. (iii) is a consequence. □

It was noted that group cores are not the only natural examples of $\underline{SID}$-groupoids arising from groups. Given a group $\mathcal{G}$ and an involutory automorphism $f \in Aut(\mathcal{G})$ of the group $\mathcal{G}$, the carrier set G along with the binary operation $(a,b) \mapsto a \diamond_f b := af(a^{-1}b)$ is an $\underline{SID}$-groupoid $(G; \diamond_f)$. If for all x from $\mathcal{G}$, $xf(x)$ is in the center $Z(\mathcal{G})$ for an involutory automorphism $f \in Aut(\mathcal{G})$ of the group $\mathcal{G}$ then $(G; \star_f)$ is also an $\underline{SID}$-groupoid where $a \star_f b = af(ba^{-1})$. The medial case will be discussed separately.

3 Cores of left Bol loops

3.1 Bol loops and cores. Originally, cores were introduced by R.H. Bruck in connection with invariants of isotopism classes of Moufang loops (isotopic Moufang loops have isomorphic cores [3, p. 120–121]). A more general definition was created by V.D. Belousov [2, p. 157]: a *(left) core* (in Russian, 1-*serdcevina*) of a loop $\mathcal{Q} = (\mathcal{Q}; \cdot, \backslash, /, \rceil)$ is a groupoid $Core(\mathcal{Q}) := (\mathcal{Q}; \circ)$ with

$$(a,b) \mapsto a \circ b := a(b \backslash a). \tag{3.1}$$

Under a left Bol loop we usually understand a loop (i.e. a quasigroup with identity element) which satisfies

(B_l) $\quad x(y(xz)) = (x(yx))z$ $\quad$ (left Bol identity).

Alternatively, the variety of left Bol loops may be introduced also in type $(2,1,0)$ and signature $(\cdot, ^{-1}, e)$, e.g. as

$$\underline{B} = Mod(\{xe = ex = x, (x^{-1})^{-1} = x, x^{-1}(xy) = y, (B_l)\}).$$

For a left Bol loop $\mathcal{B} = (\mathcal{Q}; \cdot, ^{-\infty}, \rceil) \in \underline{\mathcal{B}}$, the core operation takes the form $a \circ b := a \cdot (b^{-1} \cdot a)$, $a, b \in Q$. Particularly, for Moufang loops (including groups), $a \circ b = ab^{-1}a$ (brackets are not necessary since each pair of elements generates a subgroup). For commutative groups, the core operation is more famous in the notation $a \circ b = 2a - b$.

3.2 Cores as examples of symmetric groupoids. A core $Core(\mathcal{B}) = (\mathcal{Q}; \circ)$ of a Bol loop satisfies the identities (S_l), (D_l) and (I). The proof given by V.D. Belousov in [2, p. 211–215] is based on geometrical considerations, namely on evaluation of coordinates of points and lines in the corresponding Bol net. Let us give here a purely algebraic proof of the statement[2].

[2] Another proof is given in [14, p. 102].

Proposition 3.1. *The core $Core(\mathcal{B})$ of a Bol loop $\mathcal{B} \in \underline{B}$ satisfies:*

$$[a \circ b]^{-1} = a^{-1} \circ b^{-1} \quad \textit{for} \quad a, b \in Q \quad (\textit{automorphic inverse property}),$$

$$[a_n \circ a_{n-1} \circ \cdots \circ a_2 \circ a_1]^{-1} = a_n^{-1} \circ a_{n-1}^{-1} \circ \cdots \circ a_2^{-1} \circ a_1^{-1}, \quad n \geq 2.$$

Proof. Using (B_l), $(x^{-1})^{-1} = x$, and left inverse property we get $a^{-1} \circ b^{-1} = a^{-1}((b^{-1})^{-1}a^{-1}) = a^{-1}(ba^{-1})$, and $(a \circ b) \cdot (a^{-1} \circ b^{-1}) = (a(b^{-1}a)) \cdot (a^{-1}(ba^{-1})) = e$. Hence the second formula holds for $n = 2$. Suppose it holds for a fixed natural number $n \geq 2$. Then $[a_{n+1} \circ (a_n \circ a_{n-1} \circ \cdots \circ a_2 \circ a_1)]^{-1} = a_{n+1}^{-1} \circ [a_n^{-1} \circ a_{n-1}^{-1} \circ \cdots \circ a_2^{-1} \circ a_1^{-1}]$ as claimed. □

Proposition 3.2. *For any left Bol loop $\mathcal{B} \in \underline{B}$, the core $Core(\mathcal{B})$ belongs to the variety $\underline{SID}$.*

Proof. Let $(Q; \circ)$ be a core of a Bol loop and $a, b, c \in Q$. Then $a \circ a = a(a^{-1}a) = a \cdot e = a$, and (I) holds. Further,

$$a \circ (a \circ b) = a \circ \big(a(b^{-1}a)\big) = a\big([a(b^{-1}a)]^{-1}a\big) = a\big((a^{-1}(ba^{-1})) \cdot a\big) \underset{(B_l)}{=}$$

$$\underset{(B_l)}{=} a \cdot \big(a^{-1}[b(a^{-1}a)]\big) = a(a^{-1}b) = b$$

which proves (S_l). To prove (D_l) we can either use the fact that $[x(y^{-1}x)]^{-1} = x^{-1}(yx^{-1})$ is satisfied in $\underline{B}$,

$$a \circ (b \circ c) = a \circ (b \circ (a \circ (a \circ c))) = a\big([b \circ (a \circ (a \circ c))]^{-1}a\big) =$$

$$= a\big(\big[b \circ (a((a \circ c)^{-1}a))\big]^{-1}a\big) = a\big(\big[b([a((a \circ c)^{-1}a)]^{-1}b)\big]^{-1}a\big) =$$

$$= a\big(\big[b^{-1}([a((a \circ c)^{-1}a)]b^{-1})\big]a\big) \underset{(B_l)}{=} a\big(b^{-1}([a((a \circ c)^{-1}a)](b^{-1}a))\big) =$$

$$= a\big(b^{-1}[a((a \circ c)^{-1} \cdot (a(b^{-1}a)))]\big) = (a \circ b) \cdot \big((a \circ c)^{-1} \cdot (a \circ b)\big) = (a \circ b) \circ (a \circ c),$$

another way is to apply Proposition 3.1. □

Cores of differentiable loops are studied in [14] and in [13, p. 299–307].

3.3 Cores of groups, normal forms for terms. The subclass constituted in $\underline{SID}$ by all cores of groups is no variety, even no quasivariety. The reason is that it is not closed under subgroupoids: in cores of groups there might exist $\underline{SID}$-subgroupoids which do not arise as cores of subgroups (consequently, the same for the class of cores of Moufang loops, or cores of Bol loops, respectively). E.g. in the non-entropic $\underline{SID}$-groupoid $Core(S_3)$ there is a non-entropic subgroupoid of order four which is neither a group core nor a Bol loop core:

Example 3.1. The first non-commutative group is the symmetric group S_3, the permutation group of the three-element set. Let us denote $\Pi_1 = id$, $\Pi_2 = (2, 3)$, $\Pi_3 = (1, 2, 3)$, $\Pi_4 = (1, 2)$, $\Pi_5 = (1, 3)$, $\Pi_6 = (1, 3, 2)$. Under the isomorphism

$\Pi_k \mapsto k$, $Core(S_3)$ is isomorphic with a groupoid on a six-element set $A = \{1, \dots, 6\}$ endowed with a binary operation ”$\circ$” defined by a multiplication table the rows of which (=left translations in the core $Core(S_3) = (A, \circ)$) are given as follows: $L_1 = (3,6)$, $L_2 = (4,5)$, $L_3 = (1,6)$, $L_4 = (2,5)$, $L_5 = (2,4)$, $L_6 = (1,3)$ (cycles of length two). Mediality does not hold in the core of S_3. In fact, there exists a four-element subgroupoid with the carrier set $B = \{2,3,4,5\}$ which is not medial since $(3 \circ 4) \circ (2 \circ 5) = 4$ while $(3 \circ 2) \circ (4 \circ 5) = 2$. $(B, \circ)$ cannot be a core of a group. Indeed, up to isomorphism, there are only two groups of order four, the cyclic group Z_4 and the direct product $Z_2 \oplus Z_2$, [M. Hall Jr., The Theory of Groups, 1959]. Both are abelian, therefore must have medial cores.

But $(B, \circ)$ cannot be a core of a Bol loop, either. By R.P. Burn, [4], any Bol loop of order $2p$ and p^2, p prime, is necessarily a group.

We can ask for the variety generated by cores. Let $\underline{CG} = \langle \{Core(\mathcal{G}) | \mathcal{G} \in \underline{\mathcal{G}}\} \rangle$ denote the subvariety generated by the set of group cores in the variety $\underline{SID}$. Similarly, we might assume the subvariety $\underline{CM}$ generated by cores of Moufang loops, or $\underline{CB}$ generated by cores of left Bol loops, respectively, and the corresponding chain of subvarieties, but it appears that it is quite sufficient to consider group cores only.

Lemma 3.1. *The varieties $\underline{SID}$ and $\underline{CG}$ are identical (and consequently coincide also with $\underline{CB}$, $\underline{CM}$).*

This fact apperas already in [15, 4.12]. The statement follows e.g. from the result of [26, 27]: $\underline{SID}$ is generated by cores of groups. As a (weaker) consequence, $\underline{SID}$ is generated by cores of left Bol loops. The explanation is as follows. With respect to the variety $\underline{SID}$, any term $t \in T_{(2)}(X)$ is equivalent to a (right associated) term of the form

$$w = x_1 x_2 \dots z_{n-1} x_n, \quad z_{i+1} \neq x_i, \quad i = 1, \dots, n-1, \quad x_1, \dots, x_n \in X. \tag{3.2}$$

The proof goes on induction on complexity of terms: for a variable $t \equiv x \in X$, the statement is trivial. Let $t = t_1 t_2$ be a composed term, and let $t_1 = y_1 y_2 \dots y_{m-1} y_m$, $t_2 = z_1 \dots z_k$ are of the form (3.2). The identity (ii) from Lemma 2.3 gives

$$t_1 \cdot t_2 = y_1 y_2 \dots y_{m-1} y_m y_{m-1} \dots y_2 y_1 t_2,$$

and if $y_1 \neq z_1$ we are done. If $y_1 = z_1$ we may use left symmetry repeatedly to get rid of equal subsequent couples of variables with exception of the last two places. If the last two variables are equal then one of them can be skipped according to (I). We obtain the desired form.

Now we would like to check that (3.2) are normal forms for terms. It remains to show that for each term $t \in T_{(2)}(X)$, a term w of the form (3.2) equivalent to t in $\underline{SID}$ is uniquely determined. The proof is rather standard. Let $Z = \{z_1, z_2, \dots\}$ be a (fixed) countable infinite set. In the core $Core(\mathcal{F}_{\underline{B}}(Z)) = (T_{(2,1,0)}(Z)/Id\,\underline{B}; \circ)$ of the free Bol loop $\mathcal{F}_{\underline{B}}(Z) = (T_{(2,1,0)}(Z)/Id\,\underline{B}; \cdot, ^{-1}, e)$ freely generated by the alphabet Z (or particularly, in the core of the free group), the following formula holds for $n \geq 2$:

$$z_n \circ z_{n-1} \circ \cdots \circ z_2 \circ z_1 = z_n z_{n-1}^{-1} \dots z_2^{\epsilon_2} z_1^{\epsilon_1} z_2^{\epsilon_2} \dots z_{n-1}^{-1} z_n, \quad \epsilon_i = (-1)^{n-i}. \tag{3.3}$$

For $n = 2$, the formula holds by definition of $\circ$. We proceed by induction on n. Let (3.3) be satisfied for a fixed natural number $n \geq 2$. Let us evaluate $z = z_{n+1} \circ (z_n \circ (z_{n-1} \circ (\dots (z_2 \circ z_1) \dots))$ for $z_1, \dots, z_{n+1} \in Z$. We obtain

$$z = z_{n+1} \cdot ([z_n \circ (z_{n-1} \circ \dots \circ z_2 \circ z_1)]^{-1} \cdot z_{n+1}]) =$$

$$= z_{n+1} \cdot ([z_n^{-1} \circ z_{n-1}^{-1} \circ \dots \circ z_2^{-1} \circ z_1^{-1}] \cdot z_{n+1}) =$$

$$= z_{n+1} \cdot z_n^{-1} \cdot z_{n-1} \cdot \dots \cdot z_2^{-\epsilon_2} \cdot z_1^{-\epsilon_1} \cdot z_2^{-\epsilon_2} \dots z_{n-1} \cdot z_n^{-1} \cdot z_{n+1}.$$

Hence the power of z_i is now $-\epsilon_i = (-1)^{n+1-i}$.

In the $\underline{SID}$-groupoid $Core(\mathcal{F}_{\underline{B}(Z)})$, let us consider the subgroupoid $\mathcal{Z}$ generated by the set Z. Let us identify term variables $z_1, z_2, \dots$ from the alphabet Z with elements of the basis Z of $\mathcal{Z}$. Keeping the above notation we prove that words of the form (3.2) must be pairwise non-equivalent.

Let w, w' be a couple of different terms in the standard form (3.2). Then $w^{\mathcal{Z}}$, $w'^{\mathcal{Z}}$ are different term functions of the groupoid $\mathcal{Z}$. Indeed, let $z_1, \dots, z_n \in Z$ with $z_{i+1} \neq z_i$ for $i = 1, \dots, n-1$, and apply the term function $w^{\mathcal{Z}}$. We obtain $w^{\mathcal{Z}}(z_1, \dots, z_n) = z_n z_{n-1}^{-1} \dots z_i^{\epsilon_i} \dots z_2^{\epsilon_2} z_1^{\epsilon_1} z_2^{\epsilon_2} \dots z_{n-1}^{-1} z_n$, $\epsilon_i = (-1)^{n-i}$. Clearly, the last expression cannot be reduced by means of Bol loop identities $Id\,\underline{B}$ (or by group identities $Id\,\underline{G}$, either) since the subsequent variables are different.

That is why two different terms of the form (3.2) yield different term functions in the algebra $\mathcal{Z} \in \underline{\mathcal{SID}}$. Hence elements of the free $\underline{SID}$-groupoid $\mathcal{F}_{\underline{SID}}(Z) = (T_{(2)}(Z)/Id\,\underline{SID}, \text{juxtaposition})$ freely generated by our set Z can be presented exactly as words of the form (3.2) which proves

Lemma 3.2. *For each term t of the free $\underline{SID}$-groupoid $\mathcal{F}_{\underline{SID}}(X)$, $X \neq \emptyset$, there exists a unique right associated term w of the form (3.2) which is equivalent to t in $\underline{SID}$.*

Let us call w the *normal form* of t in $\underline{SID}$ and write $NF(t) := w$.

Keeping convention about omitting brackets let us introduce a mapping $\mathcal{L} : \mathcal{F}_{\underline{SID}}(Z) \to \mathcal{Z}$ as follows. For any equivalence class $[w]$ where $w \in T_{(2)}(X)$ with $NF(w) = z_1 z_2 \dots z_{n-1} z_n$ define $\mathcal{L}([w]) := z_1 \circ z_2 \circ \dots \circ z_{n-1} \circ z_n$.

Lemma 3.3. *The mapping $\mathcal{L} : \mathcal{F}_{\underline{SID}}(Z) \to \mathcal{Z}$, $\mathcal{L}([z_1(z_2(\dots(z_{n-1}z_n)\dots))]) = z_1 \circ (z_2 \circ (\dots \circ (z_{n-1} \circ z_n) \dots))$ is an isomorphism of groupoids.*

Proof. We have proven already that two different terms of the form (3.2) (representants of different classes) are mapped onto different elements in the algebra $\mathcal{Z}$. So $\mathcal{L}$ is injective. $\mathcal{L}$ is also surjective since according to Lemma 2.3 (ii), each element of $\mathcal{Z}$ can be written in a (reduced) right associated form $z_1 \circ \dots \circ z_n$, and hence considered as an image of a word from the free algebra. Let us verify that $\mathcal{L}([ts]) = \mathcal{L}([t]) \circ \mathcal{L}([s])$ holds. In fact, let $t = x_1 \dots x_n$, $s = y_1 \dots y_m$ be terms from $T_{(2)}(X)$ written in normal form (3.2). Then $\mathcal{L}([t]) = x_1 \circ x_2 \circ \dots \circ x_{n-1} \circ x_n$, $\mathcal{L}([s]) = y_1 \circ y_2 \circ \dots \circ y_{m-1} \circ y_m$, $NF([ts]) = x_1 \dots x_n \dots x_1 y_1 \dots y_m$, $\mathcal{L}([ts]) = \mathcal{L}([NF(ts)]) = x_1 \circ \dots \circ x_n \circ \dots \circ x_1 \circ y_1 \circ \dots \circ y_m$. Finally, again by (ii) from Lemma

2.3, $\mathcal{L}([t]) \circ \mathcal{L}([s]) = (x_1 \circ \cdots \circ x_n) \circ (y_1 \circ \cdots \circ y_m) = x_1 \circ \cdots \circ x_n \circ \cdots \circ x_1 \circ y_1 \circ \cdots \circ y_m$, and $\mathcal{L}$ is a homomorphism. □

Consequently, due to isomorphism, $\mathcal{F}_{\underline{SID}}(Z)$, $\mathcal{Z} \in \underline{\mathcal{CG}}$ and $\mathcal{Z} \in \underline{\mathcal{CB}}$ are free infinitely generated algebras in $\underline{SID}$. Hence we obtain

Corollary 3.1. *The varieties* $\underline{CB}$, $\underline{CG}$ *and* $\underline{SID}$ *are equivalent.*

Remark 3.1. In the core $Core(\mathcal{F}_{\underline{CML}}(Z))$ of the free commutative Moufang loop $\mathcal{F}_{\underline{CML}}(Z)$ over Z,

$$z_n \circ z_{n-1} \circ \cdots \circ z_2 \circ z_1 = z_n^2 z_{n-1}^{-2} \ldots z_2^{2\epsilon_2} z_1^{\epsilon_1}, \quad \epsilon_i = (-1)^{n-i} \tag{3.4}$$

holds for $n \geq 2$ (the same formula is satisfied for commutative groups). In fact, we can write (using flexibility, left alternative law and (B_l))

$$z_n((z_{n-1}^{-1}([\ldots[z_2^{\epsilon_2}(z_1^{\epsilon_1} z_2^{\epsilon_2})]\ldots]z_{n-1}^{-1})z_n) = z_n((z_{n-1}^{-1}([\ldots[z_2^{\epsilon_2}(z_2^{\epsilon_2} z_1^{\epsilon_1})]\ldots]z_{n-1}^{-1})z_n) =$$

$$= z_n((z_{n-1}^{-1}([\ldots(z_3^{\epsilon_3}([z_2^{2\epsilon_2} z_1^{\epsilon_1}]z_3^{\epsilon_3}))\ldots]z_{n-1}^{-1})z_n) =$$

$$= z_n((z_{n-1}^{-1}([\ldots(z_3^{2\epsilon_3}[z_2^{2\epsilon_2} z_1])\ldots]z_{n-1}^{-1})z_n) = \cdots = z_n^2(z_{n-1}^{-2}(\ldots(z_2^{2\epsilon_2} z_1^{\epsilon_1})\ldots)).$$

In $\underline{CML}$, the last word cannot be reduced (obviously, it can be reduced for commutative groups).

4 Mediality

4.1 $\underline{SIE}$-groupoids and mediality of group cores.

First let us pay attention to commutative groups. Denote by $\underline{AG}$ the variety of abelian groups, and by $\underline{CAG}$ the subvariety generated by cores of abelian groups in the variety $\underline{SID}$. Cores of commutative groups are medial. Indeed, for x, y, z, u from $\mathcal{G} \in \underline{\mathcal{AG}}$, $(x \circ y) \circ (z \circ u) = (x^2 y^{-1})^2 (z^2 u^{-1})^{-1} = (x^2 z^{-1})(y^2 u^{-1})(x^2 z^{-1}) = (x \circ z) \circ (y \circ u)$, hence (E) is satisfied.

Let $\underline{SIE} = Mod(\{(S_l), (I), (E)\})$. Groupoids of this variety are (left and right) distributive, elastic (=flexible), and may be regarded as a generalization of distributive quasigroups.

Note that cores of abelian groups appear also as important examples of modes. Right symmetric idempotent and medial groupoids are named *kei modes* in [19, p. 88–89]. The variety $\underline{RSIE} = Mod(\{(S_r), (I), (E)\})$ was investigated in [1, 21–24] (and denoted SIE).

Example 4.1. Let $x \circ y := 2x - y$ for $x, y \in \mathbb{R}$. Then $(\mathbb{R}; \circ)$ is a $\underline{SIE}$-groupoid, and $(\mathbb{Z}; \circ)$ is its subgroupoid ($\mathbb{R}$ are reals, $\mathbb{Z}$ denotes integers). In geometric words, $x \circ y$ is a point reflexion at x of the point y on the real line. The free $\underline{SIE}$-groupoid on two generators $\mathcal{F}_{\underline{SIE}}(\{x, y\})$ is isomorphic to the core $\mathcal{Q}_1 := Core(\mathbb{Z}; +) = (\mathbb{Z}; \circ)$ with generators 0 and 1 [11, Th. 12, p. 118], [16, p. 89–90].

Now we may paraphrase Theorem 10.5. from [9, p. 48], as follows (for the variety $\underline{RSIE}$ [21, Th. 3.1, p. 265]).

Example 4.2. On $\mathbb{R}^n$, $n \in \mathbb{N}$, let us introduce a binary operation $(x_1, \dots, x_n) \circ (y_1, \dots, y_n) := (2x_1 - y_1, \dots, 2x_n - y_n)$. Then $(\mathbb{R}^n; \circ)$ is a $\underline{SIE}$-groupoid, and $(\mathbb{Z}^n; \circ) = Core(\mathbb{Z}^n; +)$ forms its subgroupoid. In $(\mathbb{Z}^n; \circ)$, let us consider a subgroupoid $\mathcal{Q}_n = (Q_n; \circ)$ with the carrier set Q_n consisting of all n-tuples $(k_1, \dots, k_n)$ from $\mathbb{Z}^n$ such that at most one k_i is odd. Then the free groupoid on $n+1$ free generators $\mathcal{F}(n+1) = \mathcal{F}_{\underline{SIE}}(\{x_0, x_1, \dots, x_n\})$ is isomorphic to $\mathcal{Q}_n = (Q_n; \circ)$ with free generators $(0, \dots 0)$, $(1, 0, \dots, 0), \dots,$ and $(0, \dots, 0, 1)$.

Proposition 4.1. *The variety $\underline{SIE}$ is generated by cores of commutative groups.*

Proof. The statement can be proved directly from the results of D. Joyce. Since the free groupoid on n elements $\mathcal{F}(n)$ is (up to isomorphism) a subgroupoid $\mathcal{Q}_{n-1}$ of $Core(\mathbb{Z}^{n-1}; +) \in \underline{CAG} \subset \underline{SIE}$, and $\underline{SIE} = HSP(\{\mathcal{F}_{\underline{SIE}}(n) \,|\, n \in \mathbb{N}\})$ (e.g. [7, Satz 6.3.16, p. 93])[3] the assertion follows. □

Of course, commutative groups are not the only quasigroups with medial cores. In [21, Ex. 1.6, p. 4] the following is suggested.

Proposition 4.2. *A core $Core(\mathcal{G})$ of a group $\mathcal{G} = (G, \cdot, ^{-1}, e)$ (non-commutative in general) is medial if and only if $\mathcal{G}$ is nilpotent of class at most two*[4] .

Proof. Mediality (E) for group cores takes the form

$$xy^{-1}xz^{-1}uz^{-1}xy^{-1}x = xz^{-1}xy^{-1}uy^{-1}xz^{-1}x$$

which is equivalent (due to left and right cancellation in $\underline{G}$) with the condition

$$xyzuzyx = zyxuxyz \qquad \text{for all} \qquad x, y, z, u \in G. \tag{4.1}$$

Let $Core(\mathcal{G})$ of a group $\mathcal{G}$ be medial. Let us set $z = e$ in (4.1), and use $xy = yx \cdot [x, y]$ where $[x, y] = x^{-1}y^{-1}xy$ denotes the commutator. Then $yx[x, y]uyx = yxuyx[x, y]$ holds for $x, y, u \in G$. Further by cancellation, $[x, y]uyx = uyx[x, y]$. The last condition is equivalent with the condition $[x, y]g = g[x, y]$ for all $g \in G$ (if $g \in G$ is given the corresponding u takes the form $u = gx^{-1}y^{-1}$), which is satisfied iff $[x, y] \in Z(G)$. Hence nilpotency of class at most two is a necessary condition for a group to have medial core.

Vice versa, let $\mathcal{G}$ be a nilpotent group of class at most two, that is, all commutators $[a, b]$ for $a, b \in G$ are in the center $Z(\mathcal{G})$ of $\mathcal{G}$. Using commutators we can write $xyz = xzy[y, z] = zyx[x, zy][y, z]$ and similarly for zyx. Now (4.1) holds if and only if

$$zyx[x, y][xy, z]uxyz[z, xy][y, x] = zyxuxyz \tag{4.2}$$

[3] Here P denotes forming of products, S means taking of subalgebras, and H means homomorphic images.

[4] In a group $\mathcal{G}$, its centre $Z(\mathcal{G})$ is a normal subgroup, we have the canonical projection $p : \mathcal{G} \to \mathcal{G}/Z(\mathcal{G})$, and the inverse image $C_2(\mathcal{G}) = p^{-1}(Z(\mathcal{G}/Z(\mathcal{G})))$ of $Z(\mathcal{G}/Z(\mathcal{G}))$ in $\mathcal{G}$. A group is called *nilpotent of class at most two* if $C_2(\mathcal{G}) = \mathcal{G}$. A necessary and sufficient condition is that for any pair of elements of the group, the commutator belongs to the center $Z(\mathcal{G})$.

is satisfied for all $x, y, z, u \in G$. But we easily check that $[x, y][xy, z][z, xy][y, x] = e$ is valid in G. So if all commutators are in the center of the group then the condition (4.2) is satisfied, and consequently $\mathcal{G}$ has a medial core. □

4.2 Remarks on normal forms for terms in $\underline{SIE}$. Every term of the free algebra $\mathcal{F}_{\underline{SIE}}(X)$, $X \neq \emptyset$ is equivalent (in the variety $\underline{SIE}$) to a term of the form

$$w = x_n x_{n-1} \dots x_2 x_1 \qquad x_{i+1} \neq x_i, \quad i = 1, \dots, n-1, \quad x_1, \dots, x_n \in X \tag{4.3}$$

where each variable on an odd position (from the left) is different from all variables on even positions, i.e. $\{x_n, x_{n-2}, \dots\} \cap \{x_{n-1}, x_{n-3}, \dots\} = \emptyset$. The prove is based on Lemma 3.1 and Lemma 3.2. Indeed, if two variables are equal, one of them on an odd position and the other on an even one, we can use a suitable transposition so that equal variables stand on neighbour positions, and then we can use either (S_l) or (I), respectively, to reduce the term.

An infinitely countable set Z generates a $\underline{SIE}$-subgroupoid $\mathcal{Z}'$ in the core of a free abelian group $Core(\mathcal{F}_{\underline{AG}}(Z))$, and it can be checked that the formula (3.4) holds in $Core(\mathcal{F}_{\underline{AG}}(Z))$ for $n \geq 2$. The last term from (3.4) can be reduced if and only if some variable on an odd position (from the left) is equal to some variable on an even position, e.g. $z_1 \circ z_3 \circ z_2 \circ z_1 = z_2 \circ z_3 \circ z_1$ since $z_1^2 z_3^{-2} z_2^2 z_1^{-1} = z_2^2 z_3^{-2} z_2^2 z_1^1$. Therefore different terms w, w' of the form (4.3) give different term functions $w^{\mathcal{Z}'}$, $w'^{\mathcal{Z}'}$ of the groupoid $\mathcal{Z}'$.

Normal forms for terms over X in $\underline{SIE}$ can be now constructed as follows. Choose a linear order on X, $(X, \leq)$. Let us rearrange the variables in the term $w = x_n x_{n-1} \dots x_2 x_1$ of the form (4.3) in such a way that the resulting term denoted by $Nf(w)$ satisfies $x_n \leq x_{n-2} \leq \dots$ and $x_{n-1} \leq x_{n-3} \leq \dots$ (naturally also $\{x_n, x_{n-2}, \dots\} \cap \{x_{n-1}, x_{n-3}, \dots\} = \emptyset$). Then $Nf(w)$ can be called a *normal form* of w with respect to $\underline{SIE}$.

Again, we can introduce a mapping $\mathcal{L}' : \mathcal{F}_{\underline{SIE}}(Z) \to \mathcal{Z}'$ similarly as above[5]. For any equivalence class $[w]$, $w \in T_{(2)}(Z)$, with $Nf(w) = z_1 z_2 \dots z_{n-1} z_n$ define $\mathcal{L}'([w]) := z_1 \circ z_2 \circ \dots \circ z_{n-1} \circ z_n$. It can be easily seen that $\mathcal{L}'$ is a surjective homomorphism. Different terms over Z in normal form (i.e. representatives of two distinct classes from the free algebra $\mathcal{F}_{\underline{SIE}}(Z)$) obviously yield different elements of the groupoid $\mathcal{Z}' \in \underline{AGC}$. Therefore $\mathcal{L}'$ is also injective, and the groupoids $\mathcal{F}_{\underline{SIE}}(Z)$, $\mathcal{Z}'$ are isomorphic, particularly, $\mathcal{Z}'$ is free infinitely generated in $\underline{SIE}$. Hence we obtain another proof of the fact that the varieties $\underline{CAG}$ and $\underline{SIE}$ coincide (Proposition 4.1).

Lemma 4.1. *In the variety $\underline{SIE}$ the following identities are satisfied:*

$$u(z(yx)) = y(z(ux)), \tag{4.5}$$

$$y_n x_n \dots y_1 x_1 = y_{\sigma(n)} x_n \dots y_{\sigma(1)} x_1, \quad \sigma \in S_n, \tag{4.6}$$

$$x_n y_{n-1} x_{n-1} \dots x_2 y_1 x_1 = x_{\sigma(n)} y_{n-1} x_{\sigma(n-1)} \dots x_{\sigma(2)} y_1 x_1 \tag{4.7}$$

[5] Note that the equivalence classes of terms are now different, coarser.

where $\sigma \in S_n$ is a permutation such that $\sigma(1) = 1$. Moreover, the identities (4.5) *and* (E) *are equivalent in the variety* $\underline{SID}$.

Proof. By (D_l), (E) and (S_l), $u(z(yx)) = (uz)((uy)(ux)) = (u(uy))(z(ux)) = y(z(ux))$, and (4.5) holds. Since every permutation can be composed from transpositions, (4.6) follows from (4.5). If we take (y_1x_1) instead of x_1, y_i instead of x_i for $i = 2, \dots, n-1$, and x_{i+1} instead of y_i for $i = 1, \dots, n-1$ we get $x_n y_{n-1} x_{n-1} \dots y_2 x_2 (y_1 x_1) = x_{\sigma(n)} y_{n-1} x_{\sigma(n-1)} \dots y_2 x_{\sigma(2)} (y_1 x_1)$, i.e. (4.7) holds. Finally, $(xy)(zu) = x[y(x(zu))]$ holds in $\underline{SID}$, and using (4.5) we can rewrite the last term as $x[z(x(yu))] = (xz)(yu)$. □

Hence $Mod(\{(S_l), (D_l), (I), (4.5)\}) = Mod(\{(S_l), (I), (E)\})$.

4.3 Mediality of Bol loop cores. Finally, let us express mediality of a core for a Bol loop.

Lemma 4.3. *A core $Core(\mathcal{B})$ of a Bol loop $\mathcal{B} = (B, \cdot, ^{-1}, e) \in \underline{B}$ is medial if and only if the following identity holds in $\mathcal{B}$:*

$$y(x(z(u(z(xy))))) = z(x(y(u(y(xz))))). \tag{4.8}$$

Proof. For Bol loop cores, mediality $(x \circ y) \circ (z \circ u) = (x \circ z) \circ (y \circ u)$ takes the form $(x(y^{-1}x)) \cdot ((z \circ u)^{-1} \cdot (x \circ y)) = (x(z^{-1}x)) \cdot ((y \circ u)^{-1} \cdot (x \circ z))$ or equivalently, using (B_l), $x(y^{-1}(x(z \circ u)^{-1} \cdot (x \circ y)))) = x(z^{-1}(x(y \circ u)^{-1} \cdot (x \circ z))))$ for x, y, z, u from B. Let us write y, z instead of y^{-1}, z^{-1}, and use left cancellation. Then our condition is equivalent with $y(x((z \circ u^{-1}) \cdot (x(yx)))) = z(x((y \circ u^{-1}) \cdot (x(zx))))$ for all $x, y, z, u \in B$. Using (B_l) again we can write the formula as $(y((x((z \circ u^{-1}) \cdot x)) \cdot y)) \cdot x = (z((x((y \circ u^{-1}) \cdot x)) \cdot z)) \cdot x$ or, using right cancellation, in a simplified form $y((x((z(uz)) \cdot x)) \cdot y) = z((x((y(uy)) \cdot x)) \cdot z)$. Now using left Bol identity (B_l) twice we obtain that mediality holds in a Bol loop core if and only if the condition $y(x(z(u(z(xy))))) = z(x(y(u(y(xz))))$ is satisfied for all $x, y, z, u \in B$. □

Open problem 1: Is it possible to formulate mediality condition for Bol (Moufang, or commutative Moufang, respectively) loop cores similarly as in Proposition 4.1?

Open problem 2: Describe an equational theory for the variety generated by cores of commutative Moufang loops. Is the variety generated by cores of $\underline{CML}$ a proper subvariety of $\underline{SID}$?

References

[1] Arworn Sr., Denecke K. *Hyperidentities and hypersubstitutions in the variety of symmetric, idempotent, entropic groupoids.* Dem. Math., 1999, **XXXII**, N 4, p. 677–686.

[2] Belousov V.D. *Foundations of the theory of quasigroups and loops.* Moscow, Nauka, 1967.

[3] Bruck R.H. *A Survey of Binary Systems.* Berlin, Springer, 1958.

[4] Burn R.P. *Finite Bol loops.* Math. Proc. Cambridge Philos. Soc., 1978, **84**, p. 377–385.

[5] Denecke K., Wismath Sh.L. *Universal Algebra and Applications in Theoretical Computer Science.* Chapman and Hall/CRC, Boca Raton-London-New York-Washington D.C., 2002.

[6] Grätzer G. *Universal Algebra.* Van Nostrand Co., Princeton–New Yersey, 1968.

[7] Ihringer Th. *Allgemeine Algebra.* Teubner, Stuttgart, 1988.

[8] Jeřábek E., Kepka T., Stanovský D. *Non-idempotent left symmetric left distributive groupoids.* Preprint.

[9] Joyce D. *Aclassifying invariant of knots, the knot quandle.* Jour. of Pure and Appl. Alg., 1982, **23**, p. 37–65.

[10] Kinyon M.K. *Global left loop structures o spheres.* Comment. Math. Univ. Carolinae, 2000, **41**, N 2, p. 325–346.

[11] sc Lindner C.C., Mendelsohn N.S. *Constructions of n-cyclic quasigroups and applications.* Aequat. Math., 1976, **14**, p. 111–121.

[12] 2 Loos O. *Symmetric Spaces.* J. Benjamin, New York, 1969.

[13] Nagy P.T., Strambach K. *Loops, their cores and symmetric spaces.* Israel Jour. of Math., 1998, **105**, p. 285–322.

[14] Nagy P.T., Strambach K. *Loops in Group Theory and Lie Theory.* De Gruyter, Berlin–New York, 2002.

[15] Nobusawa N. *On symmetric structures of a finite set.* Osaka J. Math., 1974, **11**, p. 569–575.

[16] Nobusawa N. *Simple symmetric sets and simple groups.* Osaka J. Math., 1977, **14**, p. 411–415.

[17] Pflugfelder H.O. *Quasigroups and Loops, Introduction.* Heldermann Verlag, Berlin, 1990.

[18] Pierce R.S. *Symmetric Groupoids.* Osaka J. Math., 1978, **15**, p. 51–76.

[19] Pierce R.S. *Symmetric Groupoids II.* Osaka J. Math., 1979, **16**, p. 317–348.

[20] Romanowska A., Smith J.D.H. *Modal Theory, An Algebraic Approach to Order, Geometry, and Convexity.* Berlin, Heldermann Verlag, 1985.

[21] Roszkowska B. *The lattice of varieties of symmetric idempotent entropic groupoids.* Demonstratio Math., 1987, **XX**, N 1-2, p. 259–275.

[22] Roszkowska B. *On some varieties of symmetric idempotent entropic groupoids.* Universal and Applied Algebra (eds. K. Hałkowska, B. Stawski), World Scientific, 1989, p. 254–274.

[23] Roszkowska-Lech B. *A representation of symmetric idempotent and entropic groupoids.* Demonstratio Math., 1999, **XXXII**, N 2, p. 247–262.

[24] Roszkowska-Lech B. *Subdirectly irreducible symmetric idempotent and entropic groupoids.* Demonstratio Math., 1999, **XXXII**, N 3, p. 469–484.

[25] Smith J.D.H. *Modes and modals.* Discussiones Math., Algebra and Stochastic Methods, 1999, **19**, p. 9–40.

[26] Stanovský D. *Left distributive groupoids.* Diploma Thesis, Charles Univ. Prague.

[27] Stanovský D. *Left symmetric left distributive operations on a group.* Preprint.

[28] Takasaki M. *Abstractions of symmetric functions.* Tôhoku Math. J., 1943, **49**, p. 147–207.

[29] Vanžurová A. *Normal form hypersubstitutions with respect to the variety of left symmetric left distributive idempotent groupoids.* Contributions in General Algebra, 2004, **14**, p. 173–187.

Faculty Sciences
Department Algebra and Geometry
Palacký University
Tomkova 40, 779 00 Olomouc
Czech Republic
E-mail: *vanzurov@inf.upol.cz*

Received August 11, 2005