Quasigroups and Related Systems, **4** (1997), 1–7

IK-loops

Alexander S. Basarab

Abstract

A loop $\mathcal{Q}(\cdot)$ is called a K-loop, if the identities:

$$(x \cdot yIx) \cdot xz = x \cdot yz \,, \quad (y \cdot x) \cdot (I^{-1}xz \cdot x) = yz \cdot x$$
$$(\; Ix = x^{-1} \,, \quad I^{-1}x = {}^{-1}x \,, \quad I^{-1}x \cdot z = {}^{-1}x \cdot z \;)$$

hold. A K-loop is called an *IK*-loop if the substitution I is an automorphism of the loop. It is proved that: a K-loop generated by one element is solvable; in a *IK*-loop the center $\mathcal{Z}(\mathcal{Q})$ and the nucleus $\mathcal{N}$ coincide and every *IK*-loop is nilpotent. Examples of K-loops, generated by one element are given.

In [1] and [2] the following result is obtained: in a K-loop $\mathcal{Q}(\cdot)$ the nucleus $\mathcal{N}$ is a nontrivial ($\mathcal{N} \neq \{e\}$) normal subloop and the quotient loop $\mathcal{Q}/\mathcal{N}(\cdot)$ is an abelian group. If a K-loop $\mathcal{Q}(\cdot)$ is not a group, then the nucleus $\mathcal{N}$ of this loop has a nontrivial center $\mathcal{Z}(\mathcal{N})$.

Proposition 1. *If a loop $\mathcal{Q}(\cdot)$ has a nontrivial nucleus $\mathcal{N}$, which is a normal subloop of $\mathcal{Q}(\cdot)$ and (x,y,z) is the associator of elements $x,y,z \in \mathcal{Q}$, then $(x,y,z)n = n(x,y,z)$, where $n \in \mathcal{N}$.*

Proof. For every $x,y,z \in \mathcal{Q}$ and $n \in \mathcal{N}$ we have

$$xy \cdot zn = (xy \cdot z) \cdot n = (x \cdot yz) \cdot (x,y,z)n \,. \tag{1}$$

Since $\mathcal{N}$ is a normal subloop of $\mathcal{Q}(\cdot)$, then for every $x \in \mathcal{Q}$ and $n \in \mathcal{Q}$ there exist $n', n'' \in \mathcal{N}$ such that

$$xn = n'x \,, \quad nx = xn'' \,. \tag{2}$$

1991 Mathematics Subject Classification: 20N05
Keywords: loop, K-loop, nucleus, associator

Applying (2) to $xy \cdot zn$, we get

$$xy \cdot zn = xy \cdot n_1 z = xyn_1 \cdot z = (x \cdot n_2 y) \cdot z = (xn_2 \cdot y) \cdot z =$$
$$(n_3 x \cdot y) \cdot z = n_3(xy \cdot z) = (xn_2 \cdot yz) \cdot (x,y,z) = (x \cdot n_2 yz) \cdot (x,y,z) =$$
$$= (x \cdot yn_1 z) \cdot (x,y,z) = (x \cdot yz)n \cdot (x,y,z) = (x \cdot yz) \cdot n(x,y,z)$$

that is

$$xy \cdot zn = (x \cdot yz) \cdot n(x,y,z)\,. \tag{3}$$

If follows from (1) and (3) that $(x,y,z)n = n(x,y,z)$, which was to be proved. □

Corollary 1. *If a (nongroup) loop $\mathcal{Q}(\cdot)$ has a nontrivial nucleus $\mathcal{N}$ which is a normal subloop of $\mathcal{Q}(\cdot)$ and the associator of any three elements of $\mathcal{Q}$ belongs to $\mathcal{N}$, then $\mathcal{N}$ has a nontrivial center $\mathcal{Z}(\mathcal{N})$.* □

In [2] it is proved that in a K-loop $\mathcal{Q}(\cdot)$ the nucleus $\mathcal{N}$ contains the associator of any three elements of $\mathcal{Q}$.

Corollary 2. (Theorem 3 from [1]) *If a K-loop $\mathcal{Q}(\cdot)$ is not a group, then the nucleus $\mathcal{N}$ of $\mathcal{Q}(\cdot)$ has a nontrivial center.* □

Proposition 2. *The center $\mathcal{Z}(\mathcal{N})$ of the nucleus $\mathcal{N}$ of a K-loop $\mathcal{Q}(\cdot)$ is a normal subloop of $\mathcal{Q}(\cdot)$.*

Proof. In a K-loop $\mathcal{Q}(\cdot)$ the nucleus $\mathcal{N}$ is a normal subloop of $\mathcal{Q}(\cdot)$, therefore, $L_x^{-1}R_x c \in \mathcal{N}$ for every $c \in \mathcal{N}$ and every $x \in \mathcal{Q}$.

If $z \in \mathcal{Z}(\mathcal{N})$, then

$$z \cdot L_x^{-1}R_x c = L_x^{-1}R_x c \cdot z\,. \tag{4}$$

From the definition of a K-loop we have the autotopy

$$T = (R_x^{-1}L_x\,,\, L_x\,,\, L_x)\,. \tag{5}$$

Applying (5) to the equality (4), we get

$$R_x^{-1}L_x z \cdot L_x L_x^{-1}R_x c = L_x(L_x^{-1}R_x c \cdot z)$$

or

$$(R_x^{-1}L_xz\cdot c)=(L_xL_x^{-1}(cz\cdot x)Ix)$$

or

$$R_x^{-1}L_xz\cdot c=c\cdot(x\cdot zI_x)\,,$$

hence $R_x^{-1}L_xz\cdot c=c\cdot L_xR_{Ix}z$. Every K-loop is an Osborn loop where $R_{Ix}=L_x^{-1}R_x^{-1}L_x$ and then

$$R_x^{-1}L_xz\cdot c=c\cdot L_xL_x^{-1}R_x^{-1}L_xz$$

or

$$R_x^{-1}L_xz\cdot c=c\cdot R_x^{-1}L_xz\,,$$

which proves that $R_x^{-1}L_xz\in\mathcal{Z}(\mathcal{N})$. □

Proposition 3. *If a K-loop $\mathcal{Q}(\cdot)$ is not a group, the quotient loop $\mathcal{Q}/\mathcal{Z}(\mathcal{N})$ is a group.*

Proof. From Proposition 2 it follows that $\mathcal{Z}(\mathcal{N})$ is a normal subloop of $\mathcal{Q}(\cdot)$, hence there exists the quotient loop $\mathcal{Q}/\mathcal{Z}(\mathcal{N})$, in which

$$\begin{aligned}&a\mathcal{Z}(\mathcal{N})\cdot(b\mathcal{Z}(\mathcal{N})\cdot c\mathcal{Z}(\mathcal{N}))=\\&\qquad=a\mathcal{Z}(\mathcal{N})=(ab\cdot c)\mathcal{Z}(\mathcal{N})=(ab\cdot c)\cdot(a,b,c)\mathcal{Z}\mathcal{N})\,.\end{aligned}$$

As $(a,b,c)\in\mathcal{Z}(\mathcal{N})$, we have

$$\begin{aligned}&(ab\cdot c)\cdot(a,b,c)\mathcal{Z}(\mathcal{N})=(ab\cdot c)\mathcal{Z}(\mathcal{N})=ab\mathcal{Z}(\mathcal{N})\cdot c\mathcal{Z}\mathcal{N})=\\&\qquad=(a\mathcal{Z}(\mathcal{N})\cdot b\mathcal{Z}(\mathcal{N}))\cdot c\mathcal{Z}(\mathcal{N})\,.\end{aligned}$$

Thus,

$$a\mathcal{Z}(\mathcal{N})\cdot(b\mathcal{Z}(\mathcal{N})\cdot c\mathcal{Z}(\mathcal{N}))=(a\mathcal{Z}(\mathcal{N})\cdot b\mathcal{Z}(\mathcal{N})\cdot c\mathcal{Z}(\mathcal{N}))\,,$$

so the operation $(\cdot)$ on $\mathcal{Q}/\mathcal{Z}(\mathcal{N})$ is associative. □

Definition 1. The loop $\mathcal{Q}(\cdot)$ is called *solvable* if it has a series of the form

$$\mathcal{Q}=\mathcal{Q}_0\supseteq\mathcal{Q}_1\supseteq\mathcal{Q}_2\supseteq\ldots\supseteq\mathcal{Q}_m=E\,,$$

where $\mathcal{Q}_i$ is a normal subloop of $\mathcal{Q}_{i-1}$ and the quotient loop $\mathcal{Q}_{i-1}/\mathcal{Q}_i$ is an abelian group.

Theorem 1. *A K-loop generated by one element is solvable.*

Proof. Let an element $a \in \mathcal{Q}$ generates the K-loop $\mathcal{Q}(\cdot)$. From Proposition 3 we obtain that $\mathcal{Q}/\mathcal{Z}(\mathcal{N})$ is a group. If φ is a homomorphism of $\mathcal{Q}(\cdot)$ on $\mathcal{Q}/\mathcal{Z}(\mathcal{N})$, then the group $\mathcal{Q}/\mathcal{Z}(\mathcal{N})$ is also generated by an element, namely by $\varphi(a)$. But a group generated by an element is cyclic and since $\mathcal{Z}(\mathcal{N})$ is an abelian group, the loop $\mathcal{Q}(\mathcal{N})$ is solvable. □

Corollary. *Every subloop of a K-loop generated by one element is solvable.* □

Example 1. ([3], p.193). Let $\mathcal{F}$ be a field, $\mathcal{F}'$ be the set of nonzero elements of $\mathcal{F}$. Define on the set $\mathcal{Q} = \mathcal{F}' \times \mathcal{F}$ the operation $(\cdot)$ as follows:

$$(a,x) \cdot (b,y) = (a \cdot b\,,\ (a^{-1}-1)\cdot(b^{-1}-1) + b^{-1}x + y)\,.$$

Then $\mathcal{Q}(\cdot)$ is a K-loop. The nucleus $\mathcal{N}$ of this loop consists of pairs $(1,x), x \in \mathcal{F}$. The operation $(\cdot)$ is commutative on $\mathcal{N}$. Indeed,

$$(1,x)\cdot(1,y) = (1\,,\ x+y) = (1\,,\ y+x) = (1,y)\cdot(1,x)$$

hence, $\mathcal{N}$ is an abelian group. But then the loop $\mathcal{Q}(\cdot)$ from this example is solvable (for any field $\mathcal{F}$).

For $\mathcal{F} = \mathcal{Z}_3$ we get a K-loop consisting of six elements:

$*$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	1	6	4	5
3	3	1	2	5	6	4
4	4	5	6	2	3	1
5	5	6	4	1	2	3
6	6	4	5	3	1	2

This loop is generated by any of elements 4, 5, 6, so by Theorem 1 it is solvable. □

Example 2. Let $\mathcal{R}$ be a commutative ring (which is not $\mathcal{Z}_2$ and the zero ring). Define on $\mathcal{Q} = \mathcal{R} \times \mathcal{R}$ the operation $(\cdot)$

$$(a,x)\cdot(b,y) = (a+b\,,\ x+y+ab^2\,)$$

for any $(a,x),(b,y) \in \mathcal{Q}$. Then $\mathcal{Q}(\cdot)$ is a K-loop. If $\mathcal{R} = \mathcal{Z}_3$, we get a loop of 9 elements:

$\bullet$	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	3	1	5	6	4	8	9	7
3	3	1	2	6	4	5	9	7	8
4	4	5	6	8	9	7	3	1	2
5	5	6	4	9	7	8	1	2	3
6	6	4	5	7	8	9	2	3	1
7	7	8	9	2	3	1	6	4	5
8	8	9	7	3	1	2	4	5	6
9	9	7	8	1	2	3	5	6	4

This loop is one generated by each of the elements 4, 5, 6, 7, 8, 9. By Theorem 1 it is solvable.

Note that in this example the permutation I $(\,Ix = x^{-1}\,)$ is an automorphism of $\mathcal{Q}(\cdot)$. □

Definition 2. A K-loop is called an *IK-loop* if the permutation I is an automorphism of $\mathcal{Q}(\cdot)$, i.e. $I(x\cdot y) = Ix\cdot Iy$ for every $x,y\in\mathcal{Q}$.

Proposition 4. *If $\mathcal{N}$ is the nucleus of the loop $\mathcal{Q}(\cdot)$, then for any $x\in\mathcal{Q}$ and $c\in\mathcal{N}$ the equalities*

$$I(c\cdot x) = Ix\cdot Ic\,,\qquad I(x\cdot c) = Ic\cdot Ix \tag{6}$$

hold up.

Proof. Directly from the equality $cx\cdot I(c\cdot x) = 1$ it follows that $x\cdot I(c\cdot x) = x^{-1}$ or $I(c\cdot x) = L_x^{-1}Ic$ or $I(c\cdot x) = L_{Ix}L_{Ix}^{-1}L_x^{-1}Ic$. But

$$L_xL_{Ix}c = x\cdot Ixc = (x\cdot Ix)\cdot c = c\,.$$

Hence, $L_{Ix}^{-1}L_x^{-1}Ic = Ic$ and then $I(c\cdot x) = L_{Ix}Ic = Ix\cdot Ic$. The second equality can be proved similarly. □

Proposition 5. *The center $\mathcal{Z}(\mathcal{Q})$ and the nucleus $\mathcal{N}$ of an IK-loop $\mathcal{Q}(\cdot)$ coincide.*

Proof. Let $\mathcal{Q}(\cdot)$ be an *IK*-loop. Then the permutation I is an automorphism of $\mathcal{Q}(\cdot)$ and $I(x \cdot y) = Ix \cdot Iy$ for any $x, y \in \mathcal{Q}$. In particular, if $x \in \mathcal{Q}$ and $c \in \mathcal{N}$, then

$$I(c \cdot x) = Ic \cdot Ix\,. \tag{7}$$

From (6) and (7) it follows that

$$Ix \cdot Ic = Ic \cdot Ix\,. \tag{8}$$

From (8) and $c \in \mathcal{N}$ we obtain $c \in \mathcal{Z}(\mathcal{Q})$, therefore

$$\mathcal{N} \subseteq \mathcal{Z}(\mathcal{Q})\,. \tag{9}$$

But from the definition of the center of a loop it follows that

$$\mathcal{Z}(\mathcal{Q}) \subseteq \mathcal{N}\,. \tag{10}$$

Thus, from (9) and (10) we get $\mathcal{Z}(\mathcal{Q}) = \mathcal{N}$. □

Definition 3. A loop $\mathcal{Q}(\cdot)$ is *nilpotent* if it has a finite invariant series

$$\mathcal{Q} = \mathcal{Q}_0 \supseteq \mathcal{Q}_1 \supseteq \mathcal{Q}_2 \supseteq ... \supseteq \mathcal{Q}_k = E\,,$$

where every quotient loop $\mathcal{Q}_{i-1}/\mathcal{Q}_i$ is contained in the center of the loop $\mathcal{Q}/\mathcal{Q}_i$ $(i = 1, 2, ..., k)$.

Theorem 2. *Every IK-loop $\mathcal{Q}(\cdot)$ is nilpotent.*

Proof. Let $\mathcal{Q}(\cdot)$ be a nongroup *IK*-loop, then $\mathcal{Q}(\cdot)$ has a nontrivial nucleus $\mathcal{N}$, which by Proposition 5 coincides with the center of $\mathcal{Q}(\cdot)$, i.e. $\mathcal{N} = \mathcal{Z}(\mathcal{Q})$. Hence, for the loop $\mathcal{Q}(\cdot)$ there is a series of normal subloops

$$\mathcal{Q} = \mathcal{Q}_0 \supseteq \mathcal{Q}_1 \supseteq \mathcal{Q}_2 = E\,,$$

satisfying the condition: $\mathcal{Q}_{i-1}/\mathcal{Q}_i \subseteq \mathcal{Z}(\mathcal{Q}/\mathcal{Q}_i)$, $i = 1, 2$, and this means that $\mathcal{Q}(\cdot)$ is nilpotent.

References

[1] **A. S. Basarab**: *Non-associative extensions of groups by means of abelian groups*, Proc. Intern. Conf. on Group Theory, Timishoara 1992, $6-10$.

[2] **A. S. Basarab**: *K-loops*, (Russian), Buletinul AS Rep. Moldova, ser. Matematica **1(7)** (1992), $28-33$.

[3] **V. D. Belousov**: *Foundations of the Theory of Quasigroups and Loops*, (Russian), "Nauka", Moscow, 1967.

Department of Physics and Mathematics,
Tiraspol State University,
5 Iablocikin str.,
Kishinau, 277050
MOLDOVA

Received August 20, 1995

Quadratical quasigroups

Wiesław A. Dudek

Abstract

Quadratical quasigroups, which have a beautiful geometrical interpretation, are characterized by commutative groups and some of their automorphisms.

A groupoid $(G,\cdot)$ is said to be *quadratical* if the identity

$$xy\cdot x = zx\cdot yz \tag{1}$$

holds and the equation $ax=b$ has a unique solution $x\in G$ for all $a,b\in G$.

Quadratical groupoids arose originally from the geometrical situation described by the field of complex numbers $\mathbf{C}$ and the operation $*$ on $\mathbf{C}$ defined by

$$x*y=(1-q)x+qy\,,$$

where $q=\frac{1}{2}(1+i)$ (cf. [3] or [4]). The geometrical interpretation of $(G,*)$ motivates us to the further study of quadratical groupoids.

Quadratical groupoids are idempotent quasigroups (cf. [4]). Such quasigroups are also medial and distributive (cf. [4]). This means (cf. Theorem 8.3 from [2]) that such quasigroups are transitive. Hence (cf. Theorem 8.1 from [2]) every quadratical groupoid is isotopic to some commutative Moufang loop.

The above results together with the above example suggest that every quadratical groupoid may be described by some commutative group and some of its automorphisms.

1991 Mathematics Subject Classification: 20N05
Keywords: quadratical groupoid, quasigroup, isotopy

Theorem. *A groupoid* $(G,\cdot)$ *is a quadratical quasigroup if and only if there exists a commutative group* $(G,+)$ *in which for every* $a\in G$ *the equation* $z+z=a$ *has a unique solution* $z=\frac{1}{2}a\in G$ *and* φ, ψ *are automorphisms of* $(G,+)$ *such that for all* $x,y\in G$

$$xy=\varphi(x)+\psi(y), \tag{2}$$

$$\varphi(x)+\psi(x)=x, \tag{3}$$

$$2\psi\varphi(x)=x. \tag{4}$$

Proof. Since a quadratical groupoid $(G,\cdot)$ is a transitive distributive quasigroup, then from results obtained in [1] it follows that there exists a commutative group $(G,+)$ and its automorphisms φ, ψ such that (2) and (3) hold.

Replacing in (1) an element x by 0 (i.e. by the neutral element of $(G,+)$) and applying (2) we obtain

$$\varphi\psi(y)=\varphi^2(z)+\psi\varphi(y)+\psi^2(z),$$

which for $y=0$ gives

$$\varphi^2(z)+\psi^2(z)=0. \tag{5}$$

Hence

$$\varphi\psi(y)=\psi\varphi(y) \tag{6}$$

for every $y\in G$.

Since from (3) immediately follows $\varphi^2(x)+\varphi\psi(x)=\varphi(x)$ and $\psi^2(x)+\psi\varphi(x)=\psi(x)$, then

$$\varphi^2(x)+\psi^2(x)+\varphi\psi(x)+\psi\varphi(x)=\varphi(x)+\psi(x)=x,$$

which together with (5) and (6) implies (4).

Now applying (2) and (6) to the identity $y=xy\cdot yx$, which holds in all quadratical groupoids (cf. [4] Theorem 1) we obtain

$$y=\varphi^2(x)+\varphi\psi(y)+\psi\varphi(y)+\psi^2(x)=\varphi\psi(y)+\varphi\psi(y)\,.$$

Hence

$$\varphi^{-1}(y) = \psi(y) + \psi(y)$$

for all $y \in G$. This proves that every $a \in G$ $(a = \varphi^{-1}(y))$ may be written as $a = z + z$.

If also $a = u + u$ for some $u \in G$, then there exists $v \in G$ such that $u = \psi(v)$. Hence

$$a = \psi(v) + \psi(v) = \varphi^{-1}(v)\,,$$

which gives $\varphi^{-1}(y) = \varphi^{-1}(v)$. Thus $y = v$ and, in the consequence, $z = u$. This proves that the equation $a = z + z$ has a unique solution for every $a \in G$.

Conversely, assume that $(G, +)$ is a commutative group in which for every $a \in G$ there is only one $x = \frac{1}{2}a$ such that $x + x = a$. If φ and ψ are automorphisms of $(G, +)$ satisfying (3) and (4), then a groupoid $(G, \cdot)$ defined by (2) is a quasigroup and its quasigroup operation may be written in the form

$$xy = x + \psi(y - x). \tag{7}$$

From (3) and (4) we obtain also

$$\psi^2(x) - \psi(x) = \frac{1}{2}\,x$$

for all $x \in G$.

This together with (7) (after some simplifications) gives

$$xy \cdot x = x - \psi(x) + \psi^2(x) + \psi(y) - \psi^2(y) = \tfrac{1}{2}\,x + \tfrac{1}{2}\,y\,,$$

$$zx{\cdot}yz = \psi(x) - \psi^2(x) + \psi(y) - \psi^2(y) + z - 2\psi(z) + 2\psi^2(z) = \tfrac{1}{2}\,x + \tfrac{1}{2}\,y,$$

which proves (1). Hence this groupoid is a quadratical quasigroup. □

Corollary 1. *A finite quadratical quasigroup has odd order.*

Proof. Indeed, by Cauchy's theorem, in a group of even order there are at least two elements x satisfying $x + x = 0$. □

Corollary 2. *A quadratical groupoid defined by the additive group of a field* $(F,+,\cdot\,)$ *with* char $F\neq 2$ *has the form*

$$x*y=ax+(1-a)y\,,$$

where $a\in F$ *is a solution of the equation*

$$2a^2-2a+1=0\,. \tag{8}$$

Proof. All automorphisms of the additive group of F have the form $\varphi(x)=ax$, where $a\in F$. Moreover, (3) and (4) are equivalent to (8). Hence a quasigroup defined by $\varphi(x)=ax$ and $\psi(x)=(1-a)x$ is quadratical if and only if a satisfies (8). □

Now we compute all quadratical quasigroups of order $n\leq 24$. As it is well known commutative groups of odd order $n\leq 24$ are (up to isomorphism) either Z_n or $Z_3\times Z_3$. In the first case all automorphisms have the form $\varphi(x)=ax$, where $a\in\{1,2,...,n-1\}$. Hence, by the Theorem, all quadratical quasigroups defined on Z_n have the form $xy=ax+by$, where $a+b\equiv 1(mod\;n)$, $2ab\equiv\,1(mod\;n)$ and n is odd. Direct computations show that for odd $n\leq 24$ the last two equations have solutions (listed bellow) only for $n=5,13,17$.

n	5		13		17	
a	2	4	3	11	7	11
b	4	2	11	3	11	7

This means that a quadratical quasigroup defined on the group Z_n, $n\leq 24$, has the form

$$\begin{aligned}
x*y&=2x+4y(mod\;5),\\
x*y&=4x+2y(mod\;5),\\
x*y&=3x+11y(mod\;13),\\
x*y&=11x+3y(mod\;13),\\
x*y&=7x+11y(mod\;17),\\
x*y&=11x+7y(mod\;17).
\end{aligned}$$

In the second case, all automorphisms are determined (as a linear transformations of the vector space $Z_3 \times Z_3$) by some matrices (in the basis $e_1 = (1,0)$, $e_2 = (0,1)$) such that $A + B \equiv I(mod\, 3)$ and $2AB \equiv I(mod\, 3)$. Direct calculations show that the matrix A has the forms:

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 2 \\ 2 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}, \quad \begin{bmatrix} 2 & 1 \\ 2 & 2 \end{bmatrix}, \quad \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix}.$$

Computing B and replacing obtained matrices by corresponding linear transformations, we see that the quadratical quasigroup defined on the group $Z_3 \times Z_3$ has one of the following forms:

$$\begin{aligned}
(x,y) * (z,u) &= (y + z + 2u\,,\ x + y + 2z),\\
(x,y) * (z,u) &= (2y + z + u\,,\ 2x + y + z),\\
(x,y) * (z,u) &= (x + y + 2u\,,\ x + 2z + u),\\
(x,y) * (z,u) &= (x + 2y + u\,,\ 2x + z + u),\\
(x,y) * (z,u) &= (2x + y + 2z + 2u\,,\ 2x + 2y + z + 2u),\\
(x,y) * (z,u) &= (2x + 2y + 2z + u\,,\ x + 2y + 2z + 2u).
\end{aligned}$$

References

[1] **V. D. Belousov**: *Transitive distributive quasigroups*, (Russian), Ukrain. Math. Zh. **10** (1958), 13 – 22.

[2] **V. D. Belousov**: *Fundations of the theory of quasigroups and loops*, (Russian), Nauka, Moscow 1967.

[3] **M. Osborn**; *New loops from old geometries*, Amer. Math. Monthly **68** (1961), 103 – 107.

[4] **V. Volenec**: *Quadratical groupoids*, Note di Mat. **13** (1993), 107 – 115.

Received December 15, 1997

Institute of Mathematics
Technical University
Wybrzeże Wyspiańskiego 27
50-370 Wrocław
Poland
e-mail: dudek@im.pwr.wroc.pl

Quasigroups and Related Systems, **4** (1997), 15–21

About some computer investigation of the endomorphisms of the linear isotopes of small order non-cyclic groups

Oleg U. Kirnasovsky and Sergej Sevastianov

Abstract

The order of the automorphism group and the endomorphism monoid of linear isotopes for non-cyclic groups are found up to 15-th order.

1. Introduction

A groupoid $(Q;\cdot)$ is called a *linear isotope of a group* $(Q;+)$, or a *linear group isotope*, iff there exist an element a and automorphisms φ, ψ of the group such that the equality

$$x\cdot y=\varphi x+\psi y+a \tag{1}$$

holds. It is easy to see that a group isotope is a quasigroup.

The group isotopes were studied in [3], [4] and [5]. Isomorphisms between two group isotopes are described in [1]. The list of all pairwise non-isomorphic linear group isotopes up to 15-th order is printed in [2]. This list contains 1554 quasigroups. Exactly 975 of them are linear isotopes of non-cyclic groups.

Combining the results from [2] and [3] we obtain the following

1991 Mathematics Subject Classification: 20N05
Keywords: endomorphism, automorphism, isotopy

Lemma. *A permutation α of a linear isotope $(Q;\cdot)$ of a group $(Q;+)$ defined by the equality* (1) *is an endomorphism of the isotope iff*

$$\alpha = R_c\theta, \quad \theta\varphi = \varphi\theta, \quad I_{\varphi c}\theta\psi = \psi\theta, \quad \theta a = \varphi c + \psi c + a - c$$

for some element c and some endomorphism θ of the group, where R_c denotes the right translation of the group with an element c, and $I_{\varphi c}$ denotes the inner automorphism $I_{\varphi c}x = -\varphi c + x + \varphi c$.

2. Description of the main algorithm

An algorithm, which describes all linear isotopes of an arbitrary fixed group defined by its Cayley table and its generator system, is given in [2]. Let us alter the algorithm supplementing it with some part.

Note that for a real computer employment it is useful to execute two almost the same algorithms. In the first one we limit ourself to the search of the list of all linear isotopes of the given group saving on magnetic information carriers the respective ordinal numbers of the automorphisms and of the free members from the canonical decompositions. It gives us the possibility in the second algorithm to avoid the preservation of the Cayley table (which is important in the first algorithm) of the automorphism group of the given group which economizes the necessary operative memory. There is also no necessity to use blocks, which were needed in the initial algorithm from [2].

To construct the second algorithm we add to the algorithm from [2] new blocks:

1. we compose information on the endomorphisms of the given group as we did it in [2] for automorphisms, and, in addition, we construct the table where every square corresponds to each next endomorphism and contains the information about its bijectivity;

2. in the certain place of the algorithm we read the parameters of each next linear group isotope;

3. looking over all pairs $\langle\theta, c\rangle$, where θ is an endomorphism of the given group and c is an element of the group, we verify fulfillment of the equalities of criterion, given in the Lemma; if $R_c\theta$

is an endomorphism of the investigated isotope, we add the unit to the score of number of the endomorphisms of the isotope (endomorphism doesn't appear twice, because different pairs define different endomorphisms);

4. taking into account that the transformation $R_c\theta$ is an automorphism of this isotope iff the transformation θ is bijective, we calculate the number of automorphisms of the isotope remembering the respective pairs in an individual table (in fact, we can remember the ordinal numbers of θ and c);

5. if the number of the automorphisms is not greater than 15, we create the Cayley table of the automorphism group of the isotope; for this purpose, we make the search of all triples $\langle\alpha, \beta, \gamma\rangle$ of the automorphisms of this isotope, and we put $\gamma = \alpha\beta$ iff γ and $\alpha\beta$ define the same act on the basis set;

6. we determine commutativity of the automorphism group and the number of its subgroups in the same way as we did for the main group in [2]; these two characteristics together with the order of this automorphism group synonymously define this group up to isomorphism, since its order is not greater than 15.

3. Main results

This algorithm was applied to all 13 non-cyclic groups up to 15-th order inclusively using IBM PC.

If $(abcd, efgh, ij)$ is the representation from [2] for a linear isotope of the group D_3, then for the linear isotope of the 12-th order group

$$G_{12} = \langle\, a, b \,|\, a^4 = b^3 = 1,\ ba = ab^2\,\rangle$$

with the representation $(d^{'}cba,\ h^{'}gfe,\ ji)$, where

$$d \equiv d^{'}(\operatorname{mod} 2), \quad h \equiv h^{'}(\operatorname{mod} 2),$$

the number of all endomorphisms is twice greater than the number of all endomorphisms of the respective isotope of the group D_3. The automorphism group is isomorphic to the direct product of the group

Z_2 on the automorphism group of the respective isotope of the group D_3 (recall, that $Z_2 \times D_3 \simeq D_6$).

The numbers of all automorphisms and all endomorphisms are given across the symbol / . With that, the automorphism groups having the order up to 15 are discerned with the help of the letter placed after the number of the automorphisms. If such group is cyclic, then this letter is omitted. We use also the following symbols:

- the group $Z_2 \times Z_2$ is denoted as 4a ,
- the group $Z_6 \times Z_2$ is denoted as 12a ,
- the group $Z_3 \times Z_3$ is denoted as 9a ,
- the group $Z_2 \times Z_2 \times Z_2$ is denoted as 8a ,
- the group D_3 is denoted as 6a ,
- the group D_4 is denoted as 8b ,
- the group D_6 is denoted as 12b ,
- the group A_4 is denoted as 12c .

The symbol * denotes the automorphism group of the isotope which is isomorphic to the respective group.

The group $Z_2 \times Z_2$.
2/4. 2/4. 2/2. 2/4. 2/4. 2/2. 2/4. 2/2. 3/4. 3/4. 12c/16. 4a/4. 2/4. 3/4. 6a/16*.

The group $Z_4 \times Z_2$**.**
8b/32*. 4a/8. 4a/8. 4/8. 8b/32. 4a/8. 4a/8. 2/4. 2/4. 4a/8. 4a/8. 4a/8. 2/4. 4a/8. 2/4. 4a/8. 4a/8. 4/8. 2/4. 2/4. 4/8. 4/8. 4/8. 8b/32. 4a/8. 4a/8. 4/8. 8b/32.

The group $Z_6 \times Z_2$**.**
12b/48*. 4a/12. 6/12. 4a/12. 6/12. 12b/48. 4a/12. 4a/12. 4a/12. 4a/6. 4a/12. 4a/6. 4a/12. 4a/6. 4a/12. 4a/6. 4a/12. 4a/12. 6/12. 4a/12. 4a/6. 6/12. 4a/12. 4a/6. 24/48. 8a/12. 24/48. 8a/12. 6/12. 6/12. 4a/12.

4a/12. 4a/6. 4a/12. 4a/6. 12b/36. 6/12. 12b/36. 12b/18. 6/12. 6/6. 4a/12. 12b/36. 6/12. 12b/36. 6/6. 6/12. 12b/18. 6/12. 4a/12. 4a/6. 24/48. 8a/12. 12b/36. 12b/18. 6/12. 6/6. 18/36. 9a/12. 6/12. 18/36. 9a/12. 72/144. 24/36. 12a/12. 36/48. 12b/48. 4a/12. 6/12. 12b/36. 6/12. 18/36. 9a/12. 36/144. 18/48.

The group $Z_3 \times Z_3$.
12b/27. 6/9. 2/3. 2/3. 2/3. 6a/9. 3/3. 2/3. 6a/9. 3/3. 2/3. 4a/9. 6a/9. 3/3. 2/3. 4a/9. 2/3. 2/3. 2/3. 6a/9. 3/3. 6a/9. 3/3. 2/3. 2/3. 6a/9. 3/3. 6a/9. 3/3. 6a/9. 3/3. 12b/27. 6/9. 2/3. 2/3. 2/3. 2/3. 8/9. 6a/9. 3/3. 6a/9. 3/3. 2/3. 2/3. 6a/9. 3/3. 2/3. 8/9. 8/9. 2/3. 6a/9. 3/3. 8/9. 6a/9. 3/3. 72/81. 9a/9. 8/9. 8/9. 8/9. 2/3. 6a/9. 3/3. 8/9. 2/3. 2/3. 6a/9. 3/3. 2/3. 8/9. 6a/9. 3/3. 8/9. 2/3. 6a/9. 3/3. 8/9. 6a/9. 3/3. 72/81. 9a/9. 8/9. 8/9. 8/9. 2/3. 6a/9. 3/3. 2/3. 8/9. 2/3. 6a/9. 3/3. 8/9. 6a/9. 3/3. 2/3. 8/9. 6a/9. 3/3. 2/3. 6a/9. 3/3. 8/9. 72/81. 9a/9. 8/9. 8/9. 8/9. 6a/9. 3/3. 2/3. 2/3. 2/3. 18/27. 9a/9. 2/3. 6a/9. 3/3. 2/3. 6/9. 6a/9. 3/3. 6/9. 2/3. 6a/9. 3/3. 2/3. 6a/9. 3/3. 2/3. 54/81. 9a/9. 27/27. 6a/9. 3/3. 18/27. 9a/9. 6/9. 2/3. 2/3. 6a/9. 3/3. 6a/9. 3/3. 2/3. 6/9. 2/3. 6/9. 6a/9. 3/3. 2/3. 6/9. 2/3. 6a/9. 3/3. 2/3. 6a/9. 3/3. 6/9. 2/3. 6a/9. 3/3. 6/9. 6/9. 4a/9. 8/9. 8/9. 8/9. 6/9. 6/9. 48/81*. 48/81. 12b/27. 6/9. 8/9. 8/9. 8/9. 18/27. 9a/9. 6/9. 48/81. 432/729. 54/81.

The group $Z_2 \times Z_2 \times Z_2$.
8b/32. 2/8. 2/4. 2/4. 2/4. 2/4. 2/2. 1/2. 2/4. 2/2. 2/4. 2/2. 1/2. 1/2. 2/4. 2/2. 4a/8. 2/4. 2/2. 1/2. 2/8. 2/4. 1/2. 2/4. 2/2. 2/4. 1/2. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 4a/8. 2/4. 4/8. 8b/32. 2/8. 2/4. 3/8. 2/4. 2/2. 1/2. 2/4. 2/2. 1/2. 1/2. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 1/2. 1/2. 1/2. 1/2. 2/4. 2/2. 1/2. 2/4. 2/2. 1/2. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 1/2. 2/4. 2/2. 2/4. 2/2. 1/2. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 1/2. 2/4. 2/2. 1/2. 2/4. 2/2. 4a/8. 4a/4. 4a/4. 4a/4. 4a/8. 4a/4. 4a/4. 4a/4. 2/4. 2/2. 1/2. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 4a/8. 4a/4. 4a/4. 4a/4. 1/2. 2/4. 2/2. 3/8. 1/2. 1/2. 1/2. 2/4. 2/2. 2/4. 2/2. 12c/32. 4a/8. 4a/8. 4a/4. 4a/4. 4a/4. 4a/8. 4a/4. 4a/4. 4a/4. 2/4. 2/2. 2/4. 2/2. 2/4. 2/4. 2/2. 4/8. 2/4. 2/2. 1/2. 1/2. 2/4. 2/2. 2/4. 2/2. 4a/8. 4a/4. 4a/4. 4a/4. 4a/8. 4a/4. 4a/4. 4a/4. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 1/2. 2/4. 2/2. 1/2. 2/4. 2/2. 1/2. 2/4. 2/2. 1/2. 1/2. 2/4. 2/2. 1/2. 2/4. 2/2. 1/2.

1/2. 2/4. 2/2. 1/2. 1/2. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 4/8. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 4a/8. 4a/4. 4a/4. 4a/4. 4a/8. 4a/4. 4a/4. 4a/4. 4/8. 2/4. 2/4. 2/2. 2/4. 2/2. 4/8. 2/4. 2/2. 1/2. 1/2. 2/4. 2/2. 7/8. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 4a/8. 4a/4. 4a/4. 4a/4. 4a/8. 4a/4. 4a/4. 4a/4. 1/2. 2/4. 2/2. 1/2. 2/4. 2/2. 1/2. 2/4. 2/2. 1/2. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 4a/8. 4a/4. 4a/4. 4a/4. 7/8. 7/8. 2/4. 2/2. 7/8. 56/64. 8a/8. 7/8. 7/8. 1/2. 2/4. 2/2. 2/4. 2/2. 1/2. 2/4. 2/2. 7/8. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 4a/8. 4a/4. 4a/4. 4a/4. 2/4. 2/2. 4a/8. 4a/4. 4a/4. 4a/4. 1/2. 1/2. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 1/2. 2/4. 2/2. 1/2. 7/8. 2/4. 2/2. 2/4. 2/2. 2/4. 2/2. 7/8. 4a/8. 4a/4. 4a/4. 4a/4. 7/8. 56/64. 8a/8. 7/8. 7/8. 8b/32. 3/8. 4/8. 7/8. 7/8. 168/512*.

The group D_3.
6a/10*. 2/4. 3/4. 3/4. 1/2. 3/4. 3/4. 2/4. 2/6. 1/2. 1/1.

The group D_4.
8b/36*. 4a/20. 8b/12. 4/6. 4a/6. 4/6. 2/4. 4/6. 4/6. 2/4. 4/6. 8b/12. 4a/8. 8b/12. 4/6. 4a/6. 4a/20. 4a/20. 4a/8. 4a/8. 2/4. 2/4. 4a/6. 2/4. 4a/6. 2/4. 4a/6. 4a/6.

The group D_5.
20/26*. 4/6. 5/6. 4/6. 4/6. 5/6. 1/2. 5/6. 5/6. 5/6. 5/6. 1/2. 1/2. 4/6. 4/10. 1/2. 1/1. 4/6. 4/6. 1/2. 1/2. 4/6. 4/6. 1/2. 1/2. 4/6. 4/10. 1/2. 1/1. 4/6. 4/6. 1/2. 1/2. 4/10. 4/6. 1/1. 1/2.

The group D_6.
12b/64*. 4a/24. 6/16. 6/8. 4a/8. 12b/20. 6/8. 2/4. 6/8. 6/8. 6/8. 2/4. 6/8. 6/8. 6/16. 2/8. 6/16. 6/16. 6/8. 2/4. 6/8. 6/8. 12b/20. 4a/8. 6/8. 6/8. 4a/8. 12b/20. 4a/24. 4a/32. 2/8. 2/4. 2/4. 2/2. 4a/12. 4a/8. 4a/8. 2/2. 2/4. 4a/12. 2/4. 4a/12. 2/2. 4a/8.

The group D_7.
42/50*. 6/8. 7/8. 6/8. 6/8. 6/8. 6/8. 7/8. 1/2. 7/8. 7/8. 7/8. 7/8. 7/8. 7/8. 1/2. 1/2. 1/2. 1/2. 6/8. 6/14. 1/2. 1/1. 6/8. 6/8. 1/2. 1/2. 6/8. 6/8. 1/2. 1/2. 6/8. 6/8. 1/2. 1/2. 6/8. 6/14. 1/2. 1/1. 6/8. 6/8. 1/2. 1/2. 6/8. 6/8. 1/2. 1/2. 6/8. 6/8. 1/2. 1/2. 6/8. 6/14. 1/2. 1/1. 6/8. 6/8. 1/2. 1/2. 6/8. 6/8. 1/2. 1/2. 6/14. 6/8. 1/1. 1/2. 6/8. 6/8. 1/2.

1/2. 6/14. 6/8. 1/1. 1/2. 6/8. 6/8. 1/2. 1/2.

The group Q_8.
4a/6. 2/4. 4a/6. 1/3. 1/1. 4a/6. 2/4. 4a/6. 2/4. 2/4. 2/2. 2/2. 1/3. 1/1. 1/3. 1/1. 3/4. 1/2. 3/4. 1/2. 3/7. 1/1. 2/4. 4/6. 4/6. 1/3. 1/1. 4/6. 2/4. 4/6. 2/4. 2/4. 2/2. 2/2. 4a/6. 4/6. 3/4. 24/28*. 8b/12. 2/4. 2/4. 1/2. 8b/12. 4a/8. 8b/12. 4/6. 4a/6.

The group A_4.
24/33*. 3/6. 8b/9. 4a/9. 4/5. 3/6. 3/9. 3/6. 1/2. 1/2. 1/1. 1/5. 1/1. 1/1. 1/3. 4a/9. 1/5. 4a/5. 1/1. 2/3. 4a/21. 1/4. 4a/5. 1/1. 2/5. 4/5. 1/1. 1/3. 4/5. 2/3. 2/5. 1/1. 1/1. 4/5. 4/9. 8b/9. 1/2. 4a/5. 8b/9. 2/3. 4a/5. 4/5. 2/3.

The authors express their great thanks to Dr. Fedir Sokhatsky for the permanent attention to their work.

References

[1] **V. I. Izbash**: *Isomorphisms of quasigroups isotopic to groups*, Quasigroups and Related Systems **2** (1995), 34 – 50.

[2] **O. U. Kirnasovsky**: *Linear isotopes of small order groups*, Quasigroups and Related Systems **2** (1995), 51 – 82.

[3] **F. Sokhatsky**: *On isotopes of groups. I*, (Ukrainian), Ukrain. Math. Zh. **47** (1995), 1387 – 1398.

[4] **F. Sokhatsky**: *On isotopes of groups. II*, (Ukrainian), Ukrain. Math. Zh. **47** (1995), 1692 – 1703. (English translation in Ukrainian Math. J. **47** (1995), 1935 – 1948.)

[5] **F. Sokhatsky**: *On isotopes of groups. III*, (Ukrainian), Ukrain. Math. Zh. **48** (1996), 251 – 259.

Department of Algebra
Vinnytsia State Pedagogical University
Vinnytsia 287100
Ukraine

Received 15 September 1997

Quasigroups and Related Systems, **4** (1997), 23–38

The transitive and multitransitive automorphism groups of the multiplace quasigroups

Oleg U. Kirnasovsky

Abstract

In this paper, for every k, the multiplace group isotopes, which have $k-$transitive automorphism groups, are described.

1. Introduction

A groupoid $(G;g)$ is called an *isotope of a group* $(Q;+)$, iff for some bijections γ_1, ..., γ_n and γ of G on Q the equality

$$\gamma g(x_1,\ldots,x_n)=\gamma_1 x_1+\ldots+\gamma_n x_n$$

holds. The groupoid $(G;g)$ is called also a *group isotope*. A groupoid $(G;g)$ is called a *linear isotope* of a group $(G;+)$ iff there are automorphisms $\alpha_1,\ldots,\alpha_n$ of a group $(G;+)$ such that

$$g(x_1,\ldots,x_n)=\alpha_1 x_1+\ldots+\alpha_n x_n+a$$

for some fixed $a\in G$. It is easy to see that every group isotope is a quasigroup. Also a quasigroup isomorphic to a linear isotope is a linear isotope.

Let $S(Q)$ be a permutation group of Q. We say that a group $S(Q)$ is *k-times transitive (or k-transitive) on the set* $H\subset Q$, where k is a

1991 Mathematics Subject Classification: 20N05, 20N15
Keywords: quasigroup, isotopy, n-ary quasigroup

fixed cardinal number, iff $|H| \geq k$, $\sigma(H) = H$ for every $\sigma \in S(Q)$ and for each bijection $\varphi : A \to B$ of k-element subsets A, B of H there exists $\alpha \in S(Q)$ such that $\alpha x = \varphi x$ for all $x \in A$.

1-transitive group will be also called *transitive*. The words "on the set H" will be omitted if $H = Q$.

The D-quasigroups, i.e. the finite binary quasigroups having double-transitive automorphism groups, are investigated in [3]. The finite binary groupoids having double-transitive automorphism groups are described in [2]. Here we continue the investigation for the case of the multiplace quasigroups.

The author would like to expresses his sincere thanks to Dr. Volodymyr Derech for suggesting the problem. Author also expresses his great thanks to Dr. Fedir Sokhatsky for his very useful comments.

2. Some individual cases

Theorem 1. *The automorphism group of an unary quasigroup* $(Q; f)$ *is transitive iff either all cycles of* f *are infinite, or all these cycles are finite and have the same length.*

Proof. Let the automorphism group be transitive and

$$(x_1, \ldots, x_n), \quad (\ldots, y_1, \ldots, y_n, \ldots)$$

be some cycles of f, and let the length of the second cycle be greater than n (or be infinite). Transitivity of the automorphism group implies the existence of an automorphism α of the unary quasigroup $(Q; f)$, for which $\alpha x_1 = y_1$. Then α commutes with f, and in the consequence, with f^n. Thus $y_{n+1} = f^n y_1 = f^n \alpha x_1 = \alpha f^n x_1 = \alpha x_1 = y_1$, which is a contradiction.

On the other hand, let all cycles of f have the same (may be infinite) length and let $x, y \in Q$ be arbitrary elements. If they are in the same cycle, then there exists a positive integer n such that $f^n x = y$ and f^n is an automorphism of $(Q; +)$. If $x = x_1$, $y = y_1$, and

$$(\ldots, x_1, \ldots, x_n, \ldots), \quad (\ldots, y_1, \ldots, y_n, \ldots)$$

are different cycles of f, then the permutation α being the product of all cycles of the type (x_i, y_i) is an automorphism of $(Q; f)$, with the condition $\alpha x = y$. This proves the transitivity. $\square$

We say that a groupoid $(Q; h)$ is *derived from a group* $(Q; +)$, iff

$$h(x_1, \ldots, x_n) = x_1 + \ldots + x_n\,. \tag{1}$$

Lemma 2. *Every quasigroup with at most* 3 *elements is a linear isotope of a cyclic group.*

Proof. Let $(Q; f)$ be a quasigroup. For $|Q| = 1$ the lemma is evident. Let $|Q| > 1$. We consider the ring $(Q; +, \cdot)$. The element 0 is an idempotent of the operation g:

$$g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) - f(0, \ldots, 0).$$

Define the operation h by

$$\begin{aligned} &h(x_1, x_2, \ldots, x_n) = \\ &\quad = g(g(1, 0, \ldots, 0) \cdot x_1, g(0, 1, 0, 0, \ldots, 0) \cdot x_2, \ldots, g(0, \ldots, 0, 1) \cdot x_n). \end{aligned}$$

We prove that the groupoid $(Q; h)$ is derived from the cyclic group $(Q; +)$. For $|Q| = 2$ the equality is easy provable by the induction on the number of the appearances of the element 1 in the collection $\langle x_1, \ldots, x_n\rangle$. Let $|Q| = 3$. Denote by r_i the number of the appearances for an element i in the collection $\langle x_1, \ldots, x_n\rangle$. For $k = 0$ we have:

$$h(0, \ldots, 0) = g(0, \ldots, 0) = 0.$$

Assume by the induction that this is true for $k = j$. We prove it for $k = j + 1$. At first, we consider the case when r_1 and r_2 are positive. Then we replace either one of the appearances of the element 1 by the element 0, or one of the appearances of the element 2 by the element 0. In this case the result of the operation will be changed because h is a quasigroup operation. Then by the inductive hypothesis the result of the application of h to the given collection is not equal modulo 3 to none of the numbers

$$(r_0 + 1) \cdot 0 + (r_1 - 1) \cdot 1 + r_2 \cdot 2, \quad (r_0 + 1) \cdot 0 + r_1 \cdot 1 + (r_2 - 1) \cdot 2,$$

and consequently, is equal to $0 \cdot r_0 + 1 \cdot r_1 + 2 \cdot r_2 = r_1 + 2r_2$.

Now, let $r_1 = 0$, then $r_2 \neq 0$, since $k > 0$. For $r_2 = 1$ the statement follows from the construction of the operation h. If $r_2 > 1$, then we replace either one of the appearances of the element 2 by the element 0, or one of the appearances of the element 2 by the element 1. Then by the hypothesis and by the statement proved above, the result of the application of h to the given collection is not equal modulo 3 to none of the numbers

$$(r_0 + 1) \cdot 0 + r_1 \cdot 1 + (r_2 - 1) \cdot 2, \quad r_0 \cdot 0 + (r_1 + 1) \cdot 1 + (r_2 - 1) \cdot 2.$$

Now, let $r_2 = 0$. Then we replace either one of the appearances of the element 1 by the element 0, or one of the appearances of the element 1 by the element 2. Thence, analogously by the inductive hypothesis and by the statement proved above, we receive that the result of the application of h to the given collection is not equal modulo 3 to none of the numbers

$$(r_0 + 1) \cdot 0 + (r_1 - 1) \cdot 1 + r_2 \cdot 2, \quad r_0 \cdot 0 + (r_1 - 1) \cdot 1 + (r_2 + 1) \cdot 2,$$

which completes the proof. □

As a consequence of the above Lemma we obtain

Corollary 3. *The automorphism group of the quasigroup* $(Q; f)$ *with* $|Q| = 2$ *is double-transitive.*

A group $S(Q)$ is called *k-cotransitive*, where k is some fixed cardinal number, iff $|Q| \geq k$, and for every bijection $\varphi : Q \setminus A \to Q \setminus B$, where A and B are arbitrary k-subsets of Q, there exists $\alpha \in S(Q)$ such that $\alpha x = \varphi x$ for all $x \in Q \setminus A$.

It is clear that with $|Q| = n < \aleph_0$ such k-cotransitivity is equivalent to the $(n - k)$-times transitivity of this group.

Lemma 4. *Let* (Q, Ω) *be an algebra containing infinitary operations perhaps. If a subset* M *of* Q *is* k*-transitive with* $|M| + 1 \leq k$, $|Q \backslash M| \geq 2$, *or* k*-cotransitive with* $|Q \backslash M| \geq k + 1$, $|Q \backslash M| \geq 2$, *then* M *is a subalgebra of the given algebra.*

Proof. Since the case of the k-transitivity follows from the case of the k-cotransitivity, we prove only the case of the k-cotransitivity. If M is not a subalgebra, then there exist an operation σ of this algebra and the sequence

$$\langle x_i \,|\, i \in I \rangle \tag{2}$$

(the cardinal number of I and the arity of σ are equal), such that

$$(\forall i \in I)\, x_i \in M, \quad y = \sigma(\langle x_i \,|\, i \in I \rangle) \notin M. \tag{3}$$

But for $|Q \backslash M| \geq 2$ there exists $z \in Q \setminus M$ such that $z \neq y$. Moreover, the k-cotransitivity implies the existence of an automorphism φ of (Q, Ω) for which $\varphi y = z$ and $\varphi x_i = x_i$ for all $i \in I$. Thus

$$z = \varphi y = \varphi\sigma(\langle x_i \,|\, i \in I \rangle) = \sigma(\langle \varphi x_i \,|\, i \in I \rangle) = \sigma(\langle x_i \,|\, i \in I \rangle),$$

which is impossible. □

Corollary 5. *If the automorphism group of an algebra (Q, Ω) is k-transitive and the maximal power of the arities of the operations of the algebra exists and is equal to n, where $n + 1 \leq k$, $n + 1 < |Q|$, then each non-empty subset of the set Q is a subalgebra.*

Proof. If we assume the contrary, then we get the existence of an operation $\sigma \in \Omega$ and of a collection (2), for which the conditions (3) hold. But this contradicts to the existence of $M = \{x_i \,|\, i \in I\}$ concerning the operation σ, although such existence follows from the previous Lemma. □

Theorem 6. *The automorphism group of an unary quasigroup $(Q; f)$, where $|Q| > 2$, is double-transitive iff f is the identical permutation. In this case the automorphism group is $|Q|$-transitive.*

Proof. If the automorphism group is double-transitive, then f is the identical substitution, by Lemma 4. On the other hand, every substitution of Q commutes with the identical permutation, and in the consequence, it is an automorphism of the respective unary quasigroup. □

Theorem 7. *The automorphism group of the quasigroups* $(Q; f)$ *with* $|Q| = 3$ *is triple-transitive iff the quasigroup is idempotent.*

Proof. By Lemma 2, given quasigroup is a linear isotope of a cyclic group. Such triple-transitivity is equivalent to the isomorphism of the given automorphism group to the holomorph of the cyclic group. From results of [4] it follows that such isomorphism is equivalent to idempotency of the quasigroup $(Q; f)$. □

Lemma 8. *Non-one-element quasigroups, in which all one-element and two-element subsets are their subquasigroups, have odd arities and are described by the system of identities* $f(u_1, \ldots, u_n) = u_{n+1}$, *where metavariables* u_1, …, u_{n+1} *accept values in the set of the propositional variables* $\{x; y\}$, *and, besides* u_{n+1} *coincides with propositional variable* x *or* y, *appearing in the sequence* u_1, …, u_n *odd number of times.*

Proof. Indeed, let $\{a; b\}$ be fixed. At once we throw the case away when the arity of the quasigroup is equal to zero, because then the lemma conditions are false. The oddness of the operation arity follows by evident way from the assertion on the operation value, since an operation of an even arity may have each from the elements a and b odd number of times in the role of arguments. And we prove the assertion about the operation value by the induction on the number k of the appearances, for example, of the element b in the role. If $k = 0$, then the assertion follows from Lemma 4. Let with $k = i$ the assertion be true. We have to prove it for $k = i + 1$. By Lemma 4, the operation value on the given collection is equal to either a or b. It remains to take into account that we must get other value, if we replace one of the appearances of b on a, because f is a quasigroup operation.□

Theorem 9. *The automorphism group of a quasigroup* $(Q; f)$ *with* $|Q| = 4$ *is quadruple-transitive iff the arity of the operation is odd and the quasigroup is derived from the group* $Z_2 \times Z_2$.

Proof. Let the automorphism group be quadruple-transitive. We define on the set Q an operation $(+)$ being isomorphic to the operation of the group $Z_2 \times Z_2$. Using Lemmas 4 and 8 we get the oddness of the arity n of the quasigroup $(Q; f)$ and the truth of the formula

$$f(x_1, \ldots, x_n) = x_1 + \ldots + x_n \tag{4}$$

for the case, when $|\{x_1; \ldots; x_n\}| \leq 2$, since in the group $(Q; +)$ the identity $2x = 0$ holds.

We prove (4) for the other cases. We will do it by the induction on the value of the product

$$P = (a+1)(b+1)(c+1)(d+1),$$

where a, b, c and d are numbers of the appearances of each of four elements of Q in the collection of the arguments of the operation f in (4). Without restricting the generality we assume that

$$a \geq b \geq c \geq d,$$

whence we have $c > 0$ (with $c = 0$ the statement has just been proved above). Let $u, v, w \in Q$ correspond to the numbers a, b and c respectively. In the fixed collection of all arguments of the operation f we make three independent changes (in so doing, we receive three individual collections). First: we replace an arbitrary appearance of the element v with the element u. Second: we replace an arbitrary appearance of the element w with the element u. And third: we replace an arbitrary appearance of the element w with the element v. In this case the value of the product P is respectively replaced by the products

$$\begin{aligned} P_1 &= (a+2)b(c+1)(d+1), \\ P_2 &= (a+2)(b+1)c(d+1), \\ P_3 &= (a+1)(b+2)c(d+1), \end{aligned}$$

which are less than P. By the inductive hypothesis, values of f on three obtained collections are pairwise different and all of them must be different from the value on the given collection, because f is a quasigroup operation. But values of the right side of (4) on all these four collections are also pairwise different. Therefore, taking into account that $|Q| = 4$, we get the truth of the formula (4) on the given collection. The rest follows from the fact that the given automorphism group is isomorphic to $\mathrm{Hol}(Z_2 \times Z_2)$, and the holomorph consists of all substitutions of the basis set. $\square$

3. The general case

Lemma 10. *For all mappings α_1, ..., α_n of a group $(Q;+)$ and for the mappings β_1, ..., β_n defined by*

$$\beta_i = \alpha_1 + \ldots + \alpha_i, \qquad \textit{where} \quad i = 0, \ldots, n, \tag{5}$$

the equality of the subgroups

$$\begin{aligned} &\{\psi \in Aut(Q;+) \,|\, \psi\beta_i = \beta_i\psi, \;\; i = 1, \ldots, n\} = \\ &= \{\psi \in Aut(Q;+) \,|\, \psi\alpha_i = \alpha_i\psi, \;\; i = 1, \ldots, n\} \end{aligned}$$

of the group $Aut(Q;+)$ holds.

Proof. Let ψ commute with α_i when $i = 1, \ldots, n$. Then, for each i we have that

$$\begin{aligned} &\psi\beta_i = \psi(\alpha_1 + \ldots + \alpha_i) = \psi\alpha_1 + \ldots + \psi\alpha_i = \\ &= \alpha_1\psi + \ldots + \alpha_i\psi = (\alpha_1 + \ldots + \alpha_i)\psi = \beta_i\psi. \end{aligned}$$

Now on the contrary, let ψ commute with β_i when $i = 1, \ldots, n$. It is evident that ψ commutes with β_0 as well. Then, for all i, we have that

$$\begin{aligned} \psi\alpha_i \;&= -\psi\beta_{i-1} + \psi\beta_{i-1} + \psi\alpha_i = -\psi\beta_{i-1} + \psi(\beta_{i-1} + \alpha_i) \\ &= -\psi\beta_{i-1} + \psi\beta_i = -\beta_{i-1}\psi + \beta_i\psi = -\beta_{i-1}\psi + (\beta_{i-1} + \alpha_i)\psi \\ &= (-\beta_{i-1} + \beta_{i-1} + \alpha_i)\psi = \alpha_i\psi. \end{aligned}$$ □

We denote by L_c and R_c respectively the left and right translations of the group operation $(+)$, by I_c the inner automorphism $L_c^{-1}R_c$, and by ε the identical permutation.

For shortening of the statement wording we reach agreement about unified notations further in this point (except the end of the article). Namely: let us fix an arbitrary group, denoted as $(Q;+)$, its arbitrary element, denoted as a, an arbitrary integer greater than one, denoted as n, arbitrary n unitary substitutions, denoted as α_1, ..., α_n. Under these designations let us fix also the notation $(Q;f)$ for the group isotope specified by the equality

$$f(x_1, \ldots, x_n) = \alpha_1 x_1 + \ldots + \alpha_n x_n + a,$$

also the notation $\beta_0, \ldots, \beta_n$ for the mappings of the set Q specified by the equalities (5) (here, it is natural that β_0 is the null-endomorphism of the given group). Finally, let us fix the notation H for the subgroup of $\mathrm{Aut}(Q;+)$, consisting of all automorphisms, stated in Theorem 10, and the notation γ for the mapping, specified by the equality $\gamma = R_a\beta_n - \varepsilon$.

During the conference in Barnaul (1991) F. Sokhatsky announced the following result.

Theorem 11. *A transformation α is an endomorphism of a group isotope $(Q;f)$ iff $\alpha = R_c\theta$ for some endomorphism θ of the group $(Q;+)$ and some element c such that*

$$\theta a + c = \alpha_1 c + \ldots + \alpha_n c + a, \tag{6}$$

$$R_{\alpha_i c} I_{\alpha_1 c + \ldots + \alpha_{i-1} c}\theta\alpha_i = \alpha_i R_c\theta \qquad \textit{for all} \quad i = 1, \ldots, n. \tag{7}$$

Theorem 12. *A transformation α is an endomorphism of a group isotope $(Q;f)$ iff $\alpha = R_c\theta$ for some element c and for some endomorphism θ of the group $(Q;+)$ such that*

$$\theta a + c = \beta_n c + a, \tag{8}$$

$$R_{\beta_i c}\theta\beta_i = \beta_i R_c\theta \qquad \textit{for all} \quad i = 1, \ldots, n. \tag{9}$$

Proof. The equality (6) is equivalent to (8), therefore by Theorem 11 it is enough to show that (7) is equivalent to (9). Replace the number n by as arbitrary number k and let us prove the equivalence of the obtained systems for all natural k, not greater than n. Make that by the induction on k. For when $k = 1$ we have one equality in both systems only, which are equivalent, because $\beta_1 = \alpha_1$, $I_{\beta_0 c} = \varepsilon$. Assume that for $i = m$ these systems are equivalent. For $i = m+1$ the equality (9) may be rewritten in the form

$$R_{\alpha_{m+1}c} R_{\beta_m c}\theta(\beta_m + \alpha_{m+1}) = (\beta_m + \alpha_{m+1})R_c\theta. \tag{10}$$

Since (9) holds when $i = m$, then

$$(\beta_m + \alpha_{m+1})R_c\theta = \beta_m R_c\theta + \alpha_{m+1}R_c\theta = R_{\beta_m c}\theta\beta_m + \alpha_{m+1}R_c\theta,$$

and hence, (10) may be rewritten in the form

$$R_{\alpha_{m+1}c} R_{\beta_m c}\theta(\beta_m + \alpha_{m+1}) = R_{\beta_m c}\theta\beta_m + \alpha_{m+1}R_c\theta,$$

that is

$$\theta\beta_m + R_{\alpha_{m+1}c}R_{\beta_m c}\theta\alpha_{m+1} = \theta\beta_m + L_{\beta_m c}\alpha_{m+1}R_c\theta,$$

whence after equivalent transformations we have

$$R_{\alpha_{m+1}c}I_{\beta_m c}\theta\alpha_{m+1} = \alpha_{m+1}R_c\theta,$$

which is equivalent to (7) with $i = m+1$. This completes the proof.□

Theorem 13. *The automorphism group of a group isotope $(Q; f)$ is transitive iff for every element $c \in Q$ there exists an automorphism θ of the group $(Q; +)$ such that (9) holds and the element $\theta^{-1}\gamma c$ is the image of the element a under the action of some transformation from the group H.*

Proof. Let $\mathrm{Aut}(Q; f)$ be transitive. Then for every $c \in Q$ there exists an automorphism α of of the group isotope $(Q; f)$ which maps the neutral element of $(Q; +)$ to c. By Theorem 12 it means that for each $c \in Q$ there exists an automorphism θ of $(Q; +)$ satisfying (8) and (9). From (8) we have that $\theta^{-1}\gamma c = a$, but the identical automorphism of $(Q; +)$ maps a to itself and commutes with all β_i.

On the other hand, let for every $c \in Q$ there exist an automorphism θ of $(Q; +)$ satisfying (9), and thereto for these c and θ, the element $\theta^{-1}\gamma c$ is the image of a under the action of some automorphism ψ from H. Then for these triples of c, θ and ψ we have

$$\begin{aligned} \theta\psi a + c &= \theta\theta^{-1}(\beta_n c + a - c) + c = \beta_n c + a, \\ R_{\beta_i c}\theta\psi\beta_i &= R_{\beta_i c}\theta\beta_i\psi = \beta_i R_c\theta\psi \qquad \text{for all} \quad i = 1, \dots, n, \end{aligned} \tag{11}$$

whence taking into account bijectivity of the transformations of $R_c\theta\psi$ we have, by Theorem 12, that they are automorphisms of the group isotope $(Q; f)$. Consequently, for an arbitrary fixed $x, y \in Q$ there are automorphisms θ', ψ', θ'' and ψ'' such that $R_x\theta'\psi'$ and $R_y\theta''\psi''$ are automorphisms of the group isotope $(Q; f)$. But

$$\begin{aligned} R_y\theta''\psi''(R_x\theta'\psi')^{-1}x &= R_y\theta''\psi''(\psi')^{-1}(\theta')^{-1}R_x^{-1}x \\ &= R_y\theta''\psi''(\psi')^{-1}(\theta')^{-1}0 = R_y 0 = y, \end{aligned}$$

whence $\mathrm{Aut}(Q;f)$ is transitive. □

Corollary 14. *If transformations $\beta_1, \ldots, \beta_n$ are endomorphisms (for example, if the group $(Q;+)$ is abelian and its isotope $(Q;f)$ is linear) of a group $(Q;+)$ then the automorphism group of a group isotope $(Q;f)$ is transitive iff one of the following equivalent conditions holds:*

- *the set $\mathrm{Im}\,\gamma$ is a subset of the set of images of a under the action of all transformations of the group H;*
- *for all $x, y \in \mathrm{Im}\,\gamma$ there exists a transformation φ from the group H which maps x to y.*

Proof. If $\beta_1, \ldots, \beta_n$ are endomorphisms of $(Q;+)$, then (9) means that θ belongs to H. Since all groups are non-empty, then by Theorem 13, $\mathrm{Aut}(Q;f)$ is transitive iff for each $c \in Q$ there are transformations θ and ψ from H such that $\psi a = \theta^{-1}\gamma c$, i.e.

$$\delta a = \gamma c, \tag{12}$$

where $\delta = \theta\psi$. Hence, $\mathrm{Aut}(Q;f)$ is transitive iff for every $c \in Q$ there exists a transformation δ from H such that (12) holds, i.e, iff $\mathrm{Im}\gamma$ is a subset of the set of all images of a under the action of all transformations from H. We prove the equivalence of the two conditions of our corollary criterion. Let $\mathrm{Im}\,\gamma$ be a subset of the set of all images of a under the action of all transformations from the group H. Then for all $x, y \in \mathrm{Im}\gamma$ there exist transformations φ_1 and φ_2 from H such that $\varphi_1 a = x, \quad \varphi_2 a = y$. Thus $\varphi_2\varphi_1^{-1}x = y$. Hence, the second condition follows from the first one. Let now the second condition holds. Since γ maps the neutral element of $(Q;+)$ to a, then a belongs to $\mathrm{Im}\,\gamma$. Hence, for every $y \in \mathrm{Im}\,\gamma$ there exists $\varphi \in H$, for which $\varphi x = y$. And this is the first of the two conditions of the corollary criterion. □

Corollary 15. *If transformations $\beta_1, \ldots, \beta_n$ are endomorphisms of a group $(Q;+)$ and the group H is transitive on the set $\mathrm{Im}\,\gamma$, then the automorphism group of a group isotope $(Q;f)$ is transitive.* □

Corollary 16. *If $\beta_n = \varepsilon$, transformations $\beta_1, \ldots, \beta_{n-1}$ are endomorphisms of a group $(Q;+)$, and a is central in this group, then the automorphism group of the group isotope $(Q;f)$ is transitive.*

Proof. $\operatorname{Im}\gamma$ has only one element, which under the action of the transformation ε is mapped to itself. Hence, by Corollary 14, the group $\operatorname{Aut}(Q;f)$ is transitive. □

Corollary 17. *The automorphism group of an idempotent group isotope $(Q;f)$, where $\beta_1, \ldots, \beta_n$ are endomorphisms of the group $(Q;+)$, is transitive.* □

Corollary 18. *The automorphism group of an idempotent group isotope $(Q;f)$ is transitive iff for every element $c \in Q$ there exists an automorphism θ of the group $(Q;+)$ such that* (9) *holds.*

Proof. Idempotency of the isotope $(Q;f)$ gives $\beta_n = \varepsilon$ and $a = 0$. Therefore $\operatorname{Im}\gamma$ contains only the neutral element of $(Q;+)$. Since the identical transformation commutes with all mappings, then Theorem 13 completes our proof. □

Example. Let $(Q;+)$ be a cyclic group Z_6, and

$$n = 3, \quad a = 0, \quad \alpha_1 = \varepsilon,$$

$$\alpha_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 4 & 5 & 2 & 3 \end{pmatrix}, \quad \alpha_3 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 5 & 2 & 1 & 4 & 3 \end{pmatrix}.$$

Then the group isotope $(Q;f)$ is idempotent. The map:

$$\beta_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 2 & 0 & 2 & 0 & 2 \end{pmatrix},$$

is not an endomorphism of the group $(Q:+)$ because

$$\beta_2(1+1) = \beta_2 2 = 0 \neq 4 = 2 + 2 = \beta_2 1 + \beta_2 1.$$

But the group $\operatorname{Aut}(Q;+)$ is transitive. Indeed, by Corollary 18, for verifying of transitivity of this group it is enough to show that for every $c \in Q$ there exists an automorphism θ of $(Q;+)$ satisfying (9). In the group Z_6 there are two automorphisms: ε and $-\varepsilon$. When $i=1$ and when $i=3$, both of them satisfy (9). For $i=2$ (9) has the form

$$(\forall x \in Q) \quad \theta\beta_2 x + \beta_2 c = \beta_2(\theta x + c).$$

If $c \in \{0;2;4\}$, then $\theta = \varepsilon$ and:

$$\beta_2(\theta x + c) = \beta_2(x+c) = \beta_2 x = \beta_2 x + \beta_2 c = \theta\beta_2 x + \beta_2 c.$$

If $c \in \{1;3;5\}$, then $\theta = -\varepsilon$ and:

$$\begin{aligned}\beta_2(\theta x + c) &= \beta_2(-x+c) = \beta_2(x+c) = 2 - \beta_2 x\\ &= \beta_2 c - \beta_2 x = -\beta_2 x + \beta_2 c = \theta\beta_2 x + \beta_2 c.\end{aligned}$$

This proves that $\mathrm{Aut}(Q;f)$ is transitive. $\square$

Theorem 19. *A transitive automorphism group of a group isotope $(Q;f)$ with $|Q|>2$ is double-transitive iff $(Q;f)$ is idempotent, the group H is transitive on the set of all non-neutral elements of the group $(Q;+)$.*

Proof. While proving Lemma 4 in the both directions, we can consider that $(Q;f)$ is idempotent. Then, by Corollary 18, for every $c \in Q$ there exists an automorphism θ of $(Q;+)$ satisfying (9). Since $\beta_n = \varepsilon$, and $a=0$ (because $(Q;f)$ is idempotent), then for every c and for every automorphism θ of $(Q;+)$ (8) holds. Hence, by Theorem 12 the mapping α is an automorphism of the group isotope $(Q;f)$ iff $\alpha = R_c\theta$ for some c and some automorphism θ of $(Q;+)$ satisfying (9). Let $\mathrm{Aut}(Q;f)$ be double-transitive, then for all non-neutral $x,y \in Q$ there exist c and an automorphism θ of $(Q;+)$ such that (9) holds and also

$$R_c\theta 0 = 0, \quad R_c\theta x = y.$$

From the first of these equalities we obtain that $c=0$, and hence, $\theta x = y$. From (9) follows that θ belongs to the group H. It is also obvious that θ maps all non-neutral elements of $(Q;+)$ to non-neutral, and in the consequence, the group H is transitive on $Q\backslash\{0\}$. Let now $x,y,c \in Q$ and $x \neq 0$, $y \neq c$. By the above, there exists an automorphism θ of $(Q;+)$ satisfying (9). Since the group H is transitive on $Q\backslash\{0\}$, then there exists $\psi \in H$, for which $\psi x = \theta^{-1}(y-c)$. Then we have (11) and $\alpha 0 = c$, $\alpha x = y$, where the mapping $\alpha = R_c\theta\psi$ is an automorphism of the group isotope $(Q; f)$. If now we take arbitrary different elements $z, t \in Q$, then, analogously as in previous case, we obtain the existence of an automorphism β of the group isotope $(Q; f)$, for which $\beta 0 = z$, $\beta x = t$. Then for the automorphism $\beta\alpha^{-1}$ of the group isotope $(Q; f)$ we have

$$\beta\alpha^{-1}c = \beta 0 = z, \quad \beta\alpha^{-1}y = \beta x = t.$$

Hence, the group $\mathrm{Aut}(Q; f)$ is double-transitive. □

Theorem 20. *The automorphism group of a group isotope $(Q; f)$, where $|Q| > 3$, is triple-transitive iff n is odd, $(Q; f)$ is derived from $(Q; +)$ and $(Q; +)$ is an abelian group of period 2 whose automorphism group is double-transitive on the set of all non-neutral elements of the group $(Q; +)$.*

Proof. Assume that $\mathrm{Aut}(Q; +)$ is triple-transitive. By Lemmas 4 and 8 the number n is odd, the group isotope is idempotent, and

$$f(\underbrace{0, \ldots, 0,}_{(i-1)-times} x, 0, \ldots, 0) = x \qquad \text{for all} \quad i = 1, \ldots, n,$$

$$f(x, x, 0, \ldots, 0) = 0.$$

Thus $\alpha_i = \varepsilon$ and $2x = 0$, because from idepotency of $(Q; f)$ we have that $a = 0$. This means that $(Q; +)$ is abelian. Then by Theorem 12 all automorphisms of the group isotope $(Q; f)$ are transformations of the form $R_c\theta$, where $c \in Q$, and θ is an automorphism of $(Q; +)$. If the automorphism group of the group isotope $(Q; f)$ is triple-transitive, then for $x_1, x_2, y_1, y_2 \in Q$ such that $|\{0; x_1; x_2\}| = |\{0; y_1; y_2\}| = 3$ there exist c and an automorphism θ of $(Q; +)$, for which

$$R_c\theta 0 = 0, \quad R_c\theta x_1 = y_1, \quad R_c\theta x_2 = y_2.$$

From the first equality we obtain $c = 0$, and hence, $\theta x_1 = y_1$, $\theta x_2 = y_2$, which means that $\mathrm{Aut}(Q; +)$ is double-transitive on $Q \backslash \{0\}$. A contrary, let $\mathrm{Aut}(Q; +)$ be double-transitive on $Q \backslash \{0\}$, and x_1, x_2, x_3, y_1, y_2, $y_3 \in Q$ be such that $|\{x_1; x_2; x_3\}| = |\{y_1; y_2; y_3\}| = 3$. Then there exists an automorphism θ of $(Q; +)$, for which

$$\theta(x_2 - x_1) = y_2 - y_1, \quad \theta(x_3 - x_1) = y_3 - y_1.$$

This for $c = y_1 - \theta x_1$ gives the automorphism $R_c\theta$ of group isotope $(Q; f)$ such that

$$\begin{aligned} R_c\theta x_1 &= \theta x_1 + (y_1 - \theta x_1) = y_1, \\ R_c\theta x_2 &= \theta(x_2 - x_1) + R_c\theta x_1 = (y_2 - y_1) + y_1 = y_2, \\ R_c\theta x_3 &= \theta(x_3 - x_1) + R_c\theta x_1 = (y_3 - y_1) + y_1 = y_3. \end{aligned}$$

This proves that the group $\mathrm{Aut}(Q; +)$ is triple-transitive. □

Theorem 21. *The automorphism group of a non-unary quasigroup* $(Q; f)$ *with* $|Q| > 4$ *is not quadruple-transitive.*

Proof. If it is not quadruple-transitive, then by Lemmas 4 and 8, for arbitrary $a, b, c \in Q$ we have

$$\begin{aligned} f(a, c, \ldots, c) &= a, \\ f(a, a, c, \ldots, c) &= c, \\ f(c, b, c, c, \ldots, c) &= b. \end{aligned}$$

Thus $f(a, b, c, \ldots, c) \notin \{a; b; c\}$, which is impossible by Lemma 4. □

Note. It is easy to see that every automorphism of an operation f is an automorphism of an arbitrary diagonal operation induced by f, i.e. the operation of the arity k defined by the term $f(x_{\gamma_1}, \ldots, x_{\gamma_n})$, where γ is a permutation of {1,…,n} on the set consisting of k indexes. Whence, the k-transitivity of the automorphism group of $(G; f)$ implies the k-transitivity of the automorphism group of each diagonal operation induced by f.

References

[1] **M. Hall**: *The group theory*, Moscou 1962.

[2] **A. P. Il'inykh**: *The classification of the finite groupoids with a 2-transitive automorphism group*, (Russian) Mat. Sbornik **185** (1994), 51 − 78.

[3] **A. V. Kuznetsov, E. A. Kuznetsov**: *On the twice-generated double-homogeneous quasigroups*, (Russian), Mat. Issliedov. **71** (1983), 34 – 53.

[4] **F. Sokhatskyj, P. Syvakivskyj**: *On linear isotopes of cyclic groups*, Quasigroups and Related Systems **1** (1994), 66 – 76.

Department of Algebra
Vinnytsia State Pedagogical University
Vinnytsia 287100
Ukraine

Received 15 September 1997

Quasigroups and Related Systems, **4** (1997), 67–76

n-groups as n-groupoids with laws

Janez Ušan

Abstract

In this article n-group (Q,A) is described as an n-groupoid (Q,B) in which the following two laws hold: $B(B(x,z,b_1^{n-2}),B(y,a_1^{n-2},z),a_1^{n-2}) = B(x,y,b_1^{n-2})$ and $B(a,c_1^{n-2},B(B(B(z,c_1^{n-2},z),c_1^{n-2},b),c_1^{n-2},B(B(z,c_1^{n-2},z),c_1^{n-2},a))) = b$.

1. Preliminaries

1.1. Definition. Let $n \geq 2$ and let (Q,A) be an n–groupoid. We say that (Q,A) is a *Dörnte n–group* (briefly: *n–group*) iff it is an n–semigroup and an n–quasigroup as well.

1.2. Proposition. ([17]) *Let $n \geq 2$ and let (Q,A) be an n–groupoid. Then the following statements are equivalent:*

(i) (Q,A) *is an n-group,*

(ii) *there are mappings* $^{-1}$ *and* $\mathbf{e}$ *respectively of the sets Q^{n-1} and Q^{n-2} into the set Q such that the following laws hold in the algebra $(Q,\{A,{}^{-1},\mathbf{e}\})$ (of the type $\langle n,n-1,n-2\rangle$)*

(a) $A(x_1^{n-2},A(x_{n-1}^{2n-2}),x_{2n-1}) = A(x_1^{n-1},A(x_n^{2n-1}))\,,$

(b) $A(\mathbf{e}(a_1^{n-2}),a_1^{n-2},x) = x\,,$

(c) $A((a_1^{n-2},a)^{-1},a_1^{n-2},a) = \mathbf{e}(a_1^{n-2})\,,$

1991 Mathematics Subject Classification: 20N15, 03B30
Keywords: $n-$groupoid, $n-$semigroup, $n-$group, $\{i,j\}-$neutral operation

(iii) *there are mappings* $^{-1}$ *and* $\mathbf{e}$ *respectively of the sets* Q^{n-1} *and* Q^{n-2} *into the set* Q *such that the following laws hold in the algebra* $(Q, \{A, {}^{-1}, \mathbf{e}\})$ *(of the type* $\langle n, n-1, n-2\rangle$*)*

$(\bar{a})$ $A(A(x_1^n), x_{n+1}^{2n-1}) = A(x_1, A(x_2^{n+1}), x_{n+2}^{2n-1})$,

$(\bar{b})$ $A(x, a_1^{n-2}, \mathbf{e}(a_1^{n-2})) = x$,

$(\bar{c})$ $A(a, a_1^{n-2}, (a_1^{n-2}, a)^{-1}) = \mathbf{e}(a_1^{n-2})$.

1.3. Remarks. $\mathbf{e}$ is an $\{1, n\}$–neutral operation of n–groupoid (Q, A) iff algebra $(Q, \{A, \mathbf{e}\})$ of type $\langle n, n-2\rangle$ satisfies the laws (b) and $(\bar{b})$ from 1.2 (cf. [14]). The notion of $\{i, j\}$–neutral operation $(i, j \in \{1, ..., n\},\ i < j)$ of an n–groupoid is defined in a similar way (cf. [14]). Every n–groupoid has at most one $\{i, j\}$–neutral operation. In every n–group $(n \geq 2)$ there is an $\{1, n\}$–neutral operation (cf. [14]). There are n–groups without $\{i, j\}$–neutral operation with $\{i, j\} \neq \{1, n\}$. In [16], n–groups with $\{i, j\}$–neutral operations, for $\{i, j\} \neq \{1, n\}$ are described. Operation $^{-1}$ from 1.2 is a generalization of the inverse operation in a group. In fact, if (Q, A) is an n–group, $n \geq 2$, then for every $a \in Q$ and for every sequence a_1^{n-2} over Q is

$$(a_1^{n-2}, a)^{-1} = \mathsf{E}(a_1^{n-2}, a, a_1^{n-2}),$$

where E is an $\{1, 2n-1\}$–neutral operation of the $(2n-1)$-group $(Q, \overset{2}{A})$, $\overset{2}{A}(x_1^{2n-1}) = A(A(x_1^n), x_{n+1}^{2n-1})$ (cf. [15]). (For $n = 2$, $a^{-1} = \mathsf{E}(a)$, a^{-1} is the inverse element of the element a with respect to the neutral element $\mathbf{e}(\emptyset)$ of the group (Q, A).)

1.4. Proposition. ([18]) *Let* $n \geq 2$ *and let* (Q, A) *be an* n*-groupoid. Then,* (Q, A) *is an* n*-group iff the following statements hold:*

(1) $(\forall x_i \in Q)_1^{2n-1} A(A(x_1^n), x_{n+1}^{2n-1}) = A(x_1^{n-1}, A(x_n^{2n-1}))$,

(2) $(\forall x_i \in Q)_1^{2n-1} A(x_1^{n-2}, A(x_{n-1}^{2n-2}), x_{2n-1}) = A(x_1^{n-1}, A(x_n^{2n-1}))$ *or*
$(\forall x_i \in Q)_1^{2n-1} A(A(x_1^n), x_{n+1}^{2n-1}) = A(x_1, A(x_2^{n+1}), x_{n+2}^{2n-1})$,

(3) *for every* $a_1^n \in Q$ *there is at least one* $x \in Q$ *and at least one* $y \in Q$ *such that* $A(a_1^{n-1}, x) = a_n$ *and* $A(y, a_1^{n-1}) = a_n$.

Note that the following proposition has been proved in [13]:
An n–semigroup (Q,A) is an n–group iff for each $a_1^n \in Q$ there exists at least one $x \in Q$ and at least one $y \in Q$ such that the following equalities hold: $A(a_1^{n-1},x) = a_n$ and $A(y,a_1^{n-1}) = a_n$.

This assertion has been already formulated in [11], but the proof is missing there. W.A. Dudek has pointed my attention to this fact. Similar issues have been considered in [5] (Proposition 1).

1.5. Proposition. *Let $n \geq 3$ and let (Q,A) be an n-groupoid. Also let:*

(i) the $\langle 1,2\rangle$–associative law holds in (Q,A),

(ii) for every $x,y,a_1^{n-1} \in Q$ the following implication holds

$$A(x,a_1^{n-1}) = A(y,a_1^{n-1}) \Rightarrow x = y.$$

Then (Q,A) is an n-semigroup.

Proposition 1.5 is a part of proposition 3.5 from [17]. In the proof of this proposition we use the method of E. I. Sokolov from [11].

1.6. Proposition. *Let (Q,A) be an n–group, ${}^{-1}$ its inverse operation, $\mathbf{e}$ its $\{1,n\}$–neutral operation and $n \geq 2$. Also let*

$${}^{-1}\!A(x,a_1^{n-2},y) = z \overset{def}{\Longleftrightarrow} A(z,a_1^{n-2},y) = x$$

for all $x,y,z \in Q$ and for every sequence a_1^{n-2} over Q. Then, for all $x,y \in Q$ and for every sequence a_1^{n-2} over Q the following equalities hold:

$(\bar{1})$ ${}^{-1}\!A(x,a_1^{n-2},y) = A(x,a_1^{n-2},(a_1^{n-2},y)^{-1})$,

$(\bar{2})$ $\mathbf{e}(a_1^{n-2}) = {}^{-1}\!A(x,a_1^{n-2},x)$,

$(\bar{3})$ $(a_1^{n-2},x)^{-1} = {}^{-1}\!A({}^{-1}\!A(x,a_1^{n-2},x),a_1^{n-2},x)$,

$(\bar{4})$ $A(x,a_1^{n-2},y) = {}^{-1}\!A(x,a_1^{n-2},{}^{-1}\!A({}^{-1}\!A(y,a_1^{n-2},y),a_1^{n-2},y))$.

Sketch of the proof.

a) $^{-1}A(x, a_1^{n-2}, y) = z \Longleftrightarrow A(z, a_1^{n-2}, y) = x \Longleftrightarrow$

$A(A(z, a_1^{n-2}, y), a_1^{n-2}, (a_1^{n-2}, y)^{-1}) = A(x, a_1^{n-2}, (a_1^{n-2}, y)^{-1}) \Longleftrightarrow$

$A(z, a_1^{n-2}, A(y, a_1^{n-2}, (a_1^{n-2}, y)^{-1})) = A(x, a_1^{n-2}, (a_1^{n-2}, y)^{-1}) \Longleftrightarrow$

$A(z, a_1^{n-2}, \mathbf{e}(a_1^{n-2})) = A(x, a_1^{n-2}, (a_1^{n-2}, y)^{-1}) \Longleftrightarrow$

$z = A(x, a_1^{n-2}, (a_1^{n-2}, y)^{-1})$.

b) $^{-1}A(x, a_1^{n-2}, x) = \mathbf{e}(a_1^{n-2}) \Longleftrightarrow A(\mathbf{e}(a_1^{n-2}), a_1^{n-2}, x) = x$.

c) $^{-1}A(^{-1}A(x, a_1^{n-2}, x), a_1^{n-2}, x) = (a_1^{n-2}, x)^{-1} \Longleftrightarrow$

$A((a_1^{n-2}, x)^{-1}, a_1^{n-2}, x) = {}^{-1}A(x, a_1^{n-2}, x) \Longleftrightarrow$

$A((a_1^{n-2}, x)^{-1}, a_1^{n-2}, x) = \mathbf{e}(a_1^{n-2})$.

d) $A(x, a_1^{n-2}, y) = {}^{-1}A(x, a_1^{n-2}, {}^{-1}A(^{-1}A(y, a_1^{n-2}, y), a_1^{n-2}, y)) \Longleftrightarrow$

$x = A(A(x, a_1^{n-2}, y), a_1^{n-2}, (a_1^{n-2}, y)^{-1}) \Longleftrightarrow$

$x = A(x, a_1^{n-2}, A(y, a_1^{n-2}, (a_1^{n-2}, y)^{-1})) \Longleftrightarrow$

$x = A(x, a_1^{n-2}, \mathbf{e}(a_1^{n-2}))$. □

2. Results

2.1. Theorem. *Let $n \geq 2$ and let (Q, A) be an n–group. Furthermore, let $B = {}^{-1}A$, where*

$$^{-1}A(x, z_1^{n-2}, y) = z \Longleftrightarrow A(z, z_1^{n-2}, y) = x$$

for all $x, y, z \in Q$ and for every sequence z_1^{n-2} over Q. Then the following laws

(i) $B(B(x, z, b_1^{n-2}),\ B(y, a_1^{n-2}, z), a_1^{n-2}) = B(x, y, b_1^{n-2})$,

(ii)

$$B(a, c_1^{n-2}, B(B(B(z, c_1^{n-2}, z), c_1^{n-2}, b), c_1^{n-2}, B(B(z, c_1^{n-2}, z), c_1^{n-2}, a))) = b$$

hold in the n–groupoid (Q, B). Moreover, for all $x, y \in Q$ and for every sequence a_1^{n-2} over Q the following equality holds

$$B(x, a_1^{n-2}, y) = A(x, a_1^{n-2}, (a_1^{n-2}, y)^{-1}),$$

where $^{-1}$ *is an inverse operation of the* n*–group* (Q, A).

Proof. Let $n \geq 2$ and let (Q, A) be an n–group, $^{-1}$ its inverse operation and $\mathbf{e}$ its $\{1, n\}$–neutral operation. Also let

$$(0) \qquad {}^{-1}A(x, z_1^{n-2}, y) = z \overset{def}{\Longleftrightarrow} A(z, z_1^{n-2}, y) = x$$

for all $x, y, z \in Q$ and for every sequence z_1^{n-2} over Q.

1) By 1.1 and (0), we conclude that for all $x, y, z, u, v \in Q$, for every sequence a_1^{n-2} over Q and for every sequence b_1^{n-2} over Q the following series of implications holds

$$\begin{aligned}
&A(A(x, y, a_1^{n-2}), z, b_1^{n-2}) = A(x, A(y, a_1^{n-2}, z), b_1^{n-2}) \Longrightarrow\\
&{}^{-1}A(A(x, A(y, a_1^{n-2}, z), b_1^{n-2}), z, b_1^{n-2}) = A(x, y, a_1^{n-2}) \Longrightarrow\\
&{}^{-1}A(A(x, u, b_1^{n-2}), z, b_1^{n-2}) = A(x, {}^{-1}A(u, a_1^{n-2}, z), a_1^{n-2}) \Longrightarrow\\
&{}^{-1}A(v, z, b_1^{n-2}) = A({}^{-1}A(v, u, b_1^{n-2}), {}^{-1}A(u, a_1^{n-2}, z), a_1^{n-2}) \Longrightarrow\\
&{}^{-1}A(v, u, b_1^{n-2}) = {}^{-1}A({}^{-1}A(v, z, b_1^{n-2}), {}^{-1}A(u, a_1^{n-2}, z), a_1^{n-2}).
\end{aligned}$$

But

$$\begin{aligned}
A(y, a_1^{n-2}, z) = u \Longleftrightarrow y = {}^{-1}A(u, a_1^{n-2}, z), A(x, u, b_1^{n-2}) = v \Longleftrightarrow\\
\Longleftrightarrow x = {}^{-1}A(v, u, b_1^{n-2}).
\end{aligned}$$

Whence, by the substitution $B = {}^{-1}A$, we conclude that

$$B(B(x, z, b_1^{n-2}), B(y, a_1^{n-2}, z), a_1^{n-2}) = B(x, y, b_1^{n-2})$$

holds in the n–groupoid (Q, B).

2) By 1.1, 1.2, 1.3 and (0), we conclude that for all $a, b, x \in Q$ and for every sequence c_1^{n-2} over Q the following series of equivalences holds

$$\begin{aligned}
&{}^{-1}A(a, c_1^{n-2}, x) = b \Longleftrightarrow A(b, c_1^{n-2}, x) = a \Longleftrightarrow\\
&A((c_1^{n-2}, b)^{-1}, c_1^{n-2}, A(b, c_1^{n-2}, x)) = A((c_1^{n-2}, b)^{-1}, c_1^{n-2}, a) \Longleftrightarrow\\
&x = A((c_1^{n-2}, b)^{-1}, c_1^{n-2}, a) \Longleftrightarrow\\
&A(x, c_1^{n-2}, (c_1^{n-2}, a)^{-1}) = A(A((c_1^{n-2}, b)^{-1}, c_1^{n-2}, a), c_1^{n-2}, (c_1^{n-2}, a)^{-1}) \Longleftrightarrow\\
&A(x, c_1^{n-2}, (c_1^{n-2}, a)^{-1}) = (c_1^{n-2}, b)^{-1} \Longleftrightarrow\\
&{}^{-1}A((c_1^{n-2}, b)^{-1}, c_1^{n-2}, (c_1^{n-2}, a)^{-1}) = x \Longleftrightarrow\\
&{}^{-1}A({}^{-1}A({}^{-1}A(z, c_1^{n-2}, z), c_1^{n-2}, b), c_1^{n-2}, {}^{-1}A({}^{-1}A(z, c_1^{n-2}, z), c_1^{n-2}, a)) = x.
\end{aligned}$$

But

$(c_1^{n-2},c)^{-1} = {}^{-1}\!A(\mathbf{e}(c_1^{n-2}),c_1^{n-2},c) \Longleftrightarrow \mathbf{e}(c_1^{n-2}) = A((c_1^{n-2},c)^{-1},c_1^{n-2},c)$

and

$$\mathbf{e}(c_1^{n-2}) = {}^{-1}\!A(z,c_1^{n-2},z) \Longleftrightarrow z = A(\mathbf{e}(c_1^{n-2}),c_1^{n-2},z)\,.$$

Whence, by the substitution $B = {}^{-1}\!A$, we conclude that (ii) holds in the n–groupoid (Q,B).

3) By the substitution $B = {}^{-1}\!A$ and by Proposition 1.6, we conclude that for all $x,y\in Q$ and for every sequence a_1^{n-2} over Q the following equality holds

$$B(x,a_1^{n-2},y) = A(x,a_1^{n-2},(a_1^{n-2},y)^{-1})\,. \qquad \square$$

2.2. Theorem. *Let $n\geq 2$ and let (Q,B) be an n–groupoid in which the laws (i) and (ii) from the previous theorem holds. Then, there is an n-group (Q,A) such that ${}^{-1}\!A = B$. Moreover, for all $x,y\in Q$ and for every sequence a_1^{n-2} over Q the following equalities hold*

$$\begin{aligned}
&\mathbf{e}(a_1^{n-2}) = B(x,a_1^{n-2},x)\,,\\
&(a_1^{n-2},x)^{-1} = B(B(x,a_1^{n-2},x),a_1^{n-2},x)\,,\\
&A(x,a_1^{n-2},y) = B(x,a_1^{n-2},B(B(y,a_1^{n-2},y),a_1^{n-2},y))\,,
\end{aligned}$$

where ${}^{-1}$ is an inverse operation, and $\mathbf{e}$ is an $\{1,n\}$–neutral operation of the n–group (Q,A).

Proof. By (ii), we conclude that the following statement holds:

1^o For every $a_1^n\in Q$ there is at least one $x\in Q$ such that
$$B(a_1^{n-1},x) = a_n\,.$$

Furthermore, the following statements hold:

2^o $(\forall a\in Q)\,(\forall z\in Q)\,(\forall c_i\in Q)_1^{n-2}\quad B(a,B(z,c_1^{n-2},z),c_1^{n-2}) = a\,.$

3^o For every $a_1^n\in Q$ there is exactly one $y\in Q$ such that
$$B(y,a_1^{n-1}) = a_n\,.$$

4^o There exists n–ary operation ${}^{-1}\!B$ in Q such that for all $x,y\in Q$ and for every sequence a_1^{n-1} over Q

$(\bar{o})$ $$ {}^{-1}B(x, a_1^{n-1}) = y \Longleftrightarrow B(y, a_1^{n-1}) = x\,. $$

5^o For every $a_1^n \in Q$ there is exactly one $y \in Q$ such that
$$ {}^{-1}B(y, a_1^{n-1}) = a_n\,. $$

6^o For every $a_1^n \in Q$ there is at least one $x \in Q$ such that
$$ {}^{-1}B(a_1^{n-1}, x) = a_n\,. $$

7^o The $\langle 1,2\rangle$–associative law holds in $(Q,\ {}^{-1}B)$.

8^o $(Q,\ {}^{-1}B)$ is an n–semigroup.

Sketch of the proof of 2^o.

a) $n \geq 3$. Putting $z = y$ in (i) we obtain
$$ B(B(x, y, b_1^{n-2}), B(y, a_1^{n-2}, y), a_1^{n-2}) = B(x, y, b_1^{n-2}) $$
which together with 1^o gives
$$ (\forall x, y \in Q)\,(\forall b_i \in Q)_1^{n-3}\ (\forall a \in Q)\ (\exists b_{n-2} \in Q)\ \ B(x, y, b_1^{n-2}) = a\,. $$

b) $n = 2$. As in the previous case from (i) we obtain
$$ B(B(x,y), B(y,y)) = B(x,y)\,, $$
which for $B(x,y) = a$ (by 1^o) proves that
$$ (\forall x \in Q)\,(\forall a \in Q)\,(\exists y \in Q)\ \ B(a, B(y,y)) = a\,, $$
$$ (\forall y \in Q)\,(\forall u \in Q)\,(\exists c \in Q)\ \ y = B(u,c)\,, $$
$$ B(y,y) = B(B(u,c), B(u,c)) = B(u,u)\,, $$
which completes the proof of 2^o.

Sketch of the proof of 3^o and 4^o.

a) $B(x, a, b_1^{n-2}) = B(y, a, b_1^{n-2}) \implies$
$$ B(B(x,a,b_1^{n-2}), B(u, a_1^{n-2}, a), a_1^{n-2}) = B(B(y,a,b_1^{n-2}), B(u, a_1^{n-2}, a), a_1^{n-2}) $$
$$ \implies B(x, u, b_1^{n-2}) = B(y, u, b_1^{n-2})\,. $$
Now, putting $u = A(v, b_1^{n-2}, v)$ and using 2^o, we obtain
$$ B(x, B(v, b_1^{n-2}, v), b_1^{n-2}) = B(y, B(v, b_1^{n-2}, v), b_1^{n-2}) \implies x = y. $$

b) $B(x, a, b_1^{n-2}) = c \Longleftrightarrow$

$$B(B(x, a, b_1^{n-2}), B(u, a_1^{n-2}, a), a_1^{n-2}) = B(c, B(u, a_1^{n-2}, a), a_1^{n-2}) \Longleftrightarrow$$
$$B(x, u, b_1^{n-2}) = B(c, B(u, a_1^{n-2}, a), a_1^{n-2})$$

by (i). Putting $u = A(v, b_1^{n-2}, v)$ we obtain

$$B(x, B(v, b_1^{n-2}, v), b_1^{n-2}) = B(c, B(B(v, b_1^{n-2}, v), a_1^{n-2}, a), a_1^{n-2}),$$

which (by 2^o) is equivalent to

$$x = B(c, B(B(v, b_1^{n-2}, v), a_1^{n-2}, a), a_1^{n-2}).$$

Sketch of the proof of 5^o.

$${}^{-1}B(x, c_1^{n-1}) = u \Longleftrightarrow B(u, c_1^{n-1}) = x,$$
$${}^{-1}B(y, c_1^{n-1}) = v \Longleftrightarrow B(v, c_1^{n-1}) = y.$$

Thus

$$x = y \Longrightarrow u = v \text{ and } u = v \Rightarrow x = y.$$

Sketch of the proof of 6^o.

$${}^{-1}B(a, a_1^{n-2}, x) = b \Longleftrightarrow B(b, a_1^{n-2}, x) = a.$$

Sketch of the proof of 7^o.

$$B(v, u, b_1^{n-2}) = B(B(v, z, b_1^{n-2}), B(u, a_1^{n-2}, z), a_1^{n-2}) \Longrightarrow$$
$$B(v, z, b_1^{n-2}) = {}^{-1}B(B(v, u, b_1^{n-2}), B(u, a_1^{n-2}, z), a_1^{n-2}) \Longrightarrow$$
$$B({}^{-1}B(x, u, b_1^{n-2}), z, b_1^{n-2}) = {}^{-1}B(x, B(u, a_1^{n-2}, z)a_1^{n-2}) \Longrightarrow$$
$$B({}^{-1}B(x, {}^{-1}B(y, a_1^{n-2}, z), b_1^{n-2}), z, b_1^{n-2}) = {}^{-1}B(x, y, a_1^{n-2}) \Longrightarrow$$
$${}^{-1}B({}^{-1}B(x, y, a_1^{n-2}), z, b_1^{n-2}) = {}^{-1}B(x, {}^{-1}B(y, a_1^{n-2}, z), b_1^{n-2}).$$

Since

$$B(v, u, b_1^{n-2}) = x \Longleftrightarrow {}^{-1}B(x, u, b_1^{n-2}) = v$$

and

$$B(u, a_1^{n-2}, z) = y \Longleftrightarrow {}^{-1}B(y, a_1^{n-2}, z) = u.$$

Sketch of the proof of 8^o.

The case $n = 2$ follows from 7^o. The case $n \geq 3$ is a consequence of 7^o, 5^o and 1.5.

Now, by 5^o, 6^o, 8^o, 1.4, $(\bar{o})$ and the substitution $A = {}^{-1}B$, we conclude that (Q, A) is an n–group. Hence, 1.3 and 1.6 completes the proof. □

2.3. Remark. In this paper n–group (Q, A), $n \geq 2$, is described as an n–groupoid $(Q, {}^{-1}A)$ with two laws. Similarly, the n–group (Q, A) can be described as the n–groupoid (Q, A^{-1}) such that

$$A^{-1}(x, a_1^{n-2}, y) = z \Longleftrightarrow A(x, a_1^{n-2}, z) = y\,.$$

Variety of groups of the type $\langle 2 \rangle$ has been considered in [7] (see, also [8] and [3]). The investigation of this paper was extended in [12] for groups, for rings and, more generally, for Ω-groups. In [6] group is described as an groupoid (Q, B) which satisfies one law (i.e. our (i) for $n = 2$) and in which the equality $B(a, x) = b$ has at least one solution x for each $a, b \in Q$.

References

[1] **V. D. Belousov**: *n–ary quasigroups*, (Russian), "Stiinca", Kishinev 1972.

[2] **R. H. Bruck**: *A survey of binary systems*, Springer-Verlag, Berlin-Heidelberg-New York 1971.

[3] **P. M. Cohn**: *Universal algebra*, (Russia) "Mir", Moscow 1968.

[4] **W. Dörnte**: *Untersuchengen über einen verallgemeinerten Gruppenbegriff*, Math. Z. **29** (1928), 1 – 19.

[5] **W. A. Dudek, K. Glazek, B. Gleichgewicht**: *A note on the axioms of n-groups*, Coll. Math. Soc. J. Bolyai, **29** Universal Algebra, Esztergrom (Hungary), 1977, 195 – 202.

[6] **H. Furstenberg**: *The inverse operation in groups*, Proc. Amer. Math. Soc. **6** (1955), 991 – 997.

[7] **G. Higman, B. H. Neuman**: *Groups as groupoids with one law*, Publ. Math. Debrecen **2** (1952), 215 – 221.

[8] **A. G. Kurosh**: *The theory of groups*, (Russian), "Nauka", Moscow 1967.

[9] **A. G. Kurosh**: *General algebra* (lectures 1969-1970), (Russian), "Nauka", Moscow 1974.

[10] **E. L. Post**: *Polyadic groups*, Trans. Amer. Math. Soc. **48** (1940), $208-350$.

[11] **E. I. Sokolov**: *On Gluskin-Hosszú theorem for Dörnte n-group*, (Russian), Mat. issl. **39** (1976), $187-189$.

[12] **V. Tasić**: *On single-law definitions of groups*, Bull. Austral. Math. Soc. **37** (1988), $101-106$.

[13] **H. Tvermoes**: *Über eine Verallgemeinrung des Gruppenbegriffs*, Math. Scand. **1** (1953), $18-30$.

[14] **J. Ušan**: *Neutral operations of n-groupoids*, Rev. of Research, Fac. of Sci. Univ. of Novi Sad, Math. Ser. **18.2** (1988), $117-126$.

[15] **J. Ušan**: *A comment on n-groups*, Rev. of Research, Fac. of Sci. Univ. of Novi Sad, Math. Ser. **24.1** (1994), $281-288$.

[16] **J. Ušan**: *On n-groups with $\{i,j\}$-neutral operation for $\{i,j\} \neq \{1,n\}$*, Rev. of Research, Fac. of Sci. Univ. of Novi Sad, Math. Ser. **25.2** (1995), $167-178$.

[17] **J. Ušan**: *n-groups, $n \geq 2$, as variety of type $\langle n, n-1, n-2 \rangle$* , Algebra and Model Theory, Collection of papers edited by A.G. Pinus and K.N.Ponomaryov, Novosibirsk 1997, $182-208$.

[18] **J. Ušan**: *On n-groups*, Maced. Acad. Sci. and Arts, Contributions, Sect. Math. Techn. Sci. **XVIII 1-2** (1997), (in print).

Institute of Mathematics
University of Novi Sad
Trg D. Obradovića 4
21000 Novi Sad
Yugoslavia

Received 20 September, 1997

Quasigroups and Related Systems, **4** (1997), 77–87

On ordered $n-$groups

Janez Ušan and Mališa Žižović

Abstract

Among the results of the paper is the following proposition. Let $(Q, \{\cdot, \varphi, b\})$ be an arbitrary $nHG-$algebra associated to the n-group (Q, A), where $n \geq 3$. If $\leq$ is a partial order defined on Q, then, $(Q, A, \leq)$ is an ordered $n-$group iff $(Q, \cdot, \leq)$ is an ordered group and for every $x, y \in Q$ the following implication holds $x \leq y \Longrightarrow \varphi(x) \leq \varphi(y)$.

1. Preliminaries

Definition 1.1. Let $n \geq 2$ and let (Q, A) be an $n-$groupoid. Then:

(a) (Q, A) is an $n-$*semigroup* iff for every $i, j \in \{1, \ldots, n\}$, $i < j$ the following law (called the $(i, j)-$*associativity*) holds

$$A(x_1^{i-1}, A(x_i^{i+n-1}), x_{i+n}^{2n-1}) = A(x_1^{j-1}, A(x_j^{j+n-1}), x_{j+n}^{2n-1})\,,$$

(b) (Q, A) is an $n-$*quasigroup* iff for every $i \in \{1, \ldots, n\}$ and for every $a_1^n \in Q$ is exactly one $x_i \in Q$ such that

$$A(a_1^{i-1}, x_i, a_i^{n-1}) = a_n\,,$$

(c) (Q, A) is a *Dörnte n–group* (briefly: *n-group*) iff is an n-semigroup and an $n-$quasigroup.

1991 Mathematics Subject Classification: 20N15

Keywords: $n-$semigroup, $n-$quasigroup, $n-$group, $\{1, n\}-$neutral operation, $nHG-$algebra.

A notion of an $n-$group was introduced by W. Dörnte in [2] as a generalization of the notion of a group.

Proposition 1.2. [10] *Let $n \geq 2$ and let (Q, A) be an $n-$groupoid. Then the following statements are equivalent:*

(i) *(Q, A) is an $n-$group,*

(ii) *there are mappings $^{-1}$ and $\mathbf{e}$ respectively of the sets Q^{n-1} and Q^{n-2} into the set Q such that in the algebra $(Q, \{A,^{-1}, \mathbf{e}\})$ of the type $< n, n-1, n-2 >$ the following laws hold:*

$$(a) \quad A(x_1^{n-2}, A(x_{n-1}^{2n-2}), x_{2n-1}) = A(x_1^{n-1}, A(x_n^{2n-1})) \, ,$$
$$(b) \quad A(\mathbf{e}(a_1^{n-2}), a_1^{n-2}, x) = x \, ,$$
$$(c) \quad A((a_1^{n-2}, a)^{-1}, a_1^{n-2}, a) = \mathbf{e}(a_1^{n-2}) \, ,$$

(iii) *there are mappings $^{-1}$ and $\mathbf{e}$ respectively of the sets Q^{n-1} and Q^{n-2} into the set Q such that in the algebra $(Q, \{A,^{-1}, \mathbf{e}\})$ of the type $< n, n-1, n-2 >$ the following laws hold:*

$$(\overline{a}) \quad A(A(x_1^n), x_{n+1}^{2n-1}) = A(x_1, A(x_2^{n+1}), x_{n+2}^{2n-1}) \, ,$$
$$(\overline{b}) \quad A(x, a_1^{n-2}, \mathbf{e}(a_1^{n-2})) = x \, ,$$
$$(\overline{c}) \quad A(a, a_1^{n-2}, (a_1^{n-2}, a)^{-1}) = \mathbf{e}(a_1^{n-2}). \qquad \square$$

Remark 1.3. $\mathbf{e}$ is an $\{1, n\}-$neutral operation of $n-$grupoid (Q, A) iff algebra $(Q, \{A, \mathbf{e}\})$ of type $< n, n-2 >$ satisfies the laws (b) and $(\overline{b})$. The notion of $\{i, j\}-$neutral operation $(i, j \in \{1, \ldots, n\}, i < j)$ of an $n-$groupoid is defined in a similar way (cf. [6]). In every $n-$groupoid there is at most one $\{i, j\}-$neutral operation. A $\{1, n\}-$neutral operation there exists in every $n-$group, but there are $n-$groups without $\{i, j\}-$neutral operations with $\{i, j\} \neq \{1, n\}$ (cf. [9]). Operation $^{-1}$ is a generalization of the inverse operation in a group. In fact, if (Q, A) is an $n-$group, $n \geq 2$, then for every $a \in Q$ and for every sequence a_1^{n-2} over Q is

$$(a_1^{n-2}, a)^{-1} = \mathsf{E}(a_1^{n-2}, a, a_1^{n-2}) \, ,$$

where E is an $\{1, 2n-1\}-$neutral operation of the $(2n-1)-$group $(Q, \overset{2}{A})$ defined by $\overset{2}{A}(x_1^{2n-1}) = A(A(x_1^n), x_{n+1}^{2n-1})$ (cf. [7]). Obviously, for $n = 2$, $a^{-1} = \mathsf{E}(a)$; a^{-1} is the inverse element of the element a with respect to the neutral element $\mathbf{e}(\emptyset)$ of the group (Q, A).

Theorem 1.4. (Hosszú–Gluskin Theorem) (cf. [5], [4])
For every $n-$group (Q, A), $n \geq 3$, there is an algebra $(Q, \{\cdot, \varphi, b\})$ such that the following statements hold:

1° $(Q, \cdot)$ *is a group,*
2° $\varphi \in Aut(Q, \cdot)\,,$
3° $\varphi(b) = b\,,$
4° *for every* $x \in Q, \quad \varphi^{n-1}(x) \cdot b = b \cdot x\,,$
5° *for every* $x_1^n \in Q, \quad A(x_1^n) = x_1 \cdot \varphi(x_2) \cdot \ldots \cdot \varphi^{n-1}(x_n) \cdot b.$ □

Definition 1.5. [8] We say that an algebra $(Q, \{\cdot, \varphi, b\})$ is a *Hosszú–Gluskin algebra* of order n $(n \geq 3)$ (briefly: nHG*–algebra*) iff it satisfies $1° - 4°$ from the above theorem. If it satisfies also 5°, then we say that an nHG– algebra $(Q, \{\cdot, \varphi, b\}))$ is *associated* to the $n-$group (Q, A).

Proposition 1.6. [8] *Let $n \geq 3$, let (Q, A) be an $n-$group, and* $\mathbf{e}$ *its $\{1, n\}-$ neutral operation. Further on, let c_1^{n-2} be an arbitrary sequence over Q and let for every $x, y \in Q$*

$$B_{(c_1^{n-2})}(x, y) = A(x, c_1^{n-2}, y)\,,$$
$$\varphi_{(c_1^{n-2})}(x) = A(\mathbf{e}(c_1^{n-2}), x, c^{n-2}) \quad \textit{and}$$
$$b_{(c_1^{n-2})} = A(\mathbf{e}(c_1^{n-2}), \mathbf{e}(c_1^{n-2}), \ldots, \mathbf{e}(c_1^{n-2})).$$

Then, the following statements hold
(i) $(Q, \{B_{(c_1^{n-2})}, \varphi_{(c_1^{n-2})}, b_{(c_1^{n-2})})\}$ *is an $nHG-$algebra associated to the $n-$group (Q, A) and*
(ii) $\mathcal{C}_A = \{(Q, \{B_{(c_1^{n-2})}, \varphi_{(c_1^{n-2})}, b_{(c_1^{n-2})}\}) \,:\, c_1^{n-2} \in Q\,\}$ *is the set of all $nHG-$algebras associated to the $n-$group (Q, A).* □

Proposition 1.7. [8] *Let (Q, A) be an n–group,* $\mathbf{e}$ *its $\{1, n\}$–neutral operation and $n \geq 3$. Then for every $a_1^{n-2} \in Q$ and every $1 \leq i \leq n-2$ there is exactly one $x_i \in Q$ such that* $\mathbf{e}(a_1^{i-1}, x_i, a_i^{n-3}) = a_{n-2}\,.$ □

2. Main results

Definition 2.1. Let (Q, A) be an $n-$group, $n \geq 2$. If $\leq$ is a partial order on Q such that

$$x \leq y \;\Rightarrow\; A(z_1^{i-1}, x, z_i^{n-1}) \leq A(z_1^{i-1}, y, z_i^{n-1}) \tag{1}$$

for all $x, y, z_1, ..., z_{n-1} \in Q$ and $i \in \{1, 2, ..., n-1\}$, then, we say that $(Q, A, \leq)$ is an *ordered $n-$group.*

Note that in the case $n = 2$ $(Q, A, \leq)$ is an ordered group in the sense of [3].

Theorem 2.2. *Let $\leq$ be a partial order on Q. Also, let $n \geq 3$ and let (Q, A) be an $n-$group. In addition, let $(Q, \{\cdot, \varphi, b\}\}$ be an arbitrary $nHG-$algebra associated to the $n-$group (Q, A). Then, $(Q, A, \leq)$ is an ordered $n-$group iff for all $x, y, z \in Q$ the following two formulas hold*

$$x \leq y \;\;\Rightarrow\;\; xz \leq yz \;\wedge\; zx \leq zy \tag{2}$$

$$x \leq y \;\;\Rightarrow\;\; \varphi(x) \leq \varphi(y)). \tag{3}$$

Proof. Let $(Q, A, \leq)$ be an ordered $n-$group and let $n \geq 3$. Also, let $\mathbf{e}$ be an $\{1, n\}-$neutral operation of the $n-$group (Q, A). In addition, let $(Q, \{\cdot, \varphi, b\})$ be an arbitrary $nHG-$algebra associated to the $n-$group (Q, A). Then, by Proposition 1.6, there is at least one sequence c_1^{n-2} over Q such that for every $x, y \in Q$ the following two equalities hold:

$$x \cdot y = A(x, c_1^{n-2}, y)\,,$$

$$\varphi(x) = A(\mathbf{e}(c_1^{n-2}), x, c_1^{n-2}).$$

Hence, by Definition 2.1, we conclude that the formulas (2) and (3) hold in $(Q, \{\cdot, \varphi, b\})$.

Conversely, let $(Q, \{\cdot, \varphi, b\})$ be an arbitrary $nHG-$algebra associated to the $n-$group (Q, A). Also, let $\leq$ be a partial order on Q. Assume that an $nHG-$ algebra $(Q, \{\cdot, \varphi, b\})$ satisfies (2) and (3). Then, for every $x, y, z_1^{n-2} \in Q$ and $i \in \{1, 2, ..., n\}$ it satisfies also (1).

Indeed, for $1 \leq i \leq n-1$ $x \leq y$ implies $\varphi^{i-1}(x) \leq \varphi^{i-1}(y)$, and in the consequence

$$z_1 \cdot \ldots \cdot \varphi^{i-2}(z_{i-1}) \cdot \varphi^{i-1}(x) \leq z_1 \cdot \ldots \cdot \varphi^{i-2}(z_{i-1}) \cdot \varphi^{i-1}(y),$$

which gives

$$z_1 \cdot \ldots \cdot \varphi^{i-2}(z_{i-1}) \cdot \varphi^{i-1}(x) \cdot \varphi^{i}(z_i) \cdot \ldots \cdot b \cdot z_{n-1} \leq \\ z_1 \cdot \ldots \cdot \varphi^{i-2}(z_{i-1}) \cdot \varphi^{i-1}(y) \cdot \varphi^{i}(z_i) \cdot \ldots \cdot b \cdot z_{n-1}.$$

Hence, by Definition 1.5, we conclude that (1) holds.

The cases $i = 1$ and $i = n$ are obvious. □

Example 2.3. Let $(Z, +)$ be the additive group of all integers, and let $\leq$ by the natural order defined on Z. Then Z with the ternary operation A defined by

$$A(x, y, z) = x + (-y) + z$$

is a 3–group.

Moreover, $(Z, \{+, \varphi, 0\})$, where $\varphi(x) = -x$, is an $nHG-$algebra associated to a 3–group (Z, A).

Since for every $x, y \in Z$ $x \leq y$ implies $\varphi(y) \leq \varphi(x)$, we conclude (by Theorem 2.2) that $(Z, A, \leq)$ is not an ordered $3-$group. □

Example 2.4. Let $(Z, +, \leq)$ be as in the previous example. Let

$$B(x_1^n) = x_1 + x_2 + \ldots + x_n + 2$$

for every $x_1^n \in Z$, $n \geq 3$. Then, (Z, B) is an $n-$group with $(Z, \{+, id, 2\})$ as its associated $nHG-$algebra. Obviously $(Z, B, \leq)$ is an ordered $n-$group.

Moreover, $(Z, C, \leq)$ and $(Z, D, \leq)$ where

$$C(x_1^n) = x_1 + x_2 + \ldots + x_n,$$

$$D(x_1^n) = x_1 + x_2 + \ldots + x_n + (-2)$$

are ordered $n-$groups as well. □

Theorem 2.5. *Let $(Q, \leq)$ be a chain. Also, let (Q, A) be an $n-$group, $^{-1}$ its inverse operation,* $\mathbf{e}$ *its $\{1, n\}-$neutral operation and $n \geq 3$. Moreover, let a be an arbitrary element of the set Q and a_1^{n-2} be an sequence over Q such that* $\mathbf{e}(a_1^{n-2}) = a$. *Then*

(*i*) *$(\{x : a \leq x\}, A)$ is an $n-$subsemigroup of the $n-$group (Q, A) iff $a \leq A(\overset{n}{a})$,*

(*ii*) *$(\{x : (a_1^{n-2}, A(\overset{n}{a}))^{-1} \leq x\}, A)$ is an $n-$subsemigroup of the $n-$group (Q, A) iff $A(\overset{n}{a}) \leq a$,*

(*iii*) *let $a \leq A(\overset{n}{a})$ and let c be an arbitrary element of the set Q such that $a \leq c$. Then $(\{x : c \leq x\}, A)$ is an $n-$subsemigroup of the $n-$group (Q, A),*

(*iv*) *let $A(\overset{n}{a}) \leq a$ and let c be an arbitrary element of the set Q such that $(a_1^{n-2}, A(\overset{n}{a}))^{-1} \leq c$. Then $(\{x : c \leq x\}, A)$ is an $n-$subsemigroup of the $n-$group (Q, A).*

Proof. 1) Let a be an arbitrary element of the set Q. Also let a_1^{n-2} be an sequence over Q such that $\mathbf{e}(a_1^{n-2}) = a$. Moreover, let

(a) $\qquad x \cdot y = A(x, a_1^{n-2}, y)$,

(b) $\qquad \varphi(x) = A(a, x, a_1^{n-2})$,

(c) $\qquad b = A(\overset{n}{a})$,

(d) $\qquad x^{\mathbf{-1}} = (a_1^{n-2}, x)^{-1}$

for all $x, y \in Q$. Then:

1^o $(Q, \{\cdot, \varphi, b\})$ is an $nHG-$algebra associated to (Q, A),

2^o $a = \mathbf{e}(a_1^{n-2})$ is a neutral element of the group $(Q, \cdot)$,

3^o $^{\mathbf{-1}}$ is an inverse operation of the group $(Q, \cdot)$.

By Theorem 2.2 and 1^o, we conclude that

4^o $(Q, \cdot, \leq)$ is a linearly ordered group,

5^o $x \leq y \Rightarrow \varphi(x) \leq \varphi(y)$ for all $x, y \in Q$.

2) Assume now that $(\{x : a \leq x\}, A)$ is an $n-$subsemigroup of the $n-$group (Q, A). Then for all $x_1^n \in Q$ from $x_1^n \in \{x : a \leq x\}$ follows $A(x_1^n) \in \{x : a \leq x\})$, whence we conclude that $a \leq A(\overset{n}{a})$.

Conversely, let $a \le A(\overset{n}{a})$. Hence, by 4^o and 5^o, we conclude that for every sequence x_1^n over Q the following implications hold:

$$\bigwedge_{i=1}^{n} x_i \in \{x : a \le x\} \ \Rightarrow a \le x_1 \cdot \varphi(x_2) \cdot \ldots \cdot \varphi^{n-1}(x_n) \cdot b \ \Rightarrow a \le A(x_1^n),$$

i.e.

$$(\forall x_i \in Q)_1^n \ (\bigwedge_{i=1}^{n} \ x_i \in \{x : a \le x\} \ \Rightarrow \ A(x_1^n) \in \{x : a \le x\}).$$

3) Let $(\{x \ : \ (a_1^{n-2}, A(\overset{n}{a}))^{-1} \ \le \ x\}, A)$ be an $n-$subsemigroup of the $n-$group (Q, A). Then for all

$$\bigwedge_{i=1}^{n} x_i \in \{x : b^{-1} \le x\} \Rightarrow A(x_1^n) \in \{x : b^{-1} \le x\}$$

by (c), (d). Whence, by 4^o, $\varphi(b) = b$, $\varphi(b^{-1}) = b^{-1}$ we conclude that

$$\begin{aligned} b^{-1} \le A(b^{-1}, b^{-1}, \ldots, b^{-1}) &= b^{-1} \cdot \varphi(b^{-1}) \cdot \ldots \cdot \varphi^{n-2}(b^{-1}) \cdot b \cdot b^{-1} \\ &= b^{-1} \cdot b^{-1} \cdot \ldots \cdot b^{-1} \cdot b \cdot b^{-1}, \end{aligned}$$

i.e. $b^{n-2} \le a$. Hence $b \le a$ by 4^o.

On the other hand, if $A(\overset{n}{a}) \le a$, then, by (c),(d) and 1°-4°, we have $a \le b^{-1}$, whence, by 1° and $\varphi(b^{-1}) = b^{-1}$, we obtain

$$\begin{aligned} &b^{-1} \le b^{-1} \le b^{-1} \\ &a \le b^{-1} \le \varphi(b^{-1}) \\ &\cdots\cdots\cdots\cdots \\ &\cdots\cdots\cdots\cdots \\ &a \le b^{-1} \le \varphi^{n-2}(b^{-1}) \\ &b \le b \le b \\ &b^{-1} \le b^{-1} \le b^{-1} \ . \end{aligned}$$

Hence, by 4°, 1° and 1.5, we conclude that

$$b^{-1} \ \le \ b^{-1} \cdot \varphi(b^{-1}) \cdot \ldots \cdot \varphi^{n-2}(b^{-1}) \cdot b \cdot b^{-1} = A(b^{-1}, b^{-1}, \ \ldots, b^{-1}),$$

i.e.

$$b^{-1} \ \le \ A(b^{-1}, b^{-1}, \ldots, b^{-1}),$$

whence, by (i), we see that $(\{x : b^{-1} \le x\}, A)$ is an n-subsemigroup of the n-group (Q, A).

4) Let $a \le A(\overset{n}{a}) = b$. Also let c be an arbitrary element of the set Q such that $a \le c$. Since $a \le b$, then

(a) $\quad c \cdot \varphi(c) \cdot \ldots \cdot \varphi^{n-1}(c) \cdot a \;\le\; c \cdot \varphi(c) \cdot \ldots \cdot \varphi^{n-1}(c) \cdot b.$

By $1^\circ, 2^\circ, 5^\circ$ and $a \le c$, we obtain: $c \le c,\ a \le \varphi(c), \ldots, a \le \varphi^{n-1}(c)$, whence, by $2^\circ, 4^\circ$ and 5°, we conclude that

(b) $\quad c \le c \cdot \varphi(c) \cdot \ldots \cdot \varphi^{n-1}(c) = c \cdot \varphi(c) \cdot \ldots \cdot \varphi^{n-1}(c) \cdot a.$

By (a) and (b), we conclude that

$$c \le c \cdot \varphi(c) \cdot \ldots \cdot \varphi^{n-1}(c) \cdot b,$$

i.e. $c \le A(\overset{n}{c})$. Hence, by (i) $(\{x : c \le x\}, A)$ is an n-subsemigroup of the n-group (Q, A).

5) Let $A(\overset{n}{a}) \le a$. Also let c be an arbitrary element of the set Q such that $b^{-1} \le c$. Hence, by 1°, 1.5, 2°, 4° and 5°, we conclude

$$\begin{aligned} c &= c \cdot a \cdot \ldots \cdot a \cdot b \cdot b^{-1} = c \cdot \varphi(a) \cdot \ldots \cdot \varphi^{n-2}(a) \cdot b \cdot b^{-1} \\ &\le c \cdot \varphi(b^{-1}) \cdot \ldots \cdot \varphi^{n-2}(b^{-1}) \cdot b \cdot b^{-1} \\ &\le c \cdot \varphi(c) \cdot \ldots \cdot \varphi^{n-2}(c) \cdot b \cdot c \\ &= A(\overset{n}{c}), \end{aligned}$$

whence, by (i) we prove that $(\{x : c \le x\}, A)$ is an n-subsemigroup of the n-group (Q, A). □

Remark 2.6. The above theorem describes so-called the *right cone* (cf. [3]), i.e. the set $K_r(c) = \{x : c \le x\}$. The analogous result holds for the *left cone* $K_l(c) = \{x : x \le c\}$.

3. Four propositions more

Proposition 3.1. *If* $(Q, A, \le)$ *is an ordered* $n-$*group* $(n \ge 2)$*, then*

$$(\forall x \in Q)\ (\forall y \in Q)\ (\forall z_j \in Q)_1^{n-1}$$
$$\bigwedge_{i=1}^{n} (x \le y \iff A(z_1^{i-1}, x, z_i^{n-1}) \le A(z_1^{i-1}, y, z_i^{n-1})\,).$$

Proof. We prove only $\Leftarrow$ since the implication $\Rightarrow$ is obvious.
1) In the case $i = 1$, $A(x, a_1^{n-2}, a) \le A(y, a_1^{n-2}, a)$ implies

$$A(A(x, a_1^{n-2}, a), a_1^{n-2}, (a_1^{n-2}, a)^{-1}) \le A(A(y, a_1^{n-2}, a), a_1^{n-2}, (a_1^{n-2}, a)^{-1}),$$

and in the consequence
$A(x, a_1^{n-2}, A(a, a_1^{n-2}, (a_1^{n-2}, a)^{-1})) \le A(y, a_1^{n-2}, A(a, a_1^{n-2}, (a_1^{n-2}, a)^{-1}))$,
which gives
$A(x, a_1^{n-2}, \mathbf{e}(a_1^{n-2})) \le A(y, a_1^{n-2}, \mathbf{e}(a_1^{n-2}))$. Hence $x \le y$.

2) The case $i = n$ may be proved analogously.

3) Let now $i \in \{2, \ldots, n-1\}$. Then

$$A(a_1^{i-1}, x, a_i^{n-1}) \le A(a_1^{i-1}, y, a_i^{n-1}) \Rightarrow$$
$$A(b_i^{n-1}, A(a_1^{i-1}, x, a_i^{n-1}), b_1^{i-1}) \le A(b_i^{n-1}, A(a_1^{i-1}, y, a_i^{n-1}), b_1^{i-1}) \Rightarrow$$
$$A(A(b_i^{n-1}, a_1^{i-1}, x), a_i^{n-1}, b_1^{i-1}) \le A(A(b_i^{n-1}, a_1^{i-1}, y), a_i^{n-1}, b_1^{i-1}) \Rightarrow$$
$$A(b_i^{n-1}, a_1^{i-1}, x) \le A(b_i^{n-1}, a_1^{i-1}, y) \Rightarrow x \le y. \qquad \square$$

Proposition 3.2. *Let $(Q, A, \le)$ be an ordered $n-$group and let $n \ge 2$. Also, let $^{-1}$ be an inverse operation of the $n-$group (Q, A). Then*

$$(\forall x, y \in Q)\,(\forall a_j \in Q)_1^{n-1} \quad x \le y \Leftrightarrow (a_1^{n-1}, y)^{-1} \le (a_1^{n-1}, x)^{-1}.$$

Proof. $x \le y \Leftrightarrow A((a_1^{n-2}, x)^{-1}, a_1^{n-2}, x) \le A((a_1^{n-2}, x)^{-1}, a_1^{n-2}, y) \Leftrightarrow$
$\mathbf{e}(a_1^{n-2}) \le A((a_1^{n-2}, x)^{-1}, a_1^{n-2}, y) \Leftrightarrow A(\mathbf{e}(a_1^{n-2}), a_1^{n-2}, (a_1^{n-2}, y)^{-1}) \le$
$\le A(A((a_1^{n-2}, x)^{-1}, a_1^{n-2}, y), a_1^{n-2}, (a_1^{n-2}, y)^{-1}) \Leftrightarrow$
$(a_1^{n-2}, y)^{-1} \le A((a_1^{n-2}, x)^{-1}, a_1^{n-2}, A(y, a_1^{n-2}, (a_1^{n-2}, y)^{-1})) \Leftrightarrow$
$(a_1^{n-2}, y)^{-1} \le A((a_1^{n-2}, x)^{-1}, a_1^{n-2}, \mathbf{e}(a_1^{n-2})) \Leftrightarrow$
$(a_1^{n-2}, y)^{-1} \le (a_1^{n-2}, x)^{-1}$. $\square$

Proposition 3.3. *Let $(Q, A, \le)$ be an ordered $n-$group and let $n \ge 3$. Also, let $\mathbf{e}$ be an $\{1, n\}-$neutral operation of the $n-$group (Q, A). Then*

$$(\forall x \in Q)\,(\forall y \in Q)\,(\forall a_j \in Q)_1^{n-3}$$
$$\bigwedge_{i=1}^{n-2} (\, x \le y \Leftrightarrow \mathbf{e}(a_1^{i-1}, y, a_i^{n-3}) \le \mathbf{e}(a_1^{i-1}, x, a_i^{n-3})\,).$$

Proof. Since $A(a, x_1^{n-2}, b) = A(A(a, y_1^{n-2}, (y_1^{n-2}, \mathbf{e}(x_1^{n-2}))^{-1}), y_1^{n-2}, b)$ by Theorem 4 from [7], then

$x \leq y \Leftrightarrow A(a, a_1^{i-1}, x, a_i^{n-3}, b) \leq A(a, a_1^{i-1}, y, a_i^{n-3}, b) \Leftrightarrow$
$A(A(a, c_1^{n-2}, (c_1^{n-2}, \mathbf{e}(a_1^{i-1}, x, a_i^{n-3}))^{-1}), c_1^{n-2}, b) \leq$
$A(A(a, c_1^{n-2}, (c_1^{n-2}, \mathbf{e}(a_1^{i-1}, y, a_i^{n-3}))^{-1}), c_1^{n-2}, b) \Leftrightarrow$
$A(a, c_1^{n-2}, (c_1^{n-2}, \mathbf{e}(a_1^{i-1}, x, a_i^{n-3}))^{-1}) \leq$
$A(a, c_1^{n-2}, (c_1^{n-2}, \mathbf{e}(a_1^{i-1}, y, a_i^{n-3}))^{-1}) \Leftrightarrow$
$(c_1^{n-2}, \mathbf{e}(a_1^{i-1}, x, a_i^{n-3}))^{-1} \leq (c_1^{n-2}, \mathbf{e}(a_1^{i-1}, y, a_i^{n-3}))^{-1} \Leftrightarrow$
$\mathbf{e}(a_1^{i-1}, y, a_i^{n-3}) \leq \mathbf{e}(a_1^{i-1}, x, a_i^{n-3})\,.$ □

Proposition 3.4. *Let $(Q, A, \leq)$ be an ordered $n-$group and let $n \geq 3$. Also, let $^{-1}$ be an inverse operation of the $n-$group (Q, A). Then*

$$(\forall x \in Q)\,(\forall y \in Q)\,(\forall b \in Q)(\forall a_j \in Q)_1^{n-3}$$
$$\bigwedge_{i=1}^{n-2} (\, x \leq y \;\Rightarrow\; (a_1^{i-1}, y, a_i^{n-3}, b)^{-1} \leq (a_1^{i-1}, x, a_i^{n-3}, b)^{-1}\,).$$

Proof. Since $x \leq y$ implies

$$\mathsf{E}(a_1^{i-1}, y, a_i^{n-3}, b, a_1^{i-1}, y, a_i^{n-3}) \leq \mathsf{E}(a_1^{i-1}, y, a_i^{n-3}, b, a_1^{i-1}, x, a_i^{n-3})$$

and

$$\mathsf{E}(a_1^{i-1}, y, a_i^{n-3}, b, a_1^{i-1}, x, a_i^{n-3}) \leq \mathsf{E}(a_1^{i-1}, x, a_i^{n-3}, b, a_1^{i-1}, x, a_i^{n-3}),$$

then from the transitivity of $\leq$ follows that $x \leq y$ implies

$$\mathsf{E}(a_1^{i-1}, y, a_i^{n-3}, b, a_1^{i-1}, y, a_i^{n-3}) \leq \mathsf{E}(a_1^{i-1}, x, a_i^{n-3}, b, a_1^{i-1}, x, a_i^{n-3}).$$

This completes the proof because

$$(a_1^{i-1}, z, a_i^{n-3}, b)^{-1} = \mathsf{E}(a_1^{i-1}, z, a_i^{n-3}, b, a_1^{i-1}, z, a_i^{n-3}).$$ □

References

[1] **G. Crombez**: *On partially ordered $n-$groups*, Abh. Math. Sem., Hamburg **38** (1972), 141 − −146.

[2] **W. Dörnte**: *Untersuchengen über einen verallgemeinerten Gruppenbegriff*, Math. Z. **29** (1928), 1 − 19.

[3] **L. Fuchs**: *Partially ordered algebraic systems*, Pergamon Press, Oxford 1963.

[4] **L. M. Gluskin**: *Positional operatives*, (Russian), **68(110)** (1965), $444-472$.

[5] **M. Hosszú**: *On the explicit form of $n-$group operations*, Publ. Math., Debrecen **10** (1963), $88-92$.

[6] **J. Ušan**: *Neutral operations of $n-$groupoids*, (Russian), Rev. of Research, Fac.of Sci. Univ. of Novi Sad, Math. Ser. **18.2** (1988), $117-126$.

[7] **J. Ušan**: *A comment on $n-$groups*, Rev. of Research, Fac. of Sci. Univ. of Novi Sad, Math. Ser. **24.1** (1994), $281--288$.

[8] **J. Ušan**: *On Hosszú–Gluskin algebras corresponding to the same $n-$group*, Rev. of Research, Fac. of Sci. Univ. of Novi Sad, Math. Ser. **25.1** (1995), $101--119$.

[9] **J. Ušan**: *On $n-$groups with $\{i,j\}-$neutral operation for $\{i,j\} \neq \{1,n\}$*, Rev. of Research, Fac. of Sci. Univ. of Novi Sad, Math. Ser. **25.2** (1995), $167-178$.

[10] **J. Ušan**: *$n-$groups, $n \geq 2$, as varieties of type $\langle n, n-1, n-2\rangle$*, Algebra and Model Theory, Collection of papers edited by A. G. Pinus and K. N. Ponomaryov, Novosibirsk 1997, $182-208$.

Received September 20 1997 and in revised form March 29, 1999

J. Ušan
Institute of Mathematics
University of Novi Sad
Trg D. Obradovića 4
21000 Novi Sad
Yugoslavia

M. Žižovič
Faculty of Technical Science
University of Kragujevac
Svetog Save 65
32000 Čačak
Yugoslavia

Quasigroups and Related Systems, **4** (1997), 89–102

NLPN Sequences over $GF(q)$

Czesław Kościelny

Abstract

PN sequences over $GF(q)$ are unsuitable directly for cryptography because of their strong linear structure. In the paper it is shown that in order to obtain the sequence with the same occurence of elements and with the same length as PN sequence, but having non-linear structure, it simply suffices to *modulate* the PN sequence by its cyclic shift using two-input quasigroup operator. Thus, such new sequences, named NLPN sequences, which means Non-Linear Pseudo-Noise sequences, can be easily generated over $GF(q)$ for $q \geq 3$. The method of generating the NLPN sequences is exhaustively explained by a detailed example concerning non-linear pseudo-noise sequences over $GF(8)$. In the other example the way of constructing good keys generator for generalized stream-ciphers over the alphabet of order 256 is sketched. It is hoped that NLPN sequences will find many applications in such domains as cryptography, Monte-Carlo methods, spread-spectrum communication, GSM systems, random number generators, scrambling, testing VLSI chips and video encryption for pay-TV purposes.

1. Introduction

Non-binary pseudo-random sequences over $GF(q)$ of length $q^m - 1$, called PN sequences have been known for a long time [3,6,7]. Although they are used in many domains of modern technology, they are

1991 Mathematics Subject Classification: 94A55, 94A60, 20N05

Keywords: PN sequences, NLPN sequences, random number generators, cryptographic keys for generalized stream ciphers, finite field arithmetic, fast software encryption, quasigroups, Latin squares.

unsuitable directly for cryptographic applications, mainly because of their strong linear structure. Therefore, several concepts have been proposed in order to demolish this structure (e.g. non-linear filter generators [2,7] and multiplexed sequences [4]), consisting in non-linear *filtering* or *modulating* PN sequences over $GF(2)$.

The presented method concerns sequences over $GF(q)$ for $q \geq 3$ and it uses a quasigroup operators in order to transform PN sequence into a sequence, having much more randomness than the former. Thus the generator of NLPN sequences consists of two identical linear shift registers with feedback, determined by the same primitive polynomial of degree m over $GF(q)$, which are equipped with the possibility of *tuning* the initial states. The method is very simple and it is well adapted for both software and hardware implementations.

2. A Quasigroup-Based Method of Constructing NLPN Sequences over $GF(q)$ and Their Properties

Let

$$\mathbf{a} = a_0 a_1 \cdots a_{q^m-2} \tag{1}$$

be an arbitrary sequence of elements from $GF(q)$, and let

$$R = \begin{bmatrix} a_i & a_{i+1} & \cdots & a_{i+m+c-1} \\ a_{i+1} & a_{i+2} & \cdots & a_{i+m+c} \\ . & . & \cdots & . \\ . & . & \cdots & . \\ . & . & \cdots & . \\ a_{i+m+c-1} & a_{i+m+c} & \cdots & a_{2(i+m+c-1)} \end{bmatrix}, \tag{2}$$

be an $(c+m) \times (c+m)$ matrix over $GF(q)$, the rows of which are consecutive elements from the sequence (1). The subscripts i, $0 \leq i \leq q^m - 2$, are taken modulo $q^m - 1$.

Definition: A sequence (1) is called a non-linear PN sequence and further denoted as NLPN sequence, if

$$\exists\, i,\ 0 \leq i \leq q^m - 2,\ \exists\, c \geq 1\ [\det(R)\ \neq 0], \tag{3}$$

and if in the sequence only one element of $GF(q)$ occurs $q^{m-1}-1$ times, while every other element from $GF(q)$ occurs q^{m-1} times.

The presented method stems from the following

Conjecture: Let $q = p^k > 2$, p - prime, k - positive integer ≥ 1 and let $\mathbf{a}$ and $\mathbf{a}^i$ denote a PN sequence of length $q^m - 1$ over $GF(q)$ and its cyclic shift i places to the right, respectively. Then there exist a quasigroup

$$Q = \langle SQ, \bullet \rangle, \tag{4}$$

of order q, viz. $|SQ| = q$, SQ - set of the elements of a quasigroup, represented in the same manner as the elements of $GF(q)$, such that sequences

$$\mathbf{a} \bullet \mathbf{a}^i, \;\; \mathbf{a}^i \bullet \mathbf{a} \tag{5}$$

are NLPN sequences, if

$$i \neq 0 \pmod{(q^m - 1)/(q-1)}. \tag{6}$$

It may be supposed that in the case when in the main diagonal of the quasigroup's operation table any element occurs only once, the fulfilment of condition (6) may not be required.

The number of quasigroups, satisfying this conjecture is not yet known, and one would rather expect that it will not be determined in the near future. The experiments show, however, that it is hard to find a true quasigroup, which does not produce NLPN sequences according to the presented method.

The proof of the conjecture is the subject of current work and will be reported in due course.

At present, the author knows only the following properties of NLPN sequences:

Property I – The Number of Occurrences of Elements of $GF(q)$ in an NLPN *sequence*: If 0 denotes the identity element of the additive group of $GF(q)$, then the element equal to $0 \bullet 0$ occurs in the NLPN sequence $q^{m-1} - 1$ times, while the remaining elements of $GF(q)$ occur in this sequence q^{m-1} times.

An algebraic system $\langle SQ, \bullet \rangle$ is called a *quasigroup* if there is a binary operation $\bullet$ defined in SQ and if, when any two elements $a, b \in SQ$ are given, the equations $a \bullet x = b$ and $y \bullet a = b$, each, have exactly one solution [1].

Property II – The Set of All NLPN *Sequences Derived from One PN Sequence and One Quasigroup Q*: Let $\mathcal{S}_{\mathsf{NLPN}}$ denote the set of all different NLPN sequences generated by one PN sequence and one quasigroup. Then

$$k(q^m - 1) \geq |\mathcal{S}_{\mathsf{NLPN}}| \geq k(q^m - q - 1), \tag{7}$$

where $k = 1$ if a quasigroup Q is abelian, and $k = 2$ if it is non-abelian. This number depends on the elements forming the main diagonal of the quasigroup's operation table.

Property III – Autocorrelation function: Each NLPN sequence belonging to $\mathcal{S}_{\mathsf{NLPN}}$ has distinct autocorrelation function resembling the autocorrelation function of the random sequence of elements of $GF(q)$ having the length $q^m - 1$.

3. Example 1

Since the presented method is rather a new one, it will now be exhaustively explained.

Let 8-element finite field $GF(8) = \langle\{0, 1, \ldots, 7\}, +, \cdot\rangle$ be constructed using the polynomial $x^3 + x + 1$. Then the operations $+$ and $\cdot$ can be defined as follows:

$$x + y = x \text{ XOR } y,$$

$$x \cdot y = \begin{cases} 0 \text{ if } x = 0 \text{ or } y = 0, \\ \mathrm{etn}(\mathrm{nte}(x) + \mathrm{nte}(y) \pmod 7) \text{ otherwise.} \end{cases}$$

It is easy to observe that the above representation of $GF(8)$ results from the assumption that α, primitive element of $GF(8)$ and also a root of the polynomial $x^3 + x + 1$ over $GF(2)$, is denoted by 2. Thus, $\alpha^i = \mathrm{etn}(i)$ for $i = 0,\ 1,\ \ldots, 6$. The functions $\mathrm{nte}(x)$ and $\mathrm{etn}(x)$, named according to the tasks which they perform (nte - number to exponent of α conversion, etn - exponent of α to number conversion) are defined in Table 1.

The values of nte(0) and etn(7) are not used, therefore, they are not defined.

Table 1: FUNCTIONS NTE(x) AND ETN(x) USED FOR MULTIPLYING IN $GF(8)$

x	0	1	2	3	4	5	6	7
nte(x)	?	0	1	3	2	6	4	5
etn(x)	1	2	4	3	6	7	5	?

Table 2: ADDITION AND MULTIPLICATION TABLES IN $GF(8)$

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0	0
1	1	0	3	2	5	4	7	6	1	0	1	2	3	4	5	6	7
2	2	3	0	1	6	7	4	5	2	0	2	4	6	3	1	7	5
3	3	2	1	0	7	6	5	4	3	0	3	6	5	7	4	1	2
4	4	5	6	7	0	1	2	3	4	0	4	3	7	6	2	5	1
5	5	4	7	6	1	0	3	2	5	0	5	1	4	2	7	3	6
6	6	7	4	5	2	3	0	1	6	0	6	7	1	5	3	2	4
7	7	6	5	4	3	2	1	0	7	0	7	5	2	1	6	4	3

Although the operations in $GF(8)$ are simple, the reader can easier follow the presented example by using the tables of addition and multiplication in $GF(8)$, given in Table 2.

Let $\mathbf{s} = s_0 s_1 \cdots s_{62}$ be a PN sequence obtained from the primitive polynomial $x^2 + 2x + 2$ over $GF(8)$. Therefore

$$s_{i+2} = 2s_{i+1} + 2s_i, \quad i = 0,\ 1,\ \ldots,\ 60.$$

If one specifies the initial values as $s_0 = 1,\ s_1 = 0$, then the whole PN sequence will be

$$\mathbf{s} = \mathrm{concat}(\gamma, \alpha\gamma, \alpha^2\gamma, \alpha^3\gamma, \alpha^4\gamma, \alpha^5\gamma, \alpha^6\gamma) = s_0 s_1 \cdots s_{62}, \tag{8}$$

where $\gamma = 102476232$ and $\alpha = 2$. Finally $\mathbf{s} =$

$$102476232204357464403615373306721656607542717705134525501263141. \tag{9}$$

Further let

$$\mathbf{s}^i = s_{62-i+1}s_{62-i}\cdots s_0 s_1 \cdots s_i s_{i+1}\cdots s_{62-i}$$

where $i \in \{0,\ 1,\ \ldots,\ 62\}$ and the subscripts are computed modulo 63, denote the PN sequence $\mathbf{s}$ shifted i places to the right. Let also

$$Q = \langle\{0,1,2,3,4,5,6,7\},\bullet\rangle,$$

be a quasigroup with operation $\bullet$ defined in Table 3.

Table 3: Operation Table in the Quasigroup Q

$\bullet$	0	1	2	3	4	5	6	7
0	4	5	7	1	6	0	2	3
1	3	2	0	6	1	7	5	4
2	5	3	6	7	0	1	4	2
3	0	1	2	3	4	5	6	7
4	6	0	3	5	2	4	7	1
5	1	7	4	2	5	3	0	6
6	7	6	5	4	3	2	1	0
7	2	4	1	0	7	6	3	5

A half of all NLPN sequences $\mathbf{s}(i) = \mathbf{s}\bullet\mathbf{s}^i$, where

$$i \in \{1,\ 2,\ \ldots,\ 62\}\setminus\{9,\ 18,\ 27,\ 36,\ 45,\ 54\},$$

obtained by means of the proposed method from the PN sequence $\mathbf{s}$ in Tables 4 and 5 is presented. One can get the other half of these sequences as $\mathbf{s}(i) = \mathbf{s}^i\bullet\mathbf{s}$ since the quasigroup Q is non-abelian. In this way one quasigroup of order 8 and one primitive polynomial of degree 2 over $GF(8)$ give 110 different NLPN sequences. Taking into account that the number of primitive polynomials of degree 2 over $GF(8)$ equals to 18, that the total number of loops of order 8 is equal to 535,281,401,856 [1], and that there are much more quasigroups of the same order, which are not loops, one may easily appreciate the importance of the proposed method for cryptograhic practice, where q is often of order of a few dozen or of several hundreds.

A *loop* $\langle L,\ +\rangle$ is a quasigroup with an identity element: that is, a quasigroup in which there exists an element $e\ \in\ L$ with the property that $e+x=x+e=x$ for every $x\ \in\ L$.

Table 4: A Half of the Set $\mathcal{S}_{\mathsf{NLPN}}$ Obtained from the PN Sequence (9) and the Quasigroup defined in Table 3

i	$\mathbf{s}(i)=\mathbf{s}\bullet\mathbf{s}^i$
1	255370427676426137260457507317320602122640144531715514303356601
2	153613266773050402764760163714244571223111705436350203407562552
3	263025074613217521224332645334055046103062611556404775377171076
4	650047642475242224416631133151007316562607557713747633250012023 5
5	513246520223341635434115006104576700553374246776271117267625300
6	027076306037221372507355423652026411074044335664411653711155762
7	274543315661640356215010470326674427131771352505070621356022743
8	356706013572701553663245674011416024725404653233121726102735047
10	705011710356255755370363776467042220412016456321452427633163140
11	001645433050047113572712554663275634010172123620374566734521627
12	771426667360111207312535367423756172430264504300501304654275251
13	106467324752172331773501405761703406215255341423566615432200706
14	661362516410474652122404073533301721600657255150767123574307342
15	210412103625154073236564224300741314156217033577557056360267467
16	757265155377377066367102210412505357424352062334264041601601413
17	303572651553624260674054312064621153713747560226017340137057214
19	435444056106143562050516613277777051362273665011573743023224012
20	232666741604071740251705732375206263167154470512361430325505134
21	452122330174514315061634456215151430327567326032607667005477720
22	033157117003532057554621277674163322063525054616636024727410441
23	172050553764236663711327014725060754237020263402435146455116317
24	766140201312546470323617122431170513405570730353675250672426564
25	400356275155431426076425140260366547316624712027731271030315573
26	331210372500356324652167441073540445760310317210255672124666775
28	525163673236570223400600344157104144572551513761660376213402277
29	724652022331034534305724601456261005471127647365337712616517005
30	221737250630762465202271116353433550170435766560146247314740510
32	054431571071165620565573042616732743021236210635542170706243374
33	473761402163775174014203521224402615333456137006162552057703665
34	536032465202264106453374560171031677565037102713447501222147653
35	322341164534445001601413265055372376777676001262772005115323456
37	615755361426737300130222462507465473652422300171134600563711754
38	417630614127066251037777375202230126354130551074345325061546246

Table 5: CONTINUATION OF TABLE 4

i	$s \bullet s^i$
39	637521223407615433157033104572652504664766743114002216521073507
40	712507476324602122331041543405613641457705115372026573665030672
41	207104562657503604277646061362117775114503207524623102331434355
42	551554704270633771462026725113667216520723431730033455204014166
43	623400735433106716104547750554710237673200422166525461517236123
44	314064237521273417635306157006007532751053724275463264166104521
46	165536132716661014720075251737636335202734027451041062473045425
47	560601357215005367426743417130212452506106364757322644270533711
48	120224411735313150706136572750557623276363150467203520410674644
49	464277763111322703025151764236523274301345403055216406076650157
50	730773534305720611356250055470424736466441221317110165620752326
51	602233007454360577171170627565534012617331634122240754535642061
52	111171045720525546732653630703122067250546672470612731464453033
53	367453440517130145627520536032764660704221176254530537171212630
55	075202244066304441510144135627511566032307771601227235753637536
56	676674170462023025113756246521227340635143016103313077552554470
57	016323752022410764533430711601354255055661467673700442762372115
58	577317031267452510417461652122343033534615620704756760251360024
59	426515547132657647003062037251645762375712274063054134012061331
60	134305600701407275755442326776315110261602536415724357426331260
61	062714625014753236521266300635447107007413542652153311775764203
62	370135726565567732616672703020135201736532445207644413150441102

For such values of q the number of quasigroups can be expressed as a factorial of astronomical number. Speaking more precisely, the number of quasigroups of order n equals to the number of latin squares of the same order $L(n)$, which, for $n > 10$ satisfies [5]

$$\prod_{k=1}^{n} k!^{\frac{n}{k}} \geq L(n) \geq \frac{n!^{2n}}{n^{n^2}}. \tag{10}$$

At last it may be interesting to see the autocorrelation functions of several NLPN sequences over $GF(8)$ and to compare them with autocorrelation functions of a PN sequence and of a random sequence. Therefore, one period of the autocorrelation function for all PN sequences $\mathbf{s}^i$ in Fig. 1 can be seen.

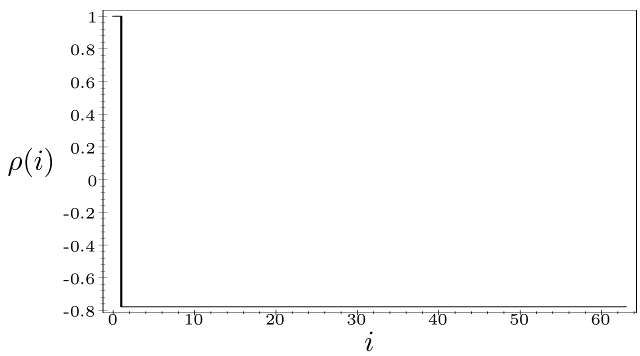

Figure 1: Autocorrelation function of all sequences $\mathbf{s}^i$

This function is of course the same for all PN sequences of length 63 over $GF(8)$, no matter which primitive polynomial of degree 2 over $GF(8)$ has been used.

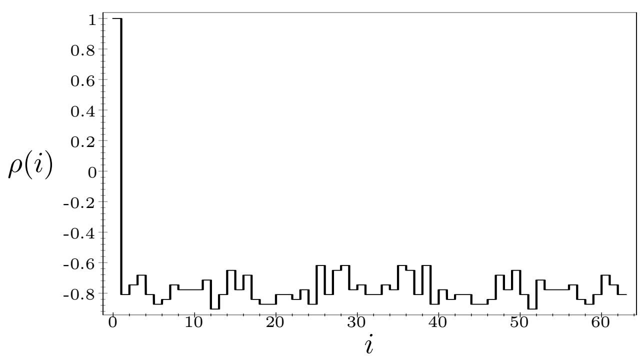

Figure 2: Autocorrelation function of the sequence $\mathbf{s}\bullet\mathbf{s}^{14}$

Figures 2, 3, 4 and 5 show one period of NLPN sequences $\mathbf{s}(i) = \mathbf{s} \bullet \mathbf{s}^i$ for $i = 14,\ 28,\ 42$ and 56, respectively, while one period of the autocorrelation function of truly random sequence of length 63 over $GF(8)$

$$\mathsf{413402332717176544257642215026016410750637616550600040162402102} \tag{11}$$

with the occurrence of elements

$$\mathsf{0} - 12,\ \mathsf{1} - 9,\ \mathsf{2} - 9,\ \mathsf{3} - 4,\ \mathsf{4} - 8,\ \mathsf{5} - 6,\ \mathsf{6} - 9,\ \mathsf{7} - 6$$

in Fig. 6 is presented.

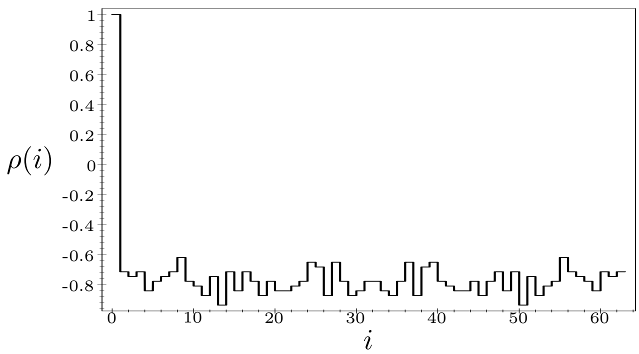

Figure 3: Autocorrelation function of the sequence $\mathbf{s}\bullet\mathbf{s}^{28}$

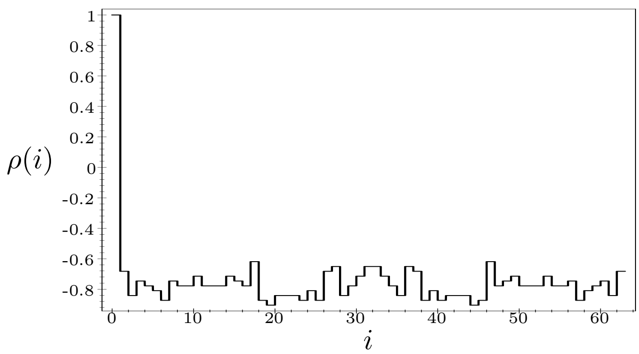

Figure 4: Autocorrelation function of the sequence $\mathbf{s}\bullet\mathbf{s}^{42}$

The autocorrelation function $\rho(i)$ is here defined as follows. Let A be the number of places where the sequence $s_0 s_1 \cdots s_{62}$ and its cyclic shift $s_i s_{i+1} \cdots s_{i-1}$ agree, and D the number of places where they disagree. Then

$$\rho(i) = \frac{A - D}{63}.$$

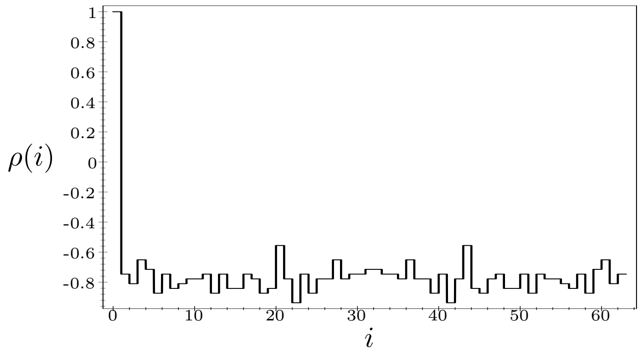

Figure 5: Autocorrelation function of the sequence $\mathbf{s}\bullet\mathbf{s}^{56}$

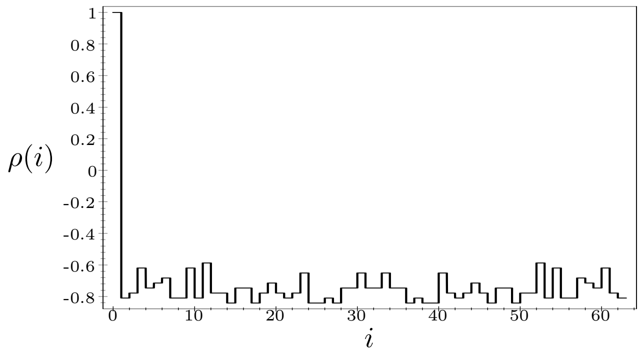

Figure 6: Autocorrelation function of the random sequence (10)

4. Example 2

In the same manner as in Example 1 the Tables of addition and multiplication in $GF(256) = \langle\{0,\ 1,\ \ldots,\ 255\}, +, \cdot\rangle$ were constructed using the primitive polynomial $x^8+x^4+x^3+x^2+1$ over $GF(2)$. Then the primitive polynomial $P(x) = x^3 + 132x^2 + 152x + 2$ over $GF(256)$ was found and the PN sequence $\mathbf{s}$ of length 16777215 was generated using the following recurrence relation over $GF(256)$

$$s_{i+3} = 132s_{i+2} + 152s_{i+1} + 2s_i, \quad i = 0,\ 1,\ \ldots,\ 16777214.$$

This sequence and its cyclic shift $\mathbf{s}^i$, i satisfying (5), was written to the disk files, say, $F1$ and $F2$. To create a disk file $F3$ containing NLPN sequence of length 16777215, as a quasigroup Q an isotope [1] of the additive group of $GF(256)$ was used. The generated NLPN sequence was then tested by means of the battery of DIEHARD tests of randomness [10], passing them all perfectly. Compared with the length of the NLPN sequence (16777215 Bytes), which may be used as a cryptographic key, to generate it one can use significantly smaller data, namely 65545 Bytes at most (addition table in the quasigroup Q, coefficients of the polynomial $P(x)$, three Bytes of initial condition for the recurrence relation and the number of places in the cyclic shift – about 0.39% of 16777215 Bytes). Since

$$7.53 \cdot 10^{102804} \geq L(256) \geq 3.04 \cdot 10^{101723},$$

it is evident that in a very easy way one can construct simple yet very good generators of cryptographic keys for universal stream-ciphers over the alphabet, containing 256 characters (ASCII code), using NLPN sequences.

5. Conclusions

In the paper only a tiny piece of the iceberg's tip of the possibilities, resulting from the application of quasigroups for generating the sequences of elements of $GF(q)$ with the desired complexity and degree of randomness is presented. E.g. by applying two PN sequences of the same length, but generated by the feedback shift registers, specified by two various primitive polynomials of the same degree, to the inputs of a quasigroup operator, an almost random non-linear sequence will appear on its output with an irregular, but flat distribution of elements and with a high degree of complexity (as, e.g, the sequence (11)). Furthermore, it is possible to combine different quasigroup operators with all linear and non-linear devices and to construct random $GF(q)$-element generators with controlled properties, having many various structures.

The method is especially convenient for fast software encryption. However, it also should be noted that there exists a large class of quasigroup operators which are easily implemented by means of binary logical circuits, appropriate for the implementation of very secure and extremely fast hardware-oriented quasigroup-based generalized stream-ciphers [6].

References

[1] **J. Dénes, A. D. Keedwell:** *Latin Squares and Their Applications*, Budapest, Akadémiai Kiadó, 1974.

[2] **J. Dj. Golić:** *On the Security of Nonlinear Filters Generators*, in D. Gollman (editor) Fast Software Encryption — Cambridge '96, LNCS, **1039** (1996). 173 – 188.

[3] **S. W. Golomb:** *Shift Register Sequences*, San Francisco: Holden Day, 1967.

[4] **S. M. Jennings:** *A Special Class of Binary Sequences*, PhD thesis, University of London, 1980.

[5] **M. T. Jacobson, P. Matthews:** *Generating Uniformly Distributed Random Latin Squares*, Journal of Combinatorial Designs **4** (1996), 405 – 437.

[6] **C. Kościelny:** *A Method of Constructing Quasigroup-Based Stream-Ciphers*, Applied Math. Comp. Sci. **6** (1996), 109 – 121.

[7] **R. Lidl, H. Niederreiter:** *Introduction to Finite Fields and Their Applications*, Cambridge University Press, 1986, 185 – 245.

[8] **F. J. MacWilliams, N. J. A. Sloane:** *Pseudo-Random Sequences and Arrays*, Proceedings of the IEEE, Vol. 64, NO 12, Dec. 1976, 1715 – 1729.

[9] **R. Rueppel:** *Analysis and Design of Stream Ciphers*, Springer Verlag, Berlin 1986.

[10] `http://stat.fsu.edu/~geo/diehard.html`

Technical University of Zielona Góra
Department of Robotics and Software Engineering
ul. Podgórna 50
65-246 Zielona Góra, Poland
e-mail: C.Koscielny@irio.pz.zgora.pl

or
Higher College of Engineering
ul. Jaworzyńska 151
59-220 Legnica
Poland

Received 15 December, 1997