Czechoslovak Mathematical Journal, 40 (115) 1990, Praha

LOOPS WHOSE TRANSLATIONS GENERATE THE ALTERNATING GROUP

ALEŠ DRÁPAL and TOMÁŠ KEPKA, Praha

(Received March 21, 1988)

In this paper, the concepts of orthogonal mappings and prolongations are used to obtain loops whose multiplication groups contain the alternating group. The results partially overlap those of [4], but here a different method is employed.

1. INTRODUCTION

For a non-empty (finite) set M, let $\mathcal{S}(M)$ denote the symmetric group and $\mathcal{A}(M)$ the alternating group on M. If G is a subgroup of $\mathcal{S}(M)$, then $\mathcal{N}(G)$ will be the normalizer of G in $\mathcal{S}(M)$.

Let Q be a quasigroup. We put $\mathcal{L}(a, Q)(x) = ax$ and $\mathcal{R}(a, Q)(x) = xa$ for all $a, x \in Q$. The transformations $\mathcal{L}(a, Q)$ and $\mathcal{R}(a, Q)$ are permutations of Q (the left translation and the right translation by a) and we put $\mathcal{M}_l(Q) = \langle \mathcal{L}(a, Q);\ a \in Q \rangle$, $\mathcal{M}_r(Q) = \langle \mathcal{R}(a, Q);\ a \in Q \rangle$ and $\mathcal{M}(Q) = \langle \mathcal{M}_1(Q), \mathcal{M}_r(Q) \rangle$.

A finite quasigroup Q is said to be of type

(1), if every translation of Q is even;

(2), if every left translation is odd and every right translation is even;

(3), if every left translation is even and every right translation is odd;

(4), if every translation of Q is odd.

A finite loop Q is said to be of type

(L1), if it is of type (1);

(L2), if $\mathcal{L}(a, Q)$ is odd and $\mathcal{R}(a, Q)$ is even for every $1 \neq a \in Q$;

(L3), if $\mathcal{L}(a, Q)$ is even and $\mathcal{R}(a, Q)$ is odd for every $1 \neq a \in Q$;

(L4), if both $\mathcal{L}(a, Q)$ and $\mathcal{R}(a, Q)$ are odd for every $1 \neq a \in Q$.

In the sequel, we shall need the following well known assertions:

1.1. Lemma. *Let Q be a primitive permutation group on a non-empty finite set M Then $\mathcal{A}(M) \subseteq G$ provided G contains either a transposition or a 3-cycle.*

1.2. Lemma. *Let A be a finite group and let G be a finite simple group from the* *variety of groups generated by A. Then there exist subgroups B and C of A such that C is a normal subgroup of B and G is isomorphic to B/C.*

Proof. There exist $n \geqq 1$ and subgroups $N \subseteq H \subseteq K = A^n$ such that N is normal in H and G is isomorphic to H/N. Assume $n \geqq 2$ and put $K_i = \{(x_1, \dots, x_n) \in K;\ x_i = 1\}$, $H_i = H \cap K_i$ for every $i = 1, \dots, n$. If $H_i \subseteq N$ for some i, then we have $G = (H/H_i)/(N/H_i)$ and $H/H_i \cong HK_i/K_i \subseteq K/K_i \cong A$. On the other hand, if $H_i \nsubseteq N$ for some i, then $H = H_iN$, $G \cong H/N = H_iN/N \cong H_i/N \cap H_i$ and $H_i \subseteq \subseteq K_i \cong A^{n-1}$. In this case, we can proceed by induction.

2. PROLONGATIONS OF IDEMPOTENT QUASIGROUPS

Let Q be a finite idempotent quasigroup and let $e \notin Q$. We denote by $P = P(*) = \mathscr{P}(Q, e)$ the corresponding prolongation of Q. That is, $P = Q \cup \{e\}$ and the operation $*$ is defined on P as follows: $x * y = xy$, $x * x = e = e * e$ and $x * e = x = e * x$ for all $x, y \in Q$, $x \neq y$. Obviously, P is a 2-elementary (and hence monoassociative) loop, e is its neutral element and P is commutative iff Q is so.

The concept of prolongation is well known (see [1] for further references) and we have the following two evident lemmas:

2.1. Lemma. $\operatorname{sgn}(\mathscr{L}(x, Q)) = -\operatorname{sgn}(\mathscr{L}(x, P))$ *and* $\operatorname{sgn}(\mathscr{R}(x, Q)) = -\operatorname{sgn}(\mathscr{R}(x, P))$ *for each* $x \in Q$.

2.2. Lemma. *The following conditions are equivalent for $f \in \mathscr{S}(Q)$:*
(i) *$fMf^{-1} = M$ for $M = \{\mathscr{R}(x, Q);\ x \in Q\}$;*
(ii) *$fNf^{-1} = N$ for $N = \{\mathscr{L}(x, Q);\ x \in Q\}$;*
(iii) *f is an automorphism of Q;*
(iv) *$\bar{f}$ is an automorphism of P (here, $\bar{f}(e) = e$ and $\bar{f} \mid Q = f$);*
(v) *$\bar{f}K\bar{f}^{-1} = K$ for $K = \{\mathscr{R}(x, P);\ x \in P\}$;*
(vi) *$\bar{f}L\bar{f}^{-1} = L$ for $L = \{\mathscr{L}(x, P);\ x \in P\}$.*
In this case, $\bar{f} \in \mathscr{N}(\mathscr{M}_r(P)), \mathscr{N}(\mathscr{M}_1(P)), \mathscr{N}(\mathscr{M}(P))$.

2.3. Lemma. *Suppose that the automorphism group* $\operatorname{Aut}(Q)$ *of Q is transitive on Q. Then the permutation groups $\mathscr{N}(\mathscr{M}_r(P))$ and $\mathscr{N}(\mathscr{M}_l(P))$ are 2-transitive.*

Proof. By 2.2, $\overline{\operatorname{Aut}(Q)} \subseteq \mathscr{N}(\mathscr{M}_r(P))$. Hence the stabiliser of e in $\mathscr{N}(\mathscr{M}_r(P))$ is transitive on Q. But $\mathscr{M}_r(P)$ is transitive on P, and therefore $\mathscr{N}(\mathscr{M}_r(P))$ is 2-transitive. Similarly for $\mathscr{N}(\mathscr{M}_1(P))$.

2.4. Lemma. *Suppose that* $\mathscr{R}(a, Q) \in \operatorname{Aut}(Q)$ *for at least one $a \in Q$. Then $\mathscr{N}(\mathscr{M}_r(P))$ contains a transposition.*

Proof. Put $h = \overline{\mathscr{R}(a, Q)}^{-1}.\ \mathscr{R}(a, P)$. Then, by 2.2, $h \in \mathscr{N}(\mathscr{M}_r(P))$. However, h is a transposition.

2.5. Corollary. *Let Q be a finite idempotent quasigroup of order at least* 4.

Suppose that $\mathrm{Aut}(Q)$ *is transitive on* Q *and that* $\mathscr{R}(a, Q) \in \mathrm{Aut}(Q)$ *for at least one* $a \in Q$ *(e.g., if* Q *is right distributive). Then* $\mathscr{A}(P) \subseteq \mathscr{M}_r(P)$, $P = \mathscr{P}(Q, e)$, $e \notin Q$.

2.6. Remark. Let $P = P(+)$ be a finite 2-elementary abelian group of order at least 4. Put $Q = P - \{0\}$ and $xy = x + y$, $xx = x$ for all $x, y \in Q$, $x \neq y$. Then Q is a symmetric idempotent quasigroup, $\mathrm{Aut}(Q)$ is tansitive on Q and $P = \mathscr{P}(Q, 0)$. However, $\mathscr{A}(P) \nsubseteq \mathscr{M}(P)$.

3. PROLONGATIONS AND ORTHOGONAL MAPPINGS

3.1. Proposition. *The following conditions are equivalent for a quasigroup* Q:

(i) Q *is right distributive and* Q *is isotopic to a group.*

(ii) *There exist a group* $Q(\circ)$ *and* $f \in \mathrm{Aut}(Q(\circ))$ *such that* $g: x \to f(x^{-1}) \circ x \in \mathscr{S}(Q)$ *and* $xy = f(x) \circ g(y) = f(x \circ y^{-1}) \circ y$ *for all* $x, y \in Q$.

Proof. (i) implies (ii). Let $a \in Q$ and $x \circ y = f^{-1}(x)\, g^{-1}(y)$, $f = \mathscr{R}(a, Q)$, $g = \mathscr{L}(a, Q)$. Then $xy = f(x) \circ g(y)$, $x = f(x) \circ g(x)$, $g(x) = f(x)^{-1} \circ x$ and $f(x \circ y) = f(f^{-1}(x)\, g^{-1}(y)) = xfg^{-1}(y) = xg^{-1}f(y) = f^{-1}f(x)\, g^{-1}f(y) = f(x) \circ f(y)$; we have $f\, g(x) = ax \,.\, a = a \,.\, xa = g\, f(x)$.

(ii) implies (i). We can write $xy \,.\, z = f(f(x) \circ g(y)) \circ g(z) = f^2(x) \circ f\, g(y) \circ g(z) = f^2(x) \circ f\, g(z) \circ f(g(z)^{-1}) \circ f^2(y^{-1}) \circ f(y) \circ g(z) = f^2(x) \circ f\, g(z) \circ g(f(y) \circ (z)) = xz \,.\, yz$.

3.2. Corollary. *The following conditions are equivalent for a quasigroup* Q:

(i) Q *is distributive and isotopic to a group.*

(ii) Q *is idempotent and medial.*

(iii) *There exist an abelian group* $Q(+)$ *and* $f \in \mathrm{Aut}(Q(+))$ *such that* $g: x \to x - f(x) \in \mathscr{S}(Q)$ *and* $xy = f(x) + g(y)$ *for all* $x, y \in Q$.

Quasigroups satisfying the equivalent conditions of 3.1 have been called left orthomorphic in [2]. Thus, orthomorphic quasigroups (i.e. both left and right orthomorphic) are nothing else than idempotent medial quasigroups.

Let G be a group and $f, g \in \mathscr{S}(G)$. Then (f, g) is said to be a *pair of left (right) orthogonal permutations of* G if $f(1) = 1$ and $g(x) = f(x^{-1})\, x$ $(g(x) = xf(x^{-1}))$ for every $x \in G$. In this case, we have also $g(1) = 1$ and $f(x) = g(x^{-1})\, x$ $(f(x) = xg(x^{-1}))$, so that (g, f) is again a pair of left (right) orthogonal permutations of G. Clearly, the pair (f, g) is a pair of left orthogonal permutations of G iff (f, g) is a pair of right orthogonal permutations of the opposite group G^{op}.

Let (f, g) be a pair of permutations of G. Put $f'(x) = f(x^{-1})^{-1}$ and $g'(x) = g(x^{-1})^{-1}$. Then $f'' = f$, $g'' = g$ and (f, g) is a pair of left orthogonal permutations of G iff (f', g') is a pair of right orthogonal permutations of G. Hence (f, g) is a pair of left orthogonal permutations of G iff (f', g') is a pair of left orthogonal permutations of G^{op} (further details on orthogonal permutations can be found in [1]).

Now, let (f, g) be a pair of left (right) orthogonal permutations of a group G.

Put $x \circ y = f(xy^{-1})\, y = g(yx^{-1})\, x$ $(x \circ y = xf(x^{-1}y) = yg(y^{-1}x))$ for all $x, y \in G$. Then $G(\circ) = \mathcal{O}_1(G, f, g)$ $(G(\circ) = \mathcal{O}_r(G, f, g))$ is an idempotent quasigroup and such a quasigroup will be called orthostrophic.

If (f, g) is a pair of left orthogonal permutations of G, then $G(\circ)^{\mathrm{op}} = \mathcal{O}_r(G^{\mathrm{op}}, f, g) = \mathcal{O}_l(G, g, f)$, $G(\circ) = \mathcal{O}_l(G, f, g)$. Further, $G(\circ) = \mathcal{O}_r(G^{\mathrm{op}}, g, f)$ and the mapping $x \to x^{-1}$ is an isomorphism of $G(\circ)$ onto $\mathcal{O}_r(G, g', f')$.

Clearly, every left (right) orthomorphic quasigroup is orthostrophic.

3.3. Lemma. *Let (f, g) be a pair of left orthogonal permutations of a finite group G. Put $G(\circ) = \mathcal{O}_1(G, f, g)$. Then* $\operatorname{sgn}(\mathscr{R}(a, G(\circ))) = \operatorname{sgn}(f)$ *and* $\operatorname{sgn}(\mathscr{L}(a, G(\circ))) = \operatorname{sgn}(g)$ *for every $a \in G$.*

Proof. Easy.

3.4. Lemma. *Let Q be an orthostrophic quasigroup, $e \notin Q$ and $P = \mathscr{P}(Q, e)$. Then the permutation groups $\mathscr{N}(\mathscr{M}_r(P))$ and $\mathscr{N}(\mathscr{M}_l(P))$ are 2-transitive on P.*

Proof. There are a group $Q(\circ)$ and a pair (f, g) of left orthogonal permutations of $Q(\circ)$ such that $xy = f(x \circ y^{-1}) \circ y$ for all $x, y \in Q$. Now, it is easy to check that $\mathscr{M}_r(Q(\circ)) \subseteq \operatorname{Aut}(Q)$, and the result follows from 2.3.

4. PROLONGATIONS AND THE SINGULAR DIRECT PRODUCT

Let R be a non-trivial finite idempotent quasigroup and Q a finite non-empty set. Further, suppose that for every ordered pair $x = (a, b) \in R^2$ a quasigroup operation $q_x\colon Q^2 \to Q$ on Q is given such that q_x is idempotent if $a = b$. Put $T = R \times Q$ and define a multiplication on T by $(a, x)(b, y) = (ab, q_{(a,b)}(x, y))$. In this way, we obtain an idempotent quasigroup T. Put also $n = \operatorname{card}(R)$ and $m = \operatorname{card}(Q)$. Then $nm = \operatorname{card}(T)$.

4.1. Lemma. $\operatorname{sgn}(\mathscr{R}((a, x), T)) = (\operatorname{sgn}(\mathscr{R}(a, r)))^m \prod_{b \in R} \operatorname{sgn}(\mathscr{R}(x, Q(q_{(b,a)}))$ *and* $\operatorname{sgn}(\mathscr{L}((a, x), T)) = \operatorname{sgn}(\mathscr{L}(a, R)))^m \prod_{b \in R} \operatorname{sgn}(\mathscr{L}(x, Q(q_{(a,b)})))$ *for all $a \in R$ and $x \in Q$.*

Proof. Easy.

Now, let $e \notin R \cup Q \cup T$. In what follows, we shall work with the prolongations $S = S(*) = \mathscr{P}(T, e)$ and $P_a = P_a(*) = (Q(q_{(a,a)}), e)$, $a \in R$. For every $a \in R$, the set $Q_a = \{(a, x);\ x \in Q\} \cup \{e\}$ is a subloop of S. Put also $H(a) = \langle \mathscr{L}((a, x), S), \mathscr{R}((a, x), S);\ x \in Q \rangle \subseteq \mathscr{M}(S)$ and denote by P the set $Q \cup \{e\}$.

4.2. Lemma. (i) $\mathscr{M}(S) = \langle \bigcup H(a);\ a \in R \rangle$.

(ii) $H(a)(Q_a) = Q_a = H(a)(e)$.

Proof. (i) This is evident.

(ii) We have $(a, x) * (a, y) = (a, q_{(a,a)}(x, y))$, $(a, x) * e = (a, x) = e * (a, x)$ and $e * e = e$ for all $x, y \in Q$, $x \neq y$.

For $a \in R$, put $S_a = S - Q_a$ and define a mapping $i_a\colon P \to S$ by $i_a(x) = (a, x)$ for each $x \in Q$ and $i_a(e) = e$. Clearly, i_a is an isomorphism of the loop P_a onto the loop Q_a. Now, we define mappings $r_a(t_a, s_a)$ of $H(a)$ into $\mathscr{S}(P)\,(\mathscr{S}(S_a), \mathscr{S}(P) \times \mathscr{S}(S_a))$ by $r_a(f) = i_a^{-1}(f \mid Q_a)\, i_a\, (t_a(f) = f \mid S_a,\ s_a(f) = (r_a(f), t_a(f))$ for every $f \in H(a)$ (see 4.2 (ii)).

Obviously, s_a is injective.

4.3. Lemma. *r_a is a homomorphism of $H(a)$ onto $\mathscr{M}(P_a)$.*

Proof. Clearly, $r_a(\mathscr{L}((a, x), S)) = \mathscr{L}(x, P_a)$ and $r_a(\mathscr{R}((a, x), S)) = \mathscr{R}(x, P_a)$.

For $a \in R$, let $K(a) \subseteq \mathscr{S}(S_a)$ be the set of all $f \in \mathscr{S}(S_a)$ such that $p(\alpha) = p(\beta)$ implies $p\,f(\alpha) = p\,f(\beta)$ for all $\alpha, \beta \in S_a$ (here, $p\colon S_a \to R$ denotes the restriction of the natural projection). Clearly, $K(a)$ is a subgroup of $\mathscr{S}(S_a)$. Further, let $L(a)$ be the set of all $f \in K(a)$ such that $p(\alpha) = p\,f(\alpha)$ for every $\alpha \in S_a$. Again, $L(a)$ is a subgroup of $K(a)$.

4.4. Lemma. *$t_a(H(a)) \subseteq K(a)$.*

Proof. Evidently, $t_a(\mathscr{L}(a, x)) \in K(a)$ and $t_a(\mathscr{R}(a, x)) \in K(a)$.

Put $G_1(a) = s_a(H(a))$, $G_2(a) = \{(f, g) \in G_1(a);\ g \in L(a)\}$ and $G_3(a) = \{(f, g) \in G_2(a);\ g = 1_{S_a}\}$. Further, put $H_2(a) = r_a s_a^{-1}(G_2(a))$ and $H_3(a) = r_a s_a^{-1}(G_3(a))$. Obviously, $H_3(a)$ is isomorphic to $G_3(a)$.

4.5. Lemma. *$H_2(a)$ is transitive on P.*

Proof. Let $x, y \in Q$, $x \neq y$, and $h = \mathscr{L}(a, x), S)$, $k = \mathscr{L}((a, y), S)$, $l = hk^{-1}$. Then $s_a(l) \in G_2(a)$ and $r_a(l)\,(e) = q_{(a,a)}^{(x,y)}$.

Let $G(a) = t_a s_a^{-1}(G_2(a))$.

4.6. Lemma. *If $H_3(a)$ is trivial, then $H_2(a)$ is isomorphic to $G(a)/N$ for a normal subgroup N of $G(a)$.*

Proof. Obviously, $G(a)$ is the set of $g \in L(a)$ such that $(f, g) \in G_2(a)$ for some $f \in \mathscr{S}(P)$. If $H_3(a)$ is trivial, then $(f, g) \to g$ is an isomorphism of $G_2(a)$ onto $G(a)$.

In the rest of this section, let $m \geqq 4$, $A = \mathscr{A}(P)$ and $B = \mathscr{A}(S)$.

4.7. Lemma. *If $A \subseteq \mathscr{M}(P_a)$, then $A \subseteq H_3(a)$.*

Proof. Since $G_3(a) \subseteq G_2(a) \subseteq G_1(a)$, we have $H_3(a) \subseteq H_2(a) \subseteq \mathscr{M}(P_a) = r_a(H(a)) \supseteq A$. But P contains at least five elements and $H_2(a)$ is non-trivial. Consequently, $A \subseteq H_2(a)$. Similarly, either $A \subseteq H_3(a)$ or $H_3(a) = 1$. Now, assume that $H_3(a) = 1$. By 4.6, A belongs to the variety generated by $G(a)$. However, $G(a) \subseteq L(a)$ and $L(a)$ is isomorphic to the direct product of $n - 1$ copies of $\mathscr{S}(Q)$. In particular, A belongs to the variety generated by $\mathscr{S}(Q)$, a contradiction with 1.2.

4.8. Proposition. *Suppose that $n \geqq 2$, $m \geqq 4$ and that $A \subseteq \mathscr{M}(P_a)$ ($A \subseteq \mathscr{M}_l(P_a)$, $A \subseteq \mathscr{M}_r(P_a)$) for every $a \in R$. Then $B \subseteq \mathscr{M}(S)$ ($B \subseteq \mathscr{M}_1(S)$, $B \subseteq \mathscr{M}_r(S)$).*

Proof. By 4.7, $H(a)$ contains every even permutation $f \in \mathscr{S}(S)$ such that $f \mid S_a = 1_{S_a}$. However, $S = \bigcup_{a \in R} Q_a$ and $Q_a \cap Q_b = \{e\}$ for $a \neq b$. The result now follows from 1.1.

5.1. Proposition. (i) *For every odd* $n \geqq 7$, $n \neq 15$, *there exist orthomorphic quasigroups of order* n *and types* (1), (2), (3), (4).

(ii) *For every* $n \geqq 4$ *divisible by* 4 *there exists an orthomorphic quasigroup of order* n *and type* (1).

(iii) *There exists orthomorphic quasigroups of orders* 5,15 *and types* (2), (3).

(iv) *There exist orthomorphic quasigroups of orders* 3,5 *and type* (4).

(v) *There exists an orthomorphic quasigroup of order* 15 *and type* (1).

Proof. See [2, Corollary 6.6].

5.2. Proposition. (i) *There exists an orthostrophic quasigroup of order* 15 *and type* (4).

(ii) *For every* $n \geqq 8$ *divisible by* 8 *there exists an orthostrophic quasigroup of order* n *and type* (4).

Proof. See [3, Propositions 7.2, 10.2].

5.3. Proposition. (i) *For every* $n \geqq 8$ *divisible by* 4 *there exists an idempotent quasigroup of order* n *and type* (4).

(ii) *Every idempotent quasigroup of order* 3 *is of type* (4).

(iii) *Every idempotent quasigroup of order* 4 *is of type* (1).

(iv) *There is no idempotent quasigroup of order* 5 *and type* (1).

(v) *There is no idempotent quasigroup of order* 6 *and types* (2), (3) *or* (4).

(vi) *There exists an idempotent quasigroup of order* 6 *and type* (1).

Proof. See [3].

5.4. Lemma. (i) *For every* $n \geqq 3$ *there exists a loop of order* n *and type* (1).

(ii) *For every* $n \geqq 3$ *there exist quasigroups of order* n *and types* (1), (2), (3), (4).

Proof. (i) If $n = 2^k m$ for $k \neq 1$, then we can take the abelian group $Z_m \times Z_2^k$. If $n = 2m$, $m \geqq 3$ odd, we may use the prolongation of an idempotent quasigroup of order $n - 1$ and type (4) (see 5.1 (i), (iv)).

(ii) Let Q be a loop of order n and type (1). For $f, g \in \mathscr{S}(Q)$, define $x * y = f(x)\, g(y)$ for all $x, y \in Q$. Then $\operatorname{sgn}(\mathscr{L}(x, Q(*)) = \operatorname{sgn}(g)$ and $\operatorname{sgn}(\mathscr{R}(x, Q(*)) = \operatorname{sgn}(f)$.

5.5. Proposition. *Let* $m \geqq 4$ *and* $1 \leqq i \leqq 4$ *be such that there exists an idempotent quasigroup* Q *of order* m *and type* (i) *and with* $\mathscr{A}(P) \subseteq \mathscr{M}_l(P) \cap \mathscr{M}_r(P)$, $P = \mathscr{P}(Q, e)$. *Then, for all* $n \geqq 3$ *and* $1 \leqq j \leqq 4$, *there exists an idempotent quasigroup* T *of order* nm, *type* (j) *and such that* $\mathscr{A}(S) \subseteq \mathscr{M}_l(S) \cap \mathscr{M}_r(S)$, $S = \mathscr{P}(T, e)$.

Proof. Let R be an idempotent quasigroup of order n and let $Q(q_{(a,a)}) = Q$ for every $a \in R$. Now, the result follows by an easy combination of 4.8, 4.1 and 5.4 (ii).

5.6. Theorem. *Let* $n \geqq 6$ *be such that* $n \neq 2p + 1$ *for every prime* $p \geqq 3$. *Then* *there exist loops* L_1, L_2, L_3 *and* L_4 *of order n and types* (L1), (L2), (L3) *and* (L4), *respectively, such that*

(i) $\mathcal{M}_l(L_1) = \mathcal{M}_r(L_1) = \mathcal{M}(L_1) = \mathcal{A}(L_1)$;

(ii) $\mathcal{M}_l(L_2) = \mathcal{M}(L_2) = \mathcal{S}(L_2)$, $\mathcal{M}_r(L_2) = \mathcal{A}(L_2)$;

(iii) $\mathcal{M}_l(L_3) = \mathcal{A}(L_3)$, $\mathcal{M}_r(L_3) = \mathcal{M}(L_3) = \mathcal{S}(L_3)$;

(iv) $\mathcal{M}_l(L_4) = \mathcal{M}_r(L_4) = \mathcal{M}(L_4) = \mathcal{S}(L_4)$.

Proof. It is divided into several parts.

(a) $n = 6$. The existence of L_1, L_2 and L_3 follows from 5.1 (iii), (iv) and 2.5. For L_4, we can take the following loop:

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

(b) $n \geqq 8$ is even, $n \neq 16$. In this case, the result follows from 5.1 (i) and 2.5.

(c) $n = 9$. The existence of L_4 follows from 5.1 (ii) and 2.5. For L_3, we can take the prolongation of the following idempotent quasigroup:

	1	2	3	4	5	6	7	8
1	1	3	2	5	4	7	8	6
2	3	2	1	6	8	4	5	7
3	2	1	3	7	6	8	4	5
4	5	6	8	4	7	1	3	2
5	6	8	7	3	5	2	1	4
6	7	5	4	8	3	6	2	1
7	8	4	6	1	2	5	7	3
8	4	7	5	2	1	3	6	8

Now, it suffices to put $L_2 = L_3^{\mathrm{op}}$ and to consider the prolongation of the following idempotent quasigroup (for L_1):

	1	2	3	4	5	6	7	8
1	1	3	2	5	6	7	8	4
2	3	2	1	6	4	8	5	7
3	2	4	3	7	8	1	6	5
4	5	8	6	4	7	2	1	3
5	6	7	8	3	5	4	2	1
6	7	1	5	8	3	6	4	2
7	8	5	4	1	2	3	7	6
8	4	6	7	2	1	5	3	8

(d) $n = 19$. Consider the following idempotent quasigroup Q:

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

Then Q is of type (1) and $\mathcal{M}_l(P) = \mathcal{M}_r(P) = \mathcal{S}(P)$, $P = \mathcal{P}(Q, e)$. The result now follows from 5.5.

(e) $n = 16$. The result follows from 5.1 (iii) and 5.5.

(f) $n \geqq 13$ is odd, $n \neq 19$. Then $n = mk$, where $k \geqq 3$ and either $m \geqq 5$ is a prime or $m = 4$. Now, the result follows from 5.1 and 5.5.

5.7. Remark. (i) There exists no idempotent quasigroup of order 5 and type (1). Consequently, the existence of L_4 for $n = 6$ cannot be proved by using the prolongation.

(ii) Every at most four-element loop is an abelian group, and hence we have the following obvious existence-table:

	1	2	3	4
L_1	+	−	+	−
L_2	+	−	−	−
L_3	+	−	−	−
L_4	+	+	−	+

(iii) The complete list of five-element non-associative loops (see e.g. [1]) shows that every such loop possesses at least one odd left translation as well as at least one odd right translation. Therefore, the loops L_2 and L_3 do not exist for $n = 5$. On the other hand, by 5.1 (ii) and 2.5, L_4 exists.

(iv) Let $n = 2p + 1$, $p \geqq 3$ a prime. For these numbers, the existence of L_1 is proved in [4]. Perhaps, using similar methods, the other cases could be solved, too.

5.8. Remark. Let (f, g) be a pair of left orthogonal permutations of a group G and let, for every $a \in G$, (h_a, k_a) be a pair of left orthogonal permutations of a group H. Define

$$h(a, x) = (f(a), h_a(x)),$$
$$k(a, x) = (g(a), k_{a^{-1}}(x)) \quad \text{for all} \quad a \in G, \quad x \in H.$$

Then (h, k) is a pair of left orthogonal permutations of the product $G \times H$. This constructions could be used to find further orthostrophic quasigroups and their prolongations with prescribed parity of translations.

5.9. Remark. *Let $n \geqq 7$, $n \neq 2p$ for every prime p. Then there exist idempotent quasigroups of order n and types* (1), (2), (3), (4). *The situation for $n = 2p$ is not clear. Using* 5.6, *we can give a somewhat simplified proof of a result from* [5]:

5.10. Proposition. *Let $n \geqq 3$. Then there exist quasigroups Q_1, Q_2, Q_3 and Q_4 of order n and types* (1), (2), (3) *and* (4), *respectively, and such that $\mathscr{A}(Q_i) \subseteq \subseteq \mathscr{M}_l(Q_i) \cap \mathscr{M}_r(Q_i)$ for every $1 \leqq i \leqq 4$.*

Proof. It is divided into several parts.

(a) $n \geqq 6$ is even. By 5.6, there exists a loop Q of order n, type (1) and such that $\mathscr{M}_l(Q) = \mathscr{M}_r(Q) = \mathscr{A}(Q)$. Hence, we can put $Q_1 = Q$. Further, let $f \in \mathscr{S}(Q)$ be an odd permutation. Now, it is enough to put $Q_2 = Q(*)$, $Q_3 = Q(\circ)$ and $Q_4 = Q(\Delta)$, where $x * y = x f(y)$, $x \circ y = f(x)\, y$ and $x \,\Delta\, y = f(x) f(y)$ for all $x, y \in Q$.

(b) $n \geqq 3$ is odd. Put $Q = Z_n(+)$ (the group of integers modulo n) and choose $f, g \in \mathscr{S}(Q)$ such that $\mathscr{A}(Q) = \langle h, f \rangle$ and $\mathscr{S}(Q) = \langle h, g \rangle$, $h = (0\,1\,2 \ldots n-1)$. Now, it is enough to put $Q_1 = Q(*)$, $Q_2 = Q(\circ)$, $Q_3 = Q(\Delta)$ and $Q_4 = Q(\nabla)$, where $x * y = f(x) + f(y)$, $x \circ y = f(x) + g(y)$, $x \,\Delta\, y = g(x) + f(y)$ and $x \nabla y = = g(x) + g(y)$ for all $x, y \in Q$.

(c) $n = 4$. We can proceed similarly as in (b) (for $Q = Z_2 \times Z_2$).

References

[1] *J. Dénes, A. D. Keedwell:* Latin squares and their applications, Akadémiai Kiadó, Budapest 1974.

[2] *A. Drápal, T. Kepka:* Parity of orthogonal automorphisms, Comment. Math. Univ. Carolinae *28* (1987), 251–259.

[3] *A. Drápal, T. Kepka:* Parity of orthogonal permutations, Comment. Math. Univ. Carolinae *28* (1987), 427–432.

[4] *A. Drápal, T. Kepka:* Alternating groups and latin squares, Europ. J. Comb. *10* (1989), 175–180.

[5] *T. Ihringer:* On multiplicatin groups of quasigroups, Europ. J. Comb. *5* (1984), 137–141.

Authors' address: 186 00 Praha 8, Sokolovská 83, Czechoslovakia (Matematicko-fyzikální fakulta UK).