Quasigroups and Related Systems **8** (2001), 1 – 6

On B-algebras and quasigroups

Jung R. Cho and Hee Sik Kim

Abstract

In this paper we discuss further relations between B-algebras and quasigroups.

1. Introduction

Y. Imai and K. Iséki introduced two classes of abstract algebras: BCK-algebras and BCI-algebras ([2, 3]). It is known that the class of BCK-algebras is a proper subclass of the class of BCI-algebras. In [4, 5] Q. P. Hu and X. Li introduced a wide class of abstract algebras: BCH-algebras. They have shown that the class of BCI-algebras is a proper subclass of the class of BCH-algebras. J. Neggers and H. S. Kim introduced in [8] the notion of d-algebras, i.e. algebras satisfying (1) $xx = 0$, (5) $0x = 0$, (6) $xy = 0$ and $yx = 0$ imply $x = y$, which is another useful generalization of BCK-algebras, and then they investigated several relations between d-algebras and BCK-algebras as well as some other interesting relations between d-algebras and oriented digraphs. Recently, Y. B. Jun, E. H. Roh and H. S. Kim introduced in [6] a new notion, called an BH-algebra, determined by (1), (2) $x0 = x$ and (6), which is a generalization of $BCH/BCI/BCK$-algebras. They also defined the notions of ideals and boundedness in BH-algebras, and showed that there is a maximal ideal in bounded BH-algebras. J. Neggers and H. S. Kim introduced in [9] and investigated a class of algebras which is related to several classes of algebras of interest such as $BCH/BCI/BCK$-algebras and which seems to have rather nice properties without being excessively complicated otherwise. In this paper we discuss further relations between B-algebras and other topics, especially quasigroups. This is a continuation of [9].

2000 Mathematics Subject Classification: 06F35, 20N05
Keywords: B-algebra, quasigroup, cancellation

2. Preliminaries

A *B-algebra* is a non-empty set X with a constant 0 and a binary operation "$\cdot$" (denoted by juxtaposition) satisfying the following axioms:

(1) $xx = 0$,

(2) $x0 = x$,

(3) $(xy)z = x(z(0y))$

for all $x, y, z \in X$.

Example 2.1. It is easy to see that $X = \{0, 1, 2, 3, 4, 5\}$ with the multiplication:

$\cdot$	0	1	2	3	4	5
0	0	2	1	3	4	5
1	1	0	2	4	5	3
2	2	1	0	5	3	4
3	3	4	5	0	2	1
4	4	5	3	1	0	2
5	5	3	4	2	1	0

is a B-algebra.

The following result is proved in [9].

Proposition 2.2. *If $(X; \cdot, 0)$ is a B-algebra, then*

(i) $x(yz) = (x(0z))y$,

(ii) $(xy)(0y) = x$,

(iii) $xz = yz$ *implies* $x = y$

for all $x, y, z \in X$.

A B-algebra $(X; \cdot, 0)$ is said to be 0-*commutative* if $x(0y) = y(0x)$ for any $x, y \in X$.

The B-algebra from the above example is not 0-commutative, since we have $3 \cdot (0 \cdot 4) = 2 \neq 1 = 4 \cdot (0 \cdot 3)$. A simple example of a 0-commutative B-algebra is a Boolean group. It is not difficult to see that a B-algebra is a Boolean group iff it satisfies one from the following identities: $0x = x$, $xy = yx$, $(xy)z = x(yz)$.

3. B-algebras and quasigroups

Lemma 3.1. *Let* $(X;\cdot,0)$ *be a* B*-algebra. Then for all* $x,y\in X$

(i) $xy=0$ *implies* $x=y$,

(ii) $0x=0y$ *implies* $x=y$,

(iii) $0(0x)=x$.

Proof. (i) Trivially follows from Proposition 2.2 (iii) and the fact that $0=yy$.

(ii) If $0x=0y$, then

$$0=xx=(xx)0=x(0(0x))=x(0(0y))=(xy)0=xy\,,$$

and hence $x=y$ by (i).

(iii) For any $x\in X$, since $0x=(0x)0=0(0(0x))$ by (ii), we have $x=0(0x)$. □

Theorem 3.2. *In any* B*-algebra the left cancellation law holds.*

Proof. Assume that $xy=xz$. Then $0(xy)=0(xz)$. By Proposition 2.2 (i), we obtain that $(0(0y))x=(0(0z))x$. By Lemma 3.1 (iii) we have $yx=zx$. Hence $y=z$ by Proposition 2.2 (iii). □

Let L_a and R_a be the *left* and *right* translation of X (respectively), i.e. let $L_a(x)=ax$ and $R_a(x)=xa$ for all $x\in X$.

Lemma 3.3. *If* $(X;\cdot,0)$ *is a* B*-algebra, then*

(i) L_0 *is a bijection,*

(ii) $R_0=R_0^{-1}=id_X$,

(iii) L_a *and* R_a *are injective for all* $a\in X$,

(iv) $L_0^{-1}(0\cdot x)=L_0^{-1}(L_0(x))=x$ *and*
$0\cdot(L_0^{-1}(x))=L_0(L_0^{-1}(x))=x$ *for* $x\in X$.

Proof. (i) Since $0(0x)=x$, $L_0^2=id_X$ and so L_0 is a bijection.

(ii) is a consequence of (2).

(iii) follows from Proposition 2.2 (iii) and Theorem 3.2. □

Lemma 3.4. L_a *and* R_a *are surjective for all* $a\in X$.

Proof. Let $c \in X$. Putting $b = (L_0^{-1}(c)) \cdot (0 \cdot a)$, we obtain

$$\begin{aligned} L_a(b) &= L_a(L_0^{-1}(c) \cdot (0 \cdot a)) = a \cdot (L_0^{-1}(c) \cdot (0 \cdot a)) \\ &= (a \cdot a) \cdot (L_0^{-1}(c))) = 0 \cdot (L_0^{-1}(c)) = c. \end{aligned}$$

Thus L_a is surjective.

Similarly, for $b = c \cdot (L_0^{-1}(a))$ we have

$$\begin{aligned} R_a(b) &= R_a((c \cdot (L_0^{-1}(a)) = (c \cdot (L_0^{-1}(a))) \cdot a \\ &= (c \cdot (L_0^{-1}(a))) \cdot (0 \cdot (L_0^{-1}(a))) = c. \end{aligned}$$

by Proposition 2.2 (ii). Hence R_a is surjective. □

Theorem 3.5. *Every B-algebra is a quasigroup.*

Proof. By Lemma 3.3 (iii) and Lemma 3.4. □

Proposition 3.6. *A B-algebra $(X; \cdot, 0)$ satisfies the identity $(yx)x = y$ if and only if it is a loop and 0 is its neutral element.*

Proof. If a B-algebra $(X; \cdot, 0)$ satisfies the identity $(yx)x = y$, then putting $y = 0$ in this identity we have $(0x)x = 0$, which by Lemma 3.1 (i) gives $0x = x$. Hence 0 is the neutral element of $(X; \cdot, 0)$. By Theorem 3.5 $(X; \cdot, 0)$ is a loop.

Conversely, if 0 is the neutral element of a B-algebra $(X; \cdot, 0)$, then

$$(yx)x = y(x(0x)) = y(xx) = y0 = y$$

for all $x, y \in X$. This proves the proposition. □

Theorem 3.7. *A B-algebra satisfies the identity $x(xy) = y$ if and only if it is 0-commutative.*

Proof. If a B-algebra $(X; \cdot, 0)$ satisfies the identity $x(xy) = y$, then

$$\begin{aligned} (x(0y))y &= x(y(0(0y))) = x(yy) = x0 = x = y(yx) \\ &= y(y(0(0x))) = (y(0x))y\,. \end{aligned}$$

Hence we have $(x(0y))y = (y(0x))y$. Then, by the right cancellation law, we obtain $x(0y) = y(0x)$.

The converse statement is proved in [9]. □

Remark. A B-algebra satisfying the identity $x(xy) = y$ is not, in general, a loop. Indeed, if $(G, +, 0)$ is an abelian group, then G with the operation $x \cdot y = x - y$ is an example of a 0-commutative B-algebra, which satisfies this identity but it is not a loop.

References

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

[2] **Q. P. Hu and X. Li** *On BCH-algebras*, Math. Seminar Notes **11** (1983), 313 – 320.

[3] **Q. P. Hu and X. Li**: *On proper BCH-algebras*, Math. Japon. **30** (1985), 659 – 661.

[4] **K. Iséki and S. Tanaka**: *An introduction to theory of BCK-algebras*, Math. Japon. **23** (1978), 1 – 26.

[5] **K. Iséki**: *On BCI-algebras*, Math. Seminar Notes **8** (1980), 125 – 130.

[6] **Y. B. Jun, E. H. Roh and H. S. Kim**: *On BH-algebras*, Sci. Mathematicae **1** (1998), 347 – 354.

[7] **J. Meng and Y. B. Jun**: *BCK-algebras*, Kyung Moon Sa Co., Seoul 1994.

[8] **J. Neggers and H. S. Kim**: *On d-algebras*, Math. Slovaca **49** (1999), 19 – 26.

[9] **J. Neggers and H. S. Kim**, *On B-algebras*, (submitted)

[10] **J. Neggers and H. S. Kim**, *A fundamental theorem of B-homomorphism for B-algebras*, Inter. Math. J. **2** (2002), (to appear)

Jung R. Cho
Department of Mathematics
Pusan National University
Pusan 609-735, Korea
jungcho@hyowon.pusan.ac.kr

Received March 21, 2001

Hee Sik Kim
Department of Mathematics
Hanyang University
Seoul 133-791, Korea
heekim@hanyang.ac.kr

Quasigroups and Related Systems **8** (2001), 7 – 14

Non-associative algebraic system in cryptology. Protection against "meet in the middle" attack

József Dénes and Tamás Dénes

Abstract

In this paper we shall mention an algorithm of zero knowledge proof based on Latin squares. We shall define the $DL_m(n)$ type Latin squares, which have a further property that is stronger than the pan-Hamiltonian squares: Every pair of $DL_m(n)$ rows and columns is a cycle of length n, if n is prime.

1. Basic notions

In general the cryptology is based on fields which are commutative and associative. There is a method which studies the evolution of differences during encryption of pairs of plaintexts, and derives the most likely keys from a pool of many pairs. It is called differential cryptanalysis. Differential cryptanalysis can also be used to find collisions in "hash" functions. For DES (Data Encryption Standard) like cryptosystems the differences are usually in terms of exclusive or of the intermediate data in the pair. Differential cryptanalysis might apply "meet in the middle attack" (introduced in [2]).

Definition 1.1. *Meet in the Middle Attack*: An attack in which the evolution of the data is studied from both directions: from the plaintext forwards towards an intermediate round and from the ciphertext backwards towards the same intermediate round. If the results at the intermediate round are not the same in both directions, then the tested value of the key is not the real value. If both results are the same in several encryptions, then the tested value of the key is the real value with high probability.

2000 Mathematics Subject Classification: 20N05
Keywords: Latin square, pan-Hamiltonian square, permutations, cryptology, zero knowledge proof

Details in cryptography one can learn e.g. [14]. The Latin squares are the tools for generalizations of finite field (see [6]).

Definition 1.2. A finite set J on which two binary operations are defined $(+)$ and $(\bullet)$ such J is a loop with respect to the operation $(+)$ with identity element 0 say, $J\backslash\{0\}$ is a group with respect to the operation $(\bullet)$ and for which for all $a, b, c \in J$ the following distributive laws

$$a(b+c) = ab + ac \quad \text{and} \quad (b+c)a = ba + ca$$

hold, is called a *neofield*.

A neofield is not necessarily commutative or associative. Neofields can be applied in cryptology (see [6]). Neofields were first introduced by L. J. Paige in 1949. In [3] the applications of algebraic systems without associativity and commutativity has been predicted to apply in the future.

The number of Latin squares without associativity and commutativity is much larger than group tables (see e.g. [1]).

The cryptosystems based on quasigroups are as follows: equipment of hardware encryption (patent [8], theoretical construction [4], [7]), hash function (see [5]), transposition cipher (see [10]) and Hamming distances (see [11]). A cipher system based on neofield (see [6]).

In the remaining part of the this paper we shall mention an algorithm of zero knowledge proof based on Latin squares.

2. Zero knowledge protocol

The classical method of authenticating a person by means of a machine is the use of a password (PIN number). There are many problems involved with the improper use of passwords. More sophisticated than simple passwords the challenge-and-response protocol.

It's hard to believe, but procedures exist that enable user A to convince user B that he knows a secret without giving B the faintest idea of what the secret is. Such procedures are naturally enough called *zero knowledge protocols*.

Jean-Jacques Quisquater and Louis Guillou explain zero-knowledge with a story about a cave (see [13]). The cave, illustrated in Figure 1. has a secret.

Someone who knows the magic words can open the secret door between C and D. To everyone else, both passages lead to dead ends.

Peggy knows the secret of the cave. She wants to prove her knowledge to Victor, but she doesn't want to reveal the magic words. Here's how she convinces him:

(1) Victor stands at point A.
(2) Peggy walks all the way into the cave, either to point C or point D.
(3) After Peggy has disappeared into the cave, Victor walks to point B.
(4) Victor shouts to Peggy, asking her either to:
    (a) come out of the left passage or
    (b) come out of the right passage.
(5) Peggy complies, using the magic words to open the secret door if she has to.
(6) Peggy and Victor repeat steps (1) through (5) n times.

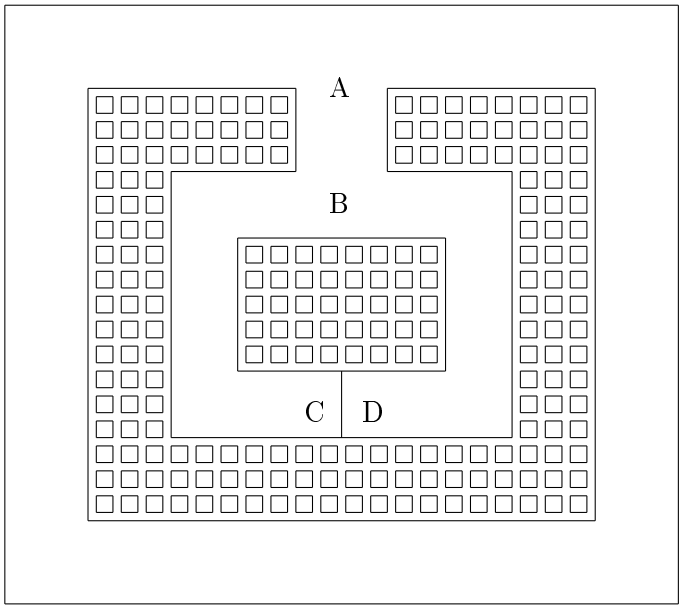


Figure 1.

3. DD algorithm

Assume the users $(u_1, u_2, ..., u_k)$ form a network. u_i has public-key L_{u_i}, L'_{u_i} (denote two isotopic Latin squares at order n and secret-key I_{u_i} (denotes the isotopism of L_{u_i} upon L'_{u_i}). u_i wants to prove identity for u_j but he

doesn't want to reveal the secret-key (zero-knowledge proof).

1. u_i randomly permutes L_{u_i} to produce another Latin square H.
2. u_i sends H to u_j.
3. u_j asks u_i either to:
   a. prove that H and L'_{u_i} are isotopic,
   b. prove that H and L_{u_i} are isotopic.
4. u_i complies. He either
   a. prove that H and L'_{u_i} are isotopic,
   b. prove that H and L_{u_i} are isotopic.
5. u_i and u_j repeat steps 1. through 4. n times.

One of the present authors gave a lecture on DD Algorithm in 1996 at USC (Los Angeles), Prof L. Welch made a comment. Prof L. Welch said that the security of the scheme varying on Latin squares which used as a public-keys. Strongest so called pan-Hamiltonian Latin squares. Pan-Hamiltonian Latin squares are introduced by J. Wanless (see [15]).

Definition 3.1. A Latin square L at order n is a *pan-Hamiltonian* if every row cycle of L has length n.

Pan-Hamiltonian squares have applications besides the cryptography in the combinatorics. These squares have no proper subrectangles.

Pan-Hamiltonian Latin squares has been called a C-type Latin squares (see [7]). When n is not prime, a C-type $n \times n$ Latin square cannot be a group table. For all $n \geqslant 7$ there exists a C-type Latin square of order n that is not group table (see [7]).

Infinitely many values of p prime ($p \geqslant 11$ and $p \equiv 2(mod\ 3)$) there exists a C-type Latin square of order p which cannot based on a group (see [7]).

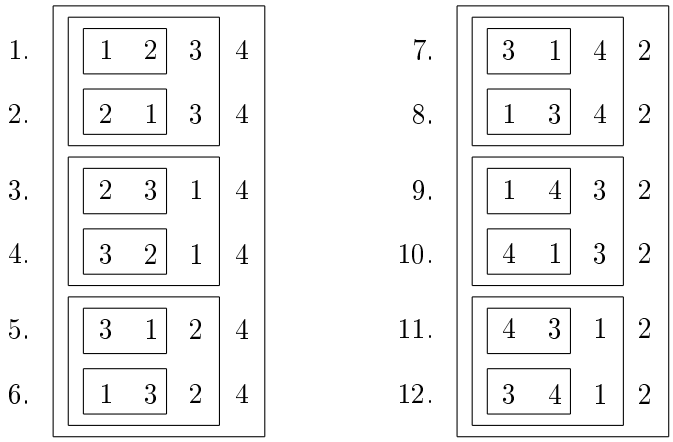
In [12] gave what is believed to be the first published example of a symmetric 11×11 Latin square (see Figure 2.) which, although not cyclic, has the property that the permutation between any two rows is an 11-cycle. In [12] there was proved how this 11×11 Latin square can be obtained by a general construction for $n \times n$ Latin square where n is prime with $n \geqslant 11$.

$$\mathbf{L} = \begin{array}{cccccccccccc} 0^* & 1^* & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 \\ 1^* & 6^* & 3 & 5 & 9 & 10 & 0 & 2 & 8 & 4 & 7 \\ 2 & 3 & 1 & 6 & 10 & 7 & 9 & 0 & 4 & 5 & 8 \\ 4 & 5 & 6 & 2 & 1^* & 9 & 3 & 7 & 0^* & 8 & 10 \\ 8 & 9 & 10 & 1 & 4 & 2 & 7 & 6 & 3 & 0 & 5 \\ 5 & 10 & 7 & 9 & 2^* & 8 & 4 & 3 & 1^* & 6 & 0 \\ 10 & 0 & 9 & 3 & 7 & 4 & 5 & 8 & 6 & 2 & 1 \\ 9 & 2 & 0 & 7 & 6 & 3 & 8 & 10 & 5 & 1 & 4 \\ 7 & 8 & 4 & 0 & 3 & 1 & 6 & 5 & 9 & 10 & 2 \\ 3 & 4 & 5 & 8 & 0 & 6 & 2 & 1 & 10 & 7 & 9 \\ 6 & 7 & 8 & 10 & 5 & 0 & 1 & 4 & 2 & 9 & 3 \end{array}$$

Figure 2.

One of the present authors introduced an algorithm in [9]. (This algorithm has been called DT algorithm.) The DT algorithm lexicography listed all elements of the symmetric group of degree n (S_n) $(\pi_1, \pi_2, ..., \pi_{n!} \in S_n)$.

DT algorithm can be demonstrated $(n = 4)$ in Figure 3.



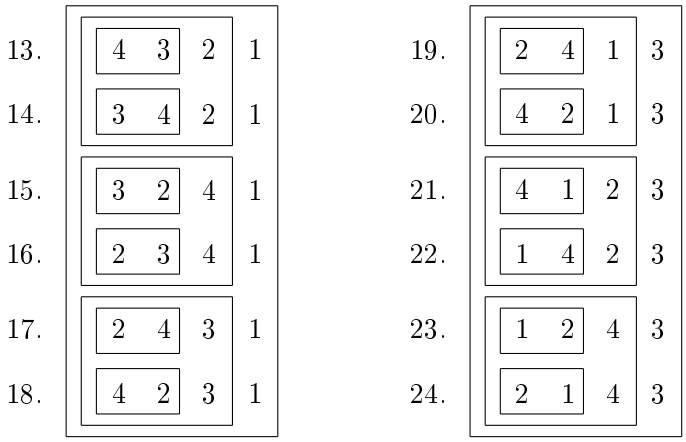


Figure 3.

The correspondence one to one the permutations of degree n and natural numbers 1 to $n!$. DT algorithm has the property for arbitrary natural number $1 \leqslant m \leqslant (n-1)!$ there corresponds a single subset of S_n containing n permutations, which are the rows of a Latin square of order n (see (1)). These Latin squares (denote $DL_m(n)$) uniquely determines the row permutations as follows:

$$DL_m(n) = \begin{bmatrix} \pi_m \\ \pi_{(n-1)!+m} \\ \pi_{2(n-1)!+m} \\ \cdot \\ \cdot \\ \cdot \\ \pi_{(n-1)(n-1)!+m} \end{bmatrix} \qquad 1 \leqslant m \leqslant (n-1)! \qquad (1)$$

A subset of Latin squares $DL_m(n)$ of order n will defined by two parameters (n, m). Consequently to store or transmission of the Latin square is not necessarily the original matrix. Similarly to this property is really applicable to zero-knowledge-proof in the cryptography.

Applying the Wilson theorem (*If p is prime number, then* $(p-1)!+1 \equiv 0(mod\, p)$) to the DT algorithm (see [9]), then we have the next theorem:

Theorem 1. *If p is prime number, then the $DL_m(p)$ are pan-Hamiltonian squares.*

Example 1. $n = 5$ and $m = 1$

$$DL_1(5) = \begin{bmatrix} \pi_1 \\ \pi_{25} \\ \pi_{49} \\ \pi_{73} \\ \pi_{97} \end{bmatrix} = \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \\ 4 & 5 & 2 & 3 & 1 \\ 5 & 3 & 4 & 1 & 2 \\ 3 & 1 & 5 & 2 & 4 \end{array}$$

Example 2. $n = 5$ but the Latin square is not $DL_m(n)$ type:

$$L(5) = \begin{bmatrix} \pi_1 \\ \pi_{43} \\ \pi_{67} \\ \pi_{88} \\ \pi_{114} \end{bmatrix} = \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \\ 5 & 3 & 4 & 2 & 1 \\ 3 & 4 & 1 & 5 & 2 \\ 2 & 1 & 5 & 3 & 4 \end{array}$$

$$\pi_{43} = \begin{pmatrix} 1\,4 \\ 4\,1 \end{pmatrix}\begin{pmatrix} 2\,3\,5 \\ 5\,2\,3 \end{pmatrix} \qquad \pi_{67} = \begin{pmatrix} 1\,5 \\ 5\,1 \end{pmatrix}\begin{pmatrix} 2\,3\,4 \\ 3\,4\,2 \end{pmatrix}$$

$$\pi_{88} = \begin{pmatrix} 1\,3 \\ 3\,1 \end{pmatrix}\begin{pmatrix} 2\,4\,5 \\ 4\,5\,2 \end{pmatrix} \qquad \pi_{114} = \begin{pmatrix} 1\,2 \\ 2\,1 \end{pmatrix}\begin{pmatrix} 3\,4\,5 \\ 5\,3\,4 \end{pmatrix}$$

From the point of view of cryptology the $DL_m(n)$ type Latin squares have a further property that is stronger than the pan-Hamiltonian squares: *Every pair of* $DL_m(n)$ *rows* (*and columns, its number* $k = \begin{pmatrix} n \\ 2 \end{pmatrix}$) *is a cycle of length* n (see [9]).

References

[1] **R. E. Cawagas**: *Generation of NAFIL loops of small order*, Quasigroups and Related Systems **7** (2000), $1 - 5$.

[2] **D. Chaum and J.-H. Evertse**: *Cryptanalysis of DES with a reduced number of rounds, Sequences of linear factors in block ciphers*, Lecture Notes in Computer Science, Advances in Cryptology, Proceedings of CRYPTO'85, Springer 1985, $192 - 211$.

[3] **J. Dénes**: *Some thoughts on the decryption possibilities at encryption messages*, (Hungarian), Híradástechnika **7** (2001), $21 - 26$.

[4] **J. Dénes**: *On latin squares and digital encrypting communication system*, (to appear in P.U.M.A).

[5] **J. Dénes and A. D. Keedwell**: *A new authentication scheme based on Latin squares*, Discrete Math. **106/107** (1992), 157 – 161.

[6] **J. Dénes and A. D. Keedwell**: *Some applications of non associative algebraic system in cryptology*, (to appear in P.U.M.A.)

[7] **J. Dénes and P. J. Owens**: *Some new Latin power sets not based on groups*, J. Comb. Theory, Ser. A. **85** (1999), 69 – 82.

[8] **J. Dénes and P. Petroczki**: *Digitális titkosító kommunikációs rendszer, (A Digital Encrypting Communication System)*, Hungarian patent No. 201437 A.

[9] **T. Dénes**: *Algorithm to the generation of all permutations of degree n*, (Hungarian), Információ Elektronika **1-2** (1975).

[10] **T. Dénes**: *Cardano and the cryptography. Mathematics of the enciphering grill*, (Hungarian), Középiskolai Matematikai és Fizikai Lapok **6** (2001), 325 – 335.

[11] **A. Drapal**: *Hamming distances of groups and quasigroups*, Discrete Math. **235** (2001), 189 – 197.

[12] **P. J. Owens and D. A. Preece**: *Some new non-cyclic Latin squares that have cyclic and Youden properties*, Ars Combinatorica **44** (1996), 137 – 148.

[13] **J.-J. Quisquater and L. C. Guillou**: *De procédés d'authentification basés sur une publication de problémes complexes et personnalisés dont les solutions maintenues secrétes constituent autant d'accréditations*, (French), Proc. of SECURI-COM'89, 7th Worldwide Congress on Computer and Communications Security and Protection, Société d'Édition et d'Organisation d'Expositions Professionnelles, 1989, 149 – 158.

[14] **G. J. Simmons**: *Contemporary cryptology*, IEEE Press, New York 1992.

[15] **J. Wanless**: *Perfect factorisations of bipartite graphs and Latin squares without proper subrectangles*, Electronic J. Combinatorics **6** (1999), #R9.

Received November 5, 2001

József Dénes: 1122 Budapest, Csaba u. 10, Hungary
Tamás Dénes: 1182 Budapest, Marosvásárhely u. 13/a, Hungary

Quasigroups and Related Systems **8** (2001), 15 – 36

On some old and new problems in n-ary groups

Wiesław A. Dudek

Abstract

In this paper some old unsolved problems connected with skew elements in n-ary groups are discussed.

1. Introduction

A nonempty set G together with one n-ary operation $f : G^n \longrightarrow G$ is called an *n-ary groupoid* and is denoted by $\langle G, f\rangle$. We say that this groupoid is *i-solvable* or *solvable at the place i* if for all $a_1, ..., a_n, b \in G$ there exists $x_i \in G$ such that

$$f(a_1, ..., a_{i-1}, x_i, a_{i+1}, ..., a_n) = b\,. \tag{1}$$

If this solution is unique, we say that this groupoid is *uniquely i-solvable*. An n-ary groupoid which is uniquely i-solvable for every $i = 1, 2, \ldots, n$ is called an *n-ary quasigroup* or *n-quasigroup* (cf. [3]).

We say that an n-ary groupoid $\langle G, f\,\rangle$ is *(i, j)-associative* if

$$f(a_1, ..., a_{i-1}, f(a_i, ..., a_{i+n-1}), a_{i+n}, ..., a_{2n-1}) \\ = f(a_1, ..., a_{j-1}, f(a_j, ..., a_{j+n-1}), a_{j+n}, ..., a_{2n-1}),$$

holds for all $a_1, \ldots, a_{2n-1} \in G$. If an n-ary operation is (i, j)-associative for every $i, j \in \{1, \ldots, n\}$, then it is called *associative*. An n-ary groupoid with an associative operation is called an *n-ary semigroup* or *n-semigroup*. An n-semigroup which is also an n-quasigroup is called an *n-ary group* (briefly: *n-group*) or a *polyadic group* (cf. [31]) .

2000 Mathematics Subject Classification: 20N15, 08N05

Keywords: n-ary group, skew element, variety

This paper is an extended version of my talk given at the First Conference of the Mathematical Society of the Republic of Moldova, Kishinev, August 16-18, 2001.

For $n = 2$ it is an ordinary group. For infinite n, where n is a countable infinite number, it is an *infinitary* group. Unfortunately all such groups are trivial (have only one element), but there are non-trivial infinitary quasigroups and semigroups (cf. [4]). In connection with this we assume throughout the whole text that $3 \leqslant n < \infty$.

The first idea of such generalization of groups was presented by E. Kasner in the lecture at the fifty-third annual meeting of the American Association for the Advancement of Science, reported by L. G. Weld in The Bulletin of the American Mathematical Society in 1904 (cf. [25]), but the first formal definition was given by W. Dörnte in the paper [6] based on his dissertation prepared under the inspiration of E. Noether.

Sets with one n-ary operation having different properties were investigated by many authors. For example, J. Certaine [5] and D. H. Lehmer [27] described some natural *ternary* (i.e. $n = 3$) operations defined on a group. Some ternary groupoids having interesting applications to projective and affine geometry were considered by R. Baer [2], H. Prüfer [32], A. K. Sushkevich [39] and V. V. Vagner [41]. Ternary quasigroups are used in [37] and [38] to the characterization of Mendelsohn and Steiner quadruple systems.

On the other hand, G. A. Miller [28] described sets of group elements involving only products of more than n elements. Some n-ary operations have interesting applications in physics. For example, Y. Nambu [29] proposed in 1973 the generalization of classical Hamiltonian mechanics based on the Poisson bracket to the case when the new bracket, now called the *Nambu bracket*, is an n-ary operation on classical observables. The author of [40] suspects that different n-ary structures such as n-Lie algebras, Lie ternary systems and linear spaces with additional internal n-ary operations, might clarify many important problems of modern mathematical physics (Yang-Baxter equation, Poisson-Lie groups, quantum groups). For example, ternary Z_3–graded algebras are important (cf. [26]) for their applications in physics of elementary interactions. Unfortunately, from the mathematical point of view all such structures are rather complicated, especially for $n > 3$.

The above definition of an n-ary group is a generalization of H. Weber's formulation of axioms of groups. Similar generalization of L. E. Dickson's axioms one leads to n-ary groups $\langle G, f \rangle$ *derived from a group* $\langle G, \cdot \rangle$, i.e. to n-ary groups with the operation

$$f(x_1, x_2, \ldots, x_n) = x_1 \cdot x_2 \cdot \ldots \cdot x_n$$

(cf. [1] and [33]). But for every $n \geqslant 3$ there are n-groups which are not

derived from any group (cf. [6], [9], [10]).

E. L. Post observed in [31] that under the assumption of the n-ary associativity it suffices only to postulate the existence of the solution of (1) at the place $i = 1$ and $i = n$, or at one place i other than 1 and n. Then one can prove uniqueness of the solution of (1) for all $i = 1, 2, \ldots, n$.

Also the assumption on the associativity can be given in the weaker form. For example, in [18] the following theorem is proved.

Theorem 1. (Dudek, Głazek, Gleichgewicht 1977) *An n-ary groupoid $\langle G, f \rangle$ is an n-ary group if and only if (at least) one of the following conditions is satisfied:*

a) the $(i, i+1)$-associative law holds for some $i \in \{2, \ldots, n-2\}$ and the equation (1) is uniquely solvable for i and some $k > i$,

b) the $(1, 2)$-associative law holds and the equation (1) is solvable for $i = n$ and uniquely solvable for $i = i$,

c) the $(n-1, n)$-associative law holds and the equation (1) is solvable for $i = 1$ and uniquely solvable for $i = n$.

The class of n-ary groups can be characterized also as the class of n-ary semigroups with two binary operations satisfying two simple identities, or as the class of n-ary semigroups in which some two equations containing only two variables are solvable (cf. [13]).

2. Skew elements and endomorphisms

According to the definition of an n-ary group $\langle G, f \rangle$ for every $x \in G$ there exists only one $z \in G$ such that

$$f(x, ..., x, z) = x\,.$$

This element is called *skew* to x and is denoted by $\bar{x}$. Since for every $x \in G$ there exists only one $\overline{x}$, the above equation induces on G the new unary operation $^{-}\colon x \to \bar{x}$. This means that an n-ary group $\langle G, f \rangle$ can be considered as an algebra $\langle G, f, ^{-} \rangle$ of type $(n, 1)$ with two fundamental operations: an n-ary one f and an unary one $^{-}\colon x \to \bar{x}$, which gives some analogy with the binary case when a group is considered as an algebra $\langle G, \cdot, ^{-1} \rangle$ of type $(2, 1)$. In a binary group we have $xe = x$ for all x and some fixed e. For $n = 3$ this identity can be generalized to the form $f(x, e, e) = x$

or $f(x,x,e)=x$. The first form, for a ternary group derived from a binary group $\langle G,\cdot\rangle$, implies that e is the neutral element of $\langle G,\cdot\rangle$, the second – that e is the inverse of x (in $\langle G,\cdot\rangle$, obviously). Thus, in some sense, the skew element is a common generalization of the identity and the inverse element of a binary group.

In n-ary groups derived from binary groups we have $\bar{x}=x^{2-n}$ and

$$f(y,x,\ldots,\bar{x},\ldots,x)=f(x,\ldots,\bar{x},\ldots,x,y)=y \tag{2}$$

for all x,y, where $\bar{x}$ can appear at any place under the sign of the n-ary operation. This shows that in an n-ary group derived from a group $\langle G,\cdot\rangle$ of the exponent $n-2$ the neutral element of $\langle G,\cdot\rangle$ is skew to every $x\in G$. In an n-ary group derived from a group $\langle G,\cdot\rangle$ of the exponent $n-3$ we have $\bar{x}=x^{-1}$ and $\bar{x}\neq\bar{y}$ for all $x\neq y$. If the exponent of $\langle G,\cdot\rangle$ is equal to $n-1$, then $\bar{x}=x$ for all $x\in G$.

An element $x=\bar{x}$ is called *idempotent*. It is also defined by the equation $f(x,\ldots,x)=x$. For every $n\geqslant 3$ there are n-ary groups without idempotents and n-ary groups in which only some elements are idempotent (cf. [10]). A group in which all elements are idempotent is called an *idempotent group*.

The operation $^-\colon x\to\bar{x}$ plays an important role in the theory of n-ary groups and in their applications to affine geometry (cf. [21] and [35]). This operation can be used also to the definition of n-ary groups (cf. [23] and [18]). The minimal axioms system defining of n-ary groups is given in the following theorem proved in [8].

Theorem 2. (Dudek 1980) *The class of n-ary groups $\langle G,f\rangle$ coincides with the variety of all $(1,2)$-associative n-ary groupoids $\langle G,f\rangle$ with an additional unary operation $^-\colon x\to\bar{x}$ satisfying the identity (2), where $\bar{x}$ appears at one fixed place.*

It is not difficult to see that in an n-ary group $\langle G,f\rangle$ derived from a commutative group the following identity holds:

$$\overline{f(x_1,x_2,\ldots,x_n)}=f(\bar{x}_1,\bar{x}_2,\ldots,\bar{x}_n)\,. \tag{3}$$

It holds also in the non-commutative 8-group derived from the group S_3 and in every idempotent n-group. For $x_1=x_2=\ldots=x_n=x$ it is satisfied in any n-ary group.

From the proof of Theorem 3 in [22] it immediately follows that this identity holds in all *medial* (in the sense of Belousov [3]) n-ary groups, i.e.

in all n-ary groups in which the identity

$$f(f(x_{11},x_{12},\ldots,x_{1n}),f(x_{21},x_{22},\ldots,x_{2n}),\ldots,f(x_{n1},x_{n2},\ldots,x_{nn}))$$
$$= f(f(x_{11},x_{21},\ldots,x_{n1}),f(x_{12},x_{22},\ldots,x_{n2}),\ldots,f(x_{1n},x_{2n},\ldots,x_{nn}))$$

is satisfied. For $n = 2$ it is the standard medial (entropic) law, which in the case of groups gives the commutativity. For $n \geqslant 3$ it not implies the commutativity of n-ary groups.

Since an n-ary group $\langle G, f\rangle$ is medial if and only if there exists $a \in G$ such that $f(x,a,\ldots,a,y) = f(y,a,\ldots,a,x)$ for all $x,y \in G$ (cf. [8]), the Hosszú theorem (cf. [24]) suggests the following result proved in [10].

Theorem 3. (Dudek 1988) *If for an n-ary group $\langle G, f\rangle$ there exists a commutative group $\langle G,+\rangle$, an element $b \in G$, and an automorphism φ of $\langle G,+\rangle$ such that $\varphi(b) = b$, $\varphi^{n-1}(x) = x$ for all $x \in G$ and*

$$f(x_1,x_2,\ldots,x_n) = x_1 + \varphi(x_2) + \varphi^2(x_3) + \ldots + \varphi^{n-2}(x_{n-1}) + x_n + b\,,$$

then (3) *is satisfied.*

Unfortunately the converse statement is not true.

In connection with this the following problem was posed in [10].

Problem 1. *Describe the class of all n-ary groups satisfying* (3)*, i.e. the class of n-ary groups for which $h(x) = \bar{x}$ is an endomorphism.*

For $n = 3$ the answer is simple, because as proved W. Dörnte (cf. [6]) in all ternary groups we have $\overline{f(x,y,z)} = f(\bar{z},\bar{y},\bar{x})$. This means that a ternary group satisfies (3) if and only if it is medial.

For $n > 3$ the problem is open. We know only the partial answer basing on the general connections between homomorphisms of n-ary groups and homomorphisms of their retracts (Theorem 2 from [20]).

Theorem 4. *A mapping $h : G \to G$ is an endomorphism of an n-ary group $\langle G, f\rangle$ if and only if there exists $a \in G$ such that*

(*i*) $h(f(x,a,\ldots,a,y)) = f(h(x),b,\ldots,b,h(y))$,

(*ii*) $h(f(\bar{a},x,a,\ldots,a)) = f(\bar{b},h(x),b,\ldots,b)$,

(*iii*) $h(f(\bar{a},\bar{a},\ldots,\bar{a})) = f(\bar{b},\bar{b},\ldots,\bar{b})$

for all $x, y \in G$ *and* $b = h(a)$.

Proof. Let $h : G \to G$ be an endomorphism of an n-ary group $\langle G, f \rangle$. If $h(a) = b$, then, according to the identity (2) and Theorem 2,

$$h(y) = h(f(y, a, \ldots, a, \bar{a}) = f(h(y), b, \ldots, b, h(\bar{a})),$$

which gives $h(\bar{a}) = \bar{b}$. Now, the conditions (i), (ii) and (iii) are obvious.

Conversely, assume that a mapping $h : G \to G$ satisfies the above three conditions for all $x, y \in G$, some fixed $a \in G$ and $b = h(a)$.

From the proof of Hosszú theorem given by E. I. Sokolov (cf. [36] or [19]) it immediately follows that $\langle G, + \rangle$, where $x + y = f(x, a, \ldots, a, y)$, is a binary group, $\varphi(x) = f(\bar{a}, x, a, \ldots, a)$ its automorphism such that for $c = f(\bar{a}, \bar{a}, \ldots, \bar{a})$ the following identity

$$f(x_1, x_2, \ldots, x_n) = x_1 + \varphi(x_2) + \varphi^2(x_3) + \ldots + \varphi^{n-1}(x_n) + c \qquad (5)$$

holds. Similarly, for $x \diamond y = f(x, b, \ldots, b, y)$, $\psi(x) = f(\bar{b}, x, b, \ldots, b)$ and $d = f(\bar{b}, \bar{b}, \ldots, \bar{b})$, we have

$$f(x_1, x_2, \ldots, x_n) = x_1 \diamond \psi(x_2) \diamond \psi^2(x_3) \diamond \ldots \diamond \psi^{n-1}(x_n) \diamond d\,.$$

Thus $h(x + y) = h(x) \diamond h(y)$ by (i), $h(\varphi(x)) = \psi(h(x))$ by (ii), and $h(c) = d$ by (iii). Therefore

$$\begin{aligned} h(f(x_1, x_2, \ldots, x_n)) &= h(x_1 + \varphi(x_2) + \varphi^2(x_3) + \ldots + \varphi^{n-1}(x_n) + c) \\ &= h(x_1) \diamond \psi(h(x_2)) \diamond \psi^2(h(x_3)) \diamond \ldots \diamond \psi^{n-1}(h(x_n)) \diamond d \\ &= f(h(x_1), h(x_2), \ldots, h(x_n))\,, \end{aligned}$$

which proves that h is an endomorphism. □

Putting in the above theorem $h(x) = \bar{x}$, we obtain

Corollary 1. *An n-ary group $\langle G, f \rangle$ satisfies* (3) *if and only if there exists $a \in G$ such that*

(i) $\overline{f(x, a, \ldots, a, y)} = f(\bar{x}, \bar{a}, \ldots, \bar{a}, \bar{y})$,

(ii) $\overline{f(\bar{a}, x, a, \ldots, a)} = f(\bar{\bar{a}}, \bar{x}, \bar{a}, \ldots, \bar{a})$,

(iii) $\overline{f(\bar{a}, \bar{a}, \ldots, \bar{a})} = f(\bar{\bar{a}}, \bar{\bar{a}}, \ldots, \bar{\bar{a}})$

for all $x, y \in G$, where $\bar{\bar{a}}$ is skew to $\bar{a}$.

Corollary 2. *An n-ary group $\langle G, f\rangle$ with an idempotent $a \in G$ satisfies* (3) *if and only if for all $x, y \in G$, we have*

(i) $\overline{f(x, a, \dots, a, y)} = f(\bar{x}, a, \dots, a, \bar{y})$,

(ii) $\overline{f(a, x, a, \dots, a)} = f(a, \bar{x}, a, \dots, a)$.

Proof. Indeed, if $a \in G$ is an idempotent, then $\bar{a} = a$ and, in the consequence, $\bar{\bar{a}} = a$, which together with $f(a, \dots, a) = a$ gives the condition (iii) from Corollary 1. The rest is obvious. □

In the same manner as Theorem 4, putting $x + y = f(x, \bar{a}, a, \dots, a, y)$, $\varphi(x) = f(a, x, \bar{a}, a, \dots, a)$, $c = f(a, a, \dots, a)$ and $x \diamond y = f(x, \bar{b}, b, \dots, b, y)$, $\psi(x) = f(b, x, \bar{b}, b, \dots, b)$, $d = f(b, b, \dots, b)$, we can prove

Theorem 5. *A mapping $h : G \to G$ is an endomorphism of an n-ary group $\langle G, f\rangle$ if and only if there exists $a \in G$ such that*

(i) $h(f(x, \bar{a}, a, \dots, a, y)) = f(h(x), \bar{b}, \dots, b, h(y))$,

(ii) $h(f(a, x, \bar{a}, a, \dots, a)) = f(b, h(x), \bar{b}, b, \dots, b)$,

(iii) $h(f(a, a, \dots, a)) = f(b, b, \dots, b)$

for all $x, y \in G$ and $b = h(a)$.

Putting in this theorem $h(x) = \bar{x}$, we obtain

Corollary 3. *An n-ary group $\langle G, f\rangle$ satisfies* (3) *if and only if there exists $a \in G$ such that*

(i) $\overline{f(x, \bar{a}, a, \dots, a, y)} = f(\bar{x}, \bar{\bar{a}}, \bar{a}, \dots, \bar{a}, \bar{y})$,

(ii) $\overline{f(a, x, \bar{a}, a, \dots, a)} = f(\bar{a}, \bar{x}, \bar{\bar{a}}, \bar{a}, \dots, \bar{a})$,

(iii) $\overline{f(a, a, \dots, a)} = f(\bar{a}, \bar{a}, \dots, \bar{a})$

for all $x, y \in G$, where $\bar{\bar{a}}$ is skew to $\bar{a}$.

Corollary 4. *If an n-ary group $\langle G, f\rangle$ has an element $a \in G$ such that*

(i) $\overline{f(x, \bar{a}, a, \dots, a, y)} = f(\bar{x}, \bar{a}, a, \dots, a, \bar{y})$,

(ii) $\overline{f(a, x, \bar{a}, a, \dots, a)} = f(a, \bar{x}, \bar{a}, a, \dots, a)$

for all $x, y \in G$, then $h(x) = \bar{x}$ is an endomorphism of $\langle G, f\rangle$.

Proof. It is not difficult to verify (using (2) and Theorem 2) that for $x+y = f(x,\bar{a},a,\ldots,a,y)$, $\varphi(x) = f(a,x,\bar{a},a,\ldots,a)$ and $c = f(a,a,\ldots,a)$ the identity (5) holds. Obviously $\langle G,+\rangle$ is a group and a is its neutral element. Thus $a = a+a$ and, in the consequence, $\bar{a} = \overline{a+a} = \bar{a}+\bar{a}$ by (i). Hence $\bar{a} = a$ and $c = a$. Therefore, in our case, the identity (5) has the form

$$f(x_1,x_2,\ldots,x_n) = x_1 + \varphi(x_2) + \varphi^2(x_3) + \ldots + \varphi^{n-1}(x_n)\,.$$

But, by (i) and (ii), for all $x,y \in G$ we have $\overline{x+y} = \bar{x}+\bar{y}$, $\overline{\varphi(x)} = \varphi(\bar{x})$, which gives

$$\begin{aligned}\overline{f(x_1,x_2,\ldots,x_n)} &= \bar{x}_1 + \overline{\varphi(x_2)} + \overline{\varphi^2(x_3)} + \ldots + \overline{\varphi^{n-1}(x_n)}\\ &= \bar{x}_1 + \varphi(\bar{x}_2) + \varphi^2(\bar{x}_3) + \ldots + \varphi^{n-1}(\bar{x}_n)\\ &= f(\bar{x}_1,\bar{x}_2,\ldots,\bar{x}_n)\,.\end{aligned}$$

Hence $h(x) = \bar{x}$ is an endomorphism of an n-ary group $\langle G,f\rangle$. □

The converse is not true. Indeed, in an n-ary group $\langle Z,f\rangle$, where Z is the set of integers, $f(x_1,\ldots,x_n) = x_1+\ldots+x_n+1$, $h(x) = \bar{x} = (2-n)x-1$ is an endomorphism, but (i) and (ii) are not satisfied. Moreover in this n-ary group $\bar{x} \neq \bar{y}$ for $x \neq y$. But there are n-groups in which $\bar{x} = \bar{y}$ for all x,y. In such n-groups one fixed element is skew to all others. Obviously this element is an idempotent. This suggest the following characterization given in [11].

Theorem 6. (Dudek 1990) *An n-ary group satisfies the identity $\bar{x} = \bar{y}$ if and only if it is derived from a binary group of the exponent $t \mid n-2$.*

If an element a is skew to all $x \in G$, then an n-group $\langle G,f\rangle$ is derived from a binary group $\langle G,\circ\rangle$, where $x \circ y = f(x,a,\ldots,a,y)$. Obviously a is the identity of $\langle G,\circ\rangle$. Moreover, by (2), for all $x \in G$ we have

$$a = f(a,x,\ldots,x,\bar{x}) = f(a,x,\ldots,x,a)\,,$$

which implies the identity

$$f(a,x,\ldots,x,a) = f(a,y,\ldots,y,a)\,. \tag{9}$$

Conversely, if there exists $a \in G$ such that (9) holds for all $x, y \in G$, then $f(a, x, \ldots, x, a) = f(a, \ldots, a)$. Therefore, applying (2), we obtain

$$\begin{aligned} f(a, \ldots, a, \bar{a}) &= a = f(a, x, \ldots, x, \bar{x}) = f(a, x, \ldots, x, f(a, \ldots, a, \bar{a}, \bar{x})) \\ &= f(f(a, x, \ldots, x, a), a, \ldots, a, \bar{a}, \bar{x}) \\ &= f(f(a, \ldots, a), a, \ldots, a, \bar{a}, \bar{x}) = f(a, \ldots, a, f(a, \ldots, a, \bar{a}, \bar{x})) \\ &= f(a, \ldots, a, \bar{x}), \end{aligned}$$

which implies $\bar{a} = \bar{x}$ for all $x \in G$.

Thus the following theorem is true.

Theorem 7. *An n-ary group satisfies the identity $\bar{x} = \bar{y}$ if and only if there exists $a \in G$ such that (9) holds for all $x, y \in G$.*

Problem 2. *Describe n-ary groups in which $\bar{x} \neq \bar{y}$ for all $x \neq y$.*

Problem 3. *When $h(x) = \bar{x}$ is an automorphism ?*

Let $\bar{x}^{(0)} = x$ and let $\bar{x}^{(k+1)}$ be the skew element to $\bar{x}^{(k)}$, where $k \geqslant 0$. In other words, $\bar{x}^{(0)} = x$, $\bar{x}^{(1)} = \bar{x}$, $\bar{x}^{(2)} = \bar{\bar{x}}$, $\bar{x}^{(3)} = \bar{\bar{\bar{x}}}$, etc.

For example, in a 4-group derived from the additive group Z_8, we have $\bar{x} \equiv 6x \,(mod\, 8)$, $\bar{\bar{x}} \equiv 4x \,(mod\, 8)$ and $\bar{x}^{(k)} \equiv 0 \,(mod\, 8)$ for $k \geqslant 3$. In the n-group derived from the additive group of integers: $\bar{x}^{(k)} \neq \bar{x}^{(t)}$ for all $x \neq 0$ and $k \neq t$. But in any ternary group $\bar{\bar{x}} = x$ for all x (cf. [6]).

If $\bar{x}^{(k)} = x$ and $\bar{y}^{(t)} = y$ for some $k, t > 1$, then $\bar{x} = \bar{y}$ if and only if $x = y$. If $h(x) = \bar{x}$ is an automorphism, then $h(x) = \bar{x}^{(k)}$ is an automorphism, too. The converse is not true, because $h(x) = \bar{\bar{x}}$ is an identity automorphism of any ternary group, but $h(x) = \bar{x}$ is an automorphism only in the case when this group is medial.

Problem 4. *Describe the class $\mathbf{W_k}$ of n-ary groups in which $h(x) = \bar{x}^{(k)}$ is an endomorphism (automorphism).*

Obviously $\mathbf{W_1} \subset \mathbf{W_2} \subset \mathbf{W_3} \subset \ldots \subset \mathbf{W_0}$. When $\mathbf{W_k} = \mathbf{W_{k+1}}$?

As a simple consequence of Theorem 4, for $h(x) = \bar{x}^{(k)}$, we obtain

Corollary 5. *$h(x) = \bar{x}^{(k)}$ is an endomorphism of an n-ary group $\langle G, f\rangle$ if and only if there exists $a \in G$ such that*

(i) $\overline{f(x, a, \ldots, a, y)}^{(k)} = f(\bar{x}^{(k)}, \bar{a}^{(k)}, \ldots, \bar{a}^{(k)}, \bar{y}^{(k)})$,

(ii) $\overline{f(\bar{a}, x, a, \ldots, a)}^{(k)} = f(\bar{a}^{(k+1)}, \bar{x}^{(k)}, \bar{a}^{(k)}, \ldots, \bar{a}^{(k)})$,

(iii) $\overline{f(\bar{a}, \bar{a}, \ldots, \bar{a})}^{(k)} = f(\bar{a}^{(k+1)}, \bar{a}^{(k+1)}, \ldots, \bar{a}^{(k+1)})$

for all $x, y \in G$.

Corollary 6. *If an n-ary group $\langle G, f\rangle$ contains an element a such that $a = \bar{a}^{(k)}$, then $h(x) = \bar{x}^{(k)}$ is an endomorphism of $\langle G, f\rangle$ if and only if*

(i) $\overline{f(x, a, \ldots, a, y)}^{(k)} = f(\bar{x}^{(k)}, a, \ldots, a, \bar{y}^{(k)})$,

(ii) $\overline{f(\bar{a}, x, a, \ldots, a)}^{(k)} = f(\bar{a}, \bar{x}^{(k)}, a, \ldots, a)$,

(iii) $\overline{f(\bar{a}, \bar{a}, \ldots, \bar{a})}^{(k)} = f(\bar{a}, \bar{a}, \ldots, \bar{a})$

for all $x, y \in G$.

Corollary 7. *If an n-ary group $\langle G, f\rangle$ contains an idempotent a, then $h(x) = \bar{x}^{(k)}$ is an endomorphism if and only if*

(i) $\overline{f(x, a, \ldots, a, y)}^{(k)} = f(\bar{x}^{(k)}, a, \ldots, a, \bar{y}^{(k)})$,

(ii) $\overline{f(a, x, a, \ldots, a)}^{(k)} = f(a, \bar{x}^{(k)}, a, \ldots, a)$

for all $x, y \in G$.

We finish this section by the following problem.

Problem 5. *Describe the class $\mathbf{U_k}$ of n-ary groups in which $\bar{x}^{(k)} = \overline{y}^{(k)}$ for all elements x, y.*

The class $\mathbf{U_k}$ contains n-ary groups with only one *k-skew element*, i.e. n-ary groups in which there exists only one element a such that $a = \bar{x}^{(k)}$ for all x. Obviously $\mathbf{U_1} \subset \mathbf{U_2} \subset \mathbf{U_3} \subset \ldots$

It is not difficult to see that a ternary group belongs to $\mathbf{U_k}$ if and only if it is trivial (has only one element). The class $\mathbf{U_1}$ coincides with the class of all n-ary groups derived from binary groups of the exponent $t | n-2$ (Theorem 6). Generally, all n-ary groups derived from the binary group of the exponent $t \,|\, (n-2)^k$ belong to $\mathbf{U_k}$, but $\mathbf{U_k}$ contains also other groups.

3. Sequences

Now we consider the sequence

$$x,\ \bar{x}\,,\ \bar{x}^{(2)}\,,\ \bar{x}^{(3)}\,,\ \bar{x}^{(4)}\,,\ \ldots\,,\ \bar{x}^{(k)}\,,\ \ldots$$

If an n-ary group $\langle G, f\,\rangle$ is finite, then obviously $\bar{x}^{(k)} = \bar{x}^{(t)}$ for some $k \neq t$. (In a 6-ary group derived from the additive group Z_{12} for $x = 1$ we have: $1, 8, 4, 8, 4, 8, 4, \ldots$) But in some infinite n-ary groups (for example in an n-ary group derived from the additive group of integers) $\bar{x}^{(k)} \neq \bar{x}^{(t)}$ for all $k \neq t$.

In connection with this the following two problems were posed in [10].

Problem 6. *Describe infinite n-ary groups in which $\overline{x}^{(k)} \neq \overline{x}^{(m)}$ for all $k \neq m$ and all $x \in G$.*

Problem 7. *Describe n-ary groups in which there exists a natural number k such that $\overline{x}^{(k)} = \overline{x}^{(m)}$ for all $m \geqslant k$ and all $x \in G$.*

Following E. L. Post (cf. [31], p.282), we define the *n-ary power* putting

$$x^{<k>} = \begin{cases} f(x^{<k-1>}, x, \ldots, x) & \text{for} \quad k > 0, \\ x & \text{for} \quad k = 0, \\ y \,:\, f(y, x^{<-k-1>}, x, \ldots, x) = x & \text{for} \quad k < 0, \end{cases}$$

i.e. $x^{<0>} = x\,,$

$x^{<1>} = f(x, x, \ldots, x)\,,$

$x^{<2>} = f(x^{<1>}, x, x, \ldots, x)\,,$

$x^{<3>} = f(x^{<2>}, x, x, \ldots, x)\,,$

. . . . . .

A minimal natural number k (if it exists) such that $x^{<k>} = x$ is called an *n-ary order of x* and is denoted by $ord_n(x)$.

It is not difficult to verify that the following exponential laws hold

$$f(x^{<s_1>}, x^{<s_2>}, \ldots, x^{<s_n>}) = x^{<s_1+s_2+\ldots+s_n+1>},$$
$$(x^{<r>})^{<s>} = x^{<rs(n-1)+s+r>} = (x^{<s>})^{<r>}.$$

Using the above laws we can see that $\bar{x} = x^{<-1>}$ and, in the consequence

$$\bar{x}^{(2)} = (x^{<-1>})^{<-1>} = x^{<n-3>},$$
$$\bar{x}^{(3)} = ((x^{<-1>})^{<-1>})^{<-1>},$$

and so on. Generally: $\bar{x}^{(k)} = (\bar{x}^{(k-1)})^{<-1>}$ for all $k \geqslant 1$. This implies that $\bar{x}^{(k)} = x^{<S_k>}$ for

$$S_k = -\sum_{i=0}^{k-1}(2-n)^i = \frac{(2-n)^k - 1}{n-1}$$

Obviously $ord_n(\bar{x})$ is a divisor of $ord_n(x)$, and $ord_n(x)$ is a divisor of $Card(G)$. This last fact is a simple conclusion from Lagrange's theorem for finite n-ary groups (sf. [31], p.222). Hence

$$ord_n(x) \geqslant ord_n(\bar{x}) \geqslant ord_n(\bar{x}^{(2)}) \geqslant ord_n(\bar{x}^{(3)}) \geqslant \dots$$

The first natural questions are:

1. When $ord_n(x) = ord_n(\bar{x})$?
2. When there exists k such that $ord_n(\bar{x}^{(k)}) = ord_n(\bar{x}^{(t)})$ for all $t \geqslant k$?
3. When $\lim\limits_{t\to\infty} ord_n(\overline{x}^{(t)}) = 1$?

From some results obtained by E. L. Post for a finite n-ary group generated by one element (cf. [31], p.283), we can deduce that

$$ord_n(x^{<s>}) = \frac{ord_n(x)}{gcd\{s(n-1)+1,\, ord_n(x)\}}$$

whenever $ord_n(x)$ is finite. Therefore for $k \geqslant 1$, we have

$$ord_n(\bar{x}^{(k)}) = ord_n(x^{<s_k>}) = \frac{ord_n(x)}{gcd\{n-2,\, ord_n(x)\}}\ .$$

Thus

$$ord_n(x) \geqslant ord_n(\bar{x}) = ord_n(\bar{x}^{(2)}) = ord_n(\bar{x}^{(3)}) = \dots$$

Moreover, $ord_n(\bar{x}) = ord_n(x) < \infty$ if and only if $ord_n(x)$ and $n-2$ are relatively prime. Obviously $\lim\limits_{t\to\infty} ord_n(\overline{x}^{(t)}) = 1$ if and only if $ord_n(x)$ is a divisor of $n-2$.

This, together with Theorem 2 from [7], gives the following characterization of orders of skew elements.

Theorem 5. *If* $ord_n(x) = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_m^{\alpha_m}$, *where* $p_1, p_2, \dots, p_m$ *are prime numbers, then for all* $t \geqslant 1$ *we have* $ord_n(\bar{x}^{(t)}) = 1$ *or* $ord_n(\bar{x}^{(t)}) = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$, *where* $k \leqslant m$ *and* $p_1 \nmid n-2$, $p_2 \nmid n-2$, $\dots$, $p_k \nmid n-2$.

Corollary 8. *If every prime divisor of $Card(G)$ is a divisor of $n-2$, then all skew elements of an n-ary group $\langle G, f\rangle$ are idempotent.*

A commutative n-ary group with this property is derived from some (commutative) binary group. All idempotents of such n-ary group are neutral elements in the sense of W. Dörnte (cf. [6]). The set of all neutral elements of a given n-ary group is empty or forms a commutative n-ary subgroup of this group (cf. [17]).

4. Special subgroups

An element x of an n-ary group $\langle G, f\rangle$ is called *potent* if for some natural $k \geqslant 1$ an element $x^{<k>}$ is idempotent. For any natural $n \geqslant 3$ there exist infinitely many pairwise non-isomorphic n-ary groups containing at least one potent element (cf. [17]). It is not difficult to see that x is potent if and only if $x^{<1>}$ is idempotent, or equivalently, if and only if $ord_n(x)$ is a divisor of n.

Problem 8. *When the set of all potents of a given n-ary group is an n-ary (normal) subgroup ?*

In [10] is considered the class $\mathbf{V_k}$ of n-ary groups in which $\overline{x}^{(k)} = x$ holds for all x. This class is a variety, $\mathbf{V_k} \cap \mathbf{V_{k+1}} = \mathbf{V_1}$ and $\mathbf{V_k} \subset \mathbf{V_{km}}$ for any natural k, m. Any $\mathbf{V_k}$ contains the variety of medial n-ary groups (and in the consequence – the variety of all commutative n-ary groups). But it contains also non-medial n-ary groups. $\mathbf{V_{2k}}$ contains the variety of ternary groups.

Problem 9. *Describe the variety $\mathbf{V_k}$.*

Note that if $h(x) = \bar{x}^{(k)}$ is an endomorphism of an n-ary group, then the relation

$$x \ \rho_k \ y \iff \overline{x}^{(k)} = \overline{y}^{(k)}$$

is a congruence on $\langle G, f\rangle$ and

$$G^{(k)} = \{\, \overline{x}^{(k)} \mid x \in G\}$$

is an n-ary subgroup of $\langle G, f\rangle$. Also

$$E^{(k)} = \{\, x \in G \mid \overline{x}^{(k)} = x\}$$

is an n-ary subgroup, if it is non-empty.

Generally $E^{(k)} \subset G^{(k)}$, but in some cases $E^{(k)} = G^{(k)}$. For example, in ternary groups we have $E^{(2k)} = G^{(2k)}$ for all natural k. Unfortunately, this not implies $E^{(2k+1)} = G^{(2k+1)}$. Nevertheless in ternary groups $G^{(k)} = G$ for all k.

Moreover, $E^{(k)} \in \mathbf{V_k}$, $E^{(1)} \subset E^{(k)}$, $E^{(s)} \subset E^{(sk)}$, $E^{(s)} \cap E^{(s+1)} = E^{(1)}$, $G^{(k+1)} = (G^{(k)})^{(1)}$ and

$$G \supset G^{(1)} \supset G^{(2)} \supset G^{(3)} \supset ...$$

In finite n-ary groups $G^{(k)} = G^{(k+1)} = ...$ for some $k \in N$, but in an n-ary group derived from the additive group of integers $G^{(k)} \neq G^{(m)}$ for all $k \neq m$.

Problem 10. *Describe the class of all n-ary groups (or only medial groups) satisfying the descending chain condition for $G^{(k)}$.*

If $G^{(k)} = G$ for some $k > 1$, then also $G^{(1)} = G$. Conversely, if $G^{(1)} = G$, then $G^{(2)} = (G^{(1)})^{(1)} = G$, and, in the consequence, $G^{(k)} = G$ for all $k > 1$. Thus the question on the equation $G^{(k)} = G$ can be reduced to the question on the equation $G^{(1)} = G$.

Problem 11. *Describe n-ary groups in which $G^{(1)} = G$.*

$G^{(k)}$ and $E^{(k)}$ are n-ary subgroups also in some n-ary groups in which $h(x) = \bar{x}^{(k)}$ is not an endomorphism. A simple illustration of such situation is a 4-group derived from the symmetric group S_3. In this 4-group we have $G^{(k)} = G^{(1)} = E^{(1)} = E^{(k)} = \{ z \in S_3 \mid z^3 = e \}$ and $\bar{x}^{(k)} = \bar{x}$ for all $x \in S_3$, but $\overline{f(a,z,a,z)} \neq f(\bar{a},\bar{z},\bar{a},\bar{z})$ for $a = (1\,2)$, $y = (1\,2\,3)$.

Problem 12. *Describe n-ary groups in which $G^{(1)}$ is an n-ary subgroup.*

Problem 13. *Describe n-ary groups in which $E^{(k)}$ is an n-ary subgroup.*

In a *distributive* n-ary group, i.e. in an n-ary group satisfying the identity

$$\overline{f(x_1,...,x_n)} = f(x_1,...,x_{i-1},\bar{x}_i,x_{i+1},...,x_n)\,, \tag{10}$$

where $i = 1,2,...,n$, we have

$$\overline{x}^{(n-1)} = x = x^{<n-1>}$$

(cf. [14]). In such n-ary group all elements have the same finite n-ary order which is a divisor of $n-1$. Moreover, if $ord_n(x) = k$, then $x^{<t>} = \bar{x}^{(k-t)}$ and $\bar{x}^{(t)} = x^{<k-t>}$ for $t = 0, 1, \ldots, k$. Thus the smallest n-ary subgroup containing x has the form

$$C_x = \{x, x^{<1>}, \ldots, x^{<k-1>}\} = \{x, \bar{x}, \ldots, \overline{x}^{(k-1)}\},$$

where $k = ord_n(x)$. Obviously C_x is commutative and has no proper subgroups. This suggest the following theorem proved in [14].

Theorem 6. (Dudek 1995) *Any distributive n-ary group is a set-theoretic union of disjoint cyclic and isomorphic n-ary groups without proper subgroups.*

Theorem 7. (Dudek 1995) *Let $a \circ b = f(a, x, \ldots, x, b)$, where x is an arbitrary element of a distributive n-ary group $\langle G, f\rangle$. Then C_x is a normal subgroup of $\langle G, \circ\rangle$ and every coset of C_x in $\langle G, \circ\rangle$ is an n-ary subgroup of $\langle G, f\rangle$ isomorphic to $\langle C_x, f\rangle$.*

Problem 14. *Prove or disprove the converse of the above theorems.*

A distributive n-ary group is a set-theoretic union of commutative subgroups but it is not commutative in general. Indeed, if $t \geqslant 2$, $(t-1)|(n-1)$ and $p = t^{n-1} - 1$, then $\varphi(x) \equiv tx (mod\, p)$ is an automorphism of the additive group Z_p such that $\varphi^{n-1}(x) \equiv x (mod\, p)$ for all $x \in Z_p$ and $\varphi(b) \equiv b$ for $b = 1 + t + t^2 + \ldots + t^{n-2}$. It is not difficult to see that Z_p with the operation

$$f(x_1, x_2, \ldots, x_n) = (x_1 + \varphi(x_2) + \ldots + \varphi^{n-2}(x_{n-1}) + x_n + b)(mod\, p)$$

is a distributive n-ary group in which $\bar{x}^{(k)} \equiv (x - kb)(mod\, p)$. This n-ary group is a set-theoretic union of t disjoint commutative n-ary subgroups $C_0, C_1, \ldots, C_{t-1}$, but it is *only* medial.

Any medial distributive n-ary group $\langle G, f\rangle$ is *autodistributive* (cf. [9]), i.e. the operation f is distributive with respect to itself. This means that for every $i = 1, 2, \ldots, n$ the following identity is satisfied

$$f(x_1, \ldots, x_{i-1}, f(y_1, y_2, \ldots, y_n), x_{i+1}, \ldots, x_n) =$$
$$f(f(x_1, \ldots, x_{i-1}, y_1, x_{i+1}, \ldots, x_n), \ldots, f(x_1, \ldots, x_{i-1}, y_n, x_{i+1}, \ldots, x_n)).$$

Any autodistributive n-ary group is distributive (cf. [9]), but for any $n > 3$ there exists at least one idempotent distributive n-ary group which

is not autodistributive. Such n-ary group can be induced by the group $(C^3, \bullet)$ and its automorphism $\varphi(x, y, z) = (\alpha x, \alpha^2 y, \alpha z)$, where C is the set of complex numbers,

$$(x, y, z) \bullet (a, b, c) = (x + a, b + xc + y, z + c)$$

and α is a primitive $(n-1)$-th root of unity (see [14], Theorem 6). For any $n \geqslant 7$ there are also non-idempotent distributive groups which are not autodistributive. Ternary distributive groups are autodistributive and vice versa. For $n = 4, 5, 6$ the problem is open.

In a distributive n-ary group $\langle G, f\rangle$ the operation $^-\colon x \to \bar{x}$ is an automorphism and induces the cyclic invariant subgroup $Aut_{\bar{s}}\langle G, f\rangle$ in the group of all automorphism $Aut\langle G, f\rangle$ and in the group $Aut_s\langle G, f\rangle$ of all *splitting-automorphism* in the sense of Płonka (cf. [30]).

Problem 15. *Describe the structure of groups:* $Aut\langle G, f\rangle/Aut_{\bar{s}}\langle G, f\rangle$, $Aut\langle G, f\rangle/Aut_s\langle G, f\rangle$ *and* $Aut_s\langle G, f\rangle/Aut_{\bar{s}}\langle G, f\rangle$.

If h is a splitting-automorphism of $\langle G, f\rangle$, then (as it is not difficult to see) $h(x) = h^n(x)$ for every $x \in G$.

Problem 16. *When* $Aut_s\langle G, f\rangle = Aut_{\bar{s}}\langle G, f\rangle$ *?*

Note by the way (cf. [14]), that if $\langle H, f\rangle$ is an n-ary subgroup of an autodistributive n-ary group $\langle G, f\rangle$, then for every $i = 1, \ldots, n$ and for all $a_1, a_2, \ldots, a_n \in G$ the coset

$$\{\, f(a_1, \ldots, a_{i-1}, h, a_{i+1}, \ldots, a_n) \,|\, h \in H\}$$

is an n-ary subgroup of $\langle G, f\rangle$ isomorphic to $\langle H, f\rangle$.

Moreover, in medial autodistributive n-ary groups

$$\{\, f(a_1, \ldots, a_{i-1}, h, a_{i+1}, \ldots, a_n) \,|\, h \in G^{(k)}\} = G^{(k)} = G$$

for all $k \geqslant 0$, and

$$\{\, f(a_1, \ldots, a_{i-1}, h, a_{i+1}, \ldots, a_n) \,|\, h \in E^{(t)}\} = E^{(t)} = G$$

for t such that $x^{<t>} = x$ for all $x \in G$. In this case we have also $G^{(k)} = G$ and $E^{(t)} = G$.

Unfortunately, this situation is not characteristic for medial autodistributive n-ary groups, because it takes place in some non-medial and non-autodistributive n-ary groups, too.

5. Fuzzy subgroups

By a *fuzzy set* μ in a set G we mean a function $\mu : G \to [0,1]$. The set

$$L(\mu, t) = \{x \in G : \mu(x) \geqslant t\},$$

where $t \in [0,1]$ is fixed, is called a *level subset of* μ.

A fuzzy set μ defined on a binary groupoid $\langle G, \cdot \rangle$ is called a *fuzzy subgroupoid* of G if $\mu(x \cdot y) \geqslant \min\{\mu(x), \mu(y)\}$ for all $x, y \in G$. A fuzzy set μ defined on a quasigroup $\langle G, \cdot, \backslash, / \rangle$ is called a *fuzzy subquasigroup* of G if $\mu(x * y) \geqslant \min\{\mu(x), \mu(y)\}$ for all $x, y \in G$ and $* \in \{\cdot, \backslash, /\}$. A fuzzy set μ defined on a group $\langle G, \cdot \rangle$ is called a *fuzzy subgroup* (or *Rosenfeld's fuzzy subgroup*) of G if it is a fuzzy subgroupoid such that $\mu(x^{-1}) \geqslant \mu(x)$ (or equivalently: $\mu(x^{-1}) = \mu(x)$) for all $x \in G$. (See the series of papers in *Fuzzy Sets and Systems.*)

The above concepts can be extended to n-ary systems in the way proposed in [16]. Namely, a fuzzy set μ defined on an n-ary groupoid $\langle G, f \rangle$ will be called an *n-ary fuzzy subgroupoid* of G if

$$\mu(f(x_1, x_2, \ldots, x_n)) \geqslant \min\{\mu(x_1), \ldots, \mu(x_n)\}$$

will be satisfied for all $x_1, \ldots, x_n \in G$.

This extension is good because for $n = 2$ it gives the standard definition. Moreover, all main results obtained for $n = 2$ can be proved also for $n > 2$ (cf. [16]).

Theorem 8. (Dudek 2000) *A fuzzy set μ of an n-ary groupoid $\langle G, f \rangle$ is an n-ary fuzzy subgroupoid of G if and only if for every $t \in [0,1]$, $L(\mu, t)$ is either empty or an n-ary subgroupoid of $\langle G, f \rangle$. Moreover, any n-ary subgroupoid of $\langle G, f \rangle$ can be realized as a level subgroupoid of some n-ary fuzzy subgroupoid.*

Theorem 9. (Dudek 2000) *If a fuzzy set μ of an n-ary groupoid $\langle G, f \rangle$ has the finite set of values $t_0 > t_1 > \ldots > t_m$ and $S_0 \subset S_1 \subset \ldots \subset S_m = G$ are n-ary subgroupoids of $\langle G, f \rangle$ such that $\mu(S_k \setminus S_{k-1}) = t_k$ for $0 \leqslant k \leqslant m$, where $S_{-1} = \emptyset$, then μ is an n-ary fuzzy subgroupoid.*

Theorem 10. (Dudek 2000) *If every n-ary fuzzy subgroupoid μ defined on $\langle G, f \rangle$ has the finite set of values, then every descending chain of n-ary subgroupoids of $\langle G, f \rangle$ terminates at finite step.*

A fuzzy set μ defined on G is said to be *normal* if there exists $x \in G$ such that $\mu(x) = 1$. A simple example of normal fuzzy sets are characteristic functions of subsets of G.

If an n-ary groupoid $\langle G, f\rangle$ is unipotent (cf. [12]), i.e. if there exists an element $\theta \in G$ such that $f(x, x, \ldots, x) = \theta$ for all $x \in G$, then a fuzzy set μ defined on G is normal if and only if $\mu(\theta) = 1$.

The set $\mathcal{N}(G)$ of all normal n-ary fuzzy subgroupoids defined on an n-ary groupoid $\langle G, f\rangle$ is partially ordered by the relation

$$\mu \sqsubseteq \rho \Longleftrightarrow \mu(x) \leqslant \rho(x)$$

for all $x \in G$.

For any n-ary fuzzy subgroupoid μ of $\langle G, f\rangle$ there exists $\rho \in \mathcal{N}(G)$ such that $\mu \sqsubseteq \rho$. Moreover, if $\langle G, f\rangle$ is unipotent, then the maximal element of $(\mathcal{N}(G), \sqsubseteq)$ is either constant or characteristic function of some subset of G.

An *n-ary subquasigroup* of an n-ary quasigroup $\langle G, f\rangle$ must be defined as a non-empty subset S of G closed with respect to $n + 1$ operations $f, f^{(1)}, \ldots, f^{(n)}$, i.e. as a subset S of G such that $g(x_1, \ldots, x_n) \in S$ for all $x_1, \ldots, x_n \in S$ and all $g \in \mathcal{F} = \{f, f^{(1)}, f^{(2)}, \ldots, f^{(n)}\}$, where $f^{(i)}$ is the i-th inverse operation of f (cf. [3] or [13]). This means that an *n-ary fuzzy quasigroup* must be defined as a fuzzy set such that

$$\mu(g(x_1, x_2, \ldots, x_n)) \geqslant \min\{\mu(x_1), \ldots, \mu(x_n)\}$$

for all $x_1, \ldots, x_n \in G$ and $g \in \mathcal{F}$.

For such defined n-ary fuzzy quasigroups many of classical results are proved in (cf. [16]).

The problem is with the fuzzification on n-ary groups. As it is well known (cf. [6]), a non-empty subset S of an n-ary group $\langle G, f\rangle$ is an n-ary subgroup of $\langle G, f\rangle$ if it is closed with respect to f and $\bar{x} \in S$ for every $x \in S$. Thus, by the analogy to the binary case, an *n-ary fuzzy subgroup* can be defined as an n-ary fuzzy subgroupoid μ such that $\mu(\bar{x}) \geqslant \mu(x)$ for all $x \in G$ or as an n-ary fuzzy subgroupoid μ such that $\mu(\bar{x}) = \mu(x)$ for all $x \in G$.

Unfortunately these two concepts are not equivalent. Indeed, it is not difficult to see that in the unipotent 4-ary group derived from the additive group Z_4 the map μ defined by $\mu(0) = 1$ and $\mu(x) = 0.5$ for all $x \neq 0$ is an example of fuzzy subgroupoid in which $\mu(\bar{x}) \geqslant \mu(x)$ for all $x \in Z_4$. Thus μ is a fuzzy subgroup in the first sense. It is not a fuzzy subgroup in the second sense because for $x = 2$ we have $\mu(\bar{x}) > \mu(x)$.

These two concepts of an n-ary fuzzy group are equivalent for ternary groups and for all n-ary groups satisfying the identity $\bar{x}^{(k)} = x$, where $k > 0$ depends (or not) on x.

Problem 17. *Find the connection between n-ary fuzzy subgroups of a given n-ary group and fuzzy subgroups of its binary retracts (creating group).*

6. r-adic skew elements

r-adic skew elements were introduced by S. A. Rusakov (cf. [34]) as a generalization of skew elements and were used to the investigation of some properties of n-ary groups connected with their subgroups.

According to [34], an element $\tilde{a}$ of an n-ary group $\langle G, f\rangle$ is called *skew of type* k and is denoted by $\bar{a}^{(k,1)}$ if the equation

$$f(a^{<k-1>}, a, \ldots, a, \tilde{a}) = a$$

is satisfied. By the *r-adic skew element of type* k, where $k, r \in N$ and $\bar{a}^{(k,0)} = a$, we mean an element

$$\bar{a}^{(k,\,r)} = \overline{\bar{a}^{(k,r-1)}}^{(k,1)}.$$

It is easy to see that $\bar{a}^{(1,\,r)} = \bar{a}^{(r)}$, i.e. r-adic skew elements of type $k = 1$ are skew in the sense of Dörnte.

Moreover, r-adic skew elements of type k can be used to the definition of n-ary groups and have similar (but not identical) properties as elements skew in the sense of Dörnte. For example, $\bar{a}^{(k,r)} = a^{<S_{kr}>}$, where

$$S_{kr} = \frac{(1 - k(n-1))^r - 1}{n-1}$$

and

$$ord_n(\bar{a}^{(k,r)}) = \frac{ord_n(a)}{gcd\{(k(n-1)-1)^r,\, ord_n(a)\}}\,.$$

But on the other hand, in a ternary group derived from the additive group of integers we have $\bar{a} = -a$, $\bar{a}^{(2)} = a$ and $\bar{a}^{(k,r)} \neq \bar{a}^{(k,t)} = (1-2k)^t a$ for all $k > 1$ and $r \neq t$. In this group we have also $\bar{a}^{(14,t)} = \bar{a}^{(2,3t)}$ for all $t \in N$.

Problems for r-adic skew elements are similar to the problems posed for skew elements in the sense of Dörnte. For example, when $\bar{a}^{(k,r)} = a$ or when $h(x) = \bar{x}^{(k,r)}$ is an automorphism.

References

[1] **D. J. Allen**: *Abstract algebras with a single operation and group-like axioms*, Amer. Math. Monthly **74** (1967), 186 – 188.

[2] **R. Baer**: *Zur Einführung des Scharbegriffs*, J. reineangew. Math. **160** (1929), 199 – 207.

[3] **V. D. Belousov**: *n-ary quasigroups*, (Russian), Ştiinţa, Kishinev 1972.

[4] **V. D. Belousov and Z. Stojaković**: *On infinitary quasigroups*, Publ. Inst. Math. (Beograd) **15(29)** (1973), 31 – 42.

[5] **J. Certaine**: *The ternary operation* $(abc) = ab^{-1}c$ *of a group*, Bull. Amer. Math. Soc. **49** (1943), 869 – 677.

[6] **W. Dörnte**: *Untersuchungen über einen verallgemeinerten Gruppenbegriff*, Math. Zeitschr. **29** (1928), 1 – 19.

[7] **I. M. Dudek and W. A. Dudek**: *On skew elements in n-groups*, Demonstratio Math. **14** (1981), 827 – 833.

[8] **W. A. Dudek**: *Remarks on n-groups*, Demonstratio Math. **13** (1980), 165 – 181.

[9] **W. A. Dudek**: *Autodistributive n-groups*, Commentationes Math. Annales Soc. Math. Polonae, Prace Matematyczne **23** (1983), 1 – 11.

[10] **W. A. Dudek**: *Medial n-groups and skew elements*, Proc. V Universal Algebra Symp. "Universal and Applied Algebra", Turawa 1988, World Scientific, Singapore 1989, 55 – 80.

[11] **W. A. Dudek**: *On n-ary group with only one skew element*, Radovi Matematički (Sarajevo), **6** (1990), 171 – 175.

[12] **W. A. Dudek**: *Unipotent n-ary groups*, Demonstratio Math. **24** (1991), 75 – 81.

[13] **W. A. Dudek**: *Varieties of polyadic groups*, Filomat **9** (1995), 657 – 674.

[14] **W. A. Dudek**: *On distributive n-ary groups*, Quasigroups and Related Systems **2** (1995), 132 – 151.

[15] **W. A. Dudek**: *On the class of weakly semiabelian poliadic groups*, Discrete Math. Appl. **6** (1996) no. 5, 427 – 433 (*translation from Diskretnaya Mat.* **8** (1996), 40 – 46).

[16] **W. A. Dudek**: *Fuzzification of n-ary groupoids*, Quasigroups and Related Systems **7** (2000), 45 – 66.

[17] **W. A. Dudek**: *Idempotents in n-ary semigroups*, Southeast Asian Bull. Math. **25** (2001), 97 – 104.

[18] **W. A. Dudek, K. Głazek and B. Gleichgewicht**: *A note on the axioms of n-groups*, Colloquia Math. Soc. J. Bolyai **29** "Universal Algebra", Esztergom (Hungary) 1977, 195 – 202. (North-Holland, Amsterdam 1982.)

[19] **W. A. Dudek and J. Michalski**: *On a generalization of Hosszú theorem*, Demonstratio Math. **15** (1982), 783 – 805.

[20] **W. A. Dudek and J. Michalski**: *On retracts of polyadic groups*, Demonstratio Math. **17** (1984), 281 – 301.

[21] **W. A. Dudek and Z. Stojaković**: *On Rusakov's n-ary rs-groups*, Czechoslovak Math. J. **51(126)** (2001), 275 – 283.

[22] **K. Głazek and B. Gleichgewicht**: *Abelian n-groups*, Colloquia Math. Soc. J. Bolyai **29** "Universal Algebra", Esztergom (Hungary) 1977, 321 – 329. (North-Holland, Amsterdam 1982.)

[23] **B. Gleichgewicht and K. Głazek**: *Remarks on n-groups as abstract algebras*, Coll. Math. **17** (1967), 209 – 219.

[24] **M. Hosszú**: *On the explicit form of n-groups*, Publ. Math. **10** (1963), 88 – 92.

[25] **E. Kasner**: *An extension of the group concept*, Bull. Amer. Math. Soc. **10** (1904), 290 – 291.

[26] **R. Kerner**: *Ternary structures and Z_3-grading*, Generalized Symmetries in Physics, World Scientific, Singapore 1994, 375 – 394.

[27] **D. H. Lehmer**: *A ternary analogue of abelian groups*, Amer. J. Math. **59** (1932), 328 – 338.

[28] **G. A. Miller**: *Sets of group elements involving only products of more than n*, Proc. Nat. Acad. Sci. **21** (1935), 45 – 47.

[29] **Y. Nambu**: *Generalized Hamiltonian mechanics*, Phys. Rev. D7 (1973), 2405 – 2412.

[30] **J. Płonka**: *On splitting-automorphisms of algebras*, Bull. Soc. Royale Sci. Liège **42** (1973), 302 – 306.

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

[32] **H. Prüfer**: *Teorie der Abelishen Gruppen*, Math. Zeitschr. **20** (1924), 165 – 187.

[33] **D. W. Robinson**: *n-groups with identity elements*, Math. Mag. **31** (1958), 255 – 258.

[34] **S. A. Rusakov**: *r-adic skew elements of the type k in n-ary groups*, (Russian), Dok.Akad. Nauk BSSR **26** (1982), 110 – 112.

[35] **S. A. Rusakov**: *Some applications of n-ary group theory*, (Russian), Belaruskaya navuka, Minsk 1998.

[36] **E. I. Sokolov**: *On the Gluskin-Hosszú theorem for Dörnte n-groups*, (Russian), Mat. Issled. **39** (1976), 187 – 189.

[37] **Z. Stojaković**: *Single identities for Mendelsohn and Steiner* 3*-quasigroups*, Bull. Austral. Math. Soc. **53** (1996), 419 – 424.

[38] **Z. Stojaković and W. A. Dudek**: *Single identities for varieties equivalent to quadruple systems*, Discrete Math. **183** (1998), 277 – 284.

[39] **A. K. Sushkevich**: *Theory of generalized groups*, (Russian), Gos. Naučno-Tehn. Izdat. Ukrainy, Kharkov 1937.

[40] **L. Takhtajan**: *On foundation of the generalized Nambu mechanics*, Commun. Math. Phys. **160** (1994), 295 – 315.

[41] **V. V. Vagner**: *Theory of generalized heaps and generalized groups*, (Russian), Mat. Sbornik **32(74)** (1953), 545 – 632.

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

Received August 16, 2001

Quasigroups and Related Systems **8** (2001), 37 – 44

Transversals in groups. 3. Semidirect product of a transversal operation and subgroup

Eugene A. Kuznetsov

Abstract

The investigation of transversals in groups beginned in [6, 7] is continued in a present article. The main aim of this article is a demonstration of a natural way of a construction of a semidirect product of a left quasigroup with two-sided unit and some group by the help of transversals.

The present article is a continuation of a cycle of works about the investigations of transversals in groups, beginned in [6, 7]. As it is known, the concept of transversal is introduced for investigation of left (right) cosets in a group by its proper subgroup. The case when this subgroup is not normal, is the most interesting one.

In [6] it was proved that the operation of $\langle E, \overset{(T)}{\bullet} \rangle$, corresponding to the left transversal T in a group G to its subgroup H, is a left quasigroup with two-sided unit 1. So, by the natural way, the following problem is appears define correctly such product of the left quasigroup $\langle E, \overset{(T)}{\bullet}, 1 \rangle$ with two-sided unit 1 and a subgroup H that the result of this product will be isomorphic to the initial group G.

The analogous investigations took place in [8, 9, 2] and especially in [10]. In these works we may see some formula (formula (7) in the present article) of a semidirect product mentioned above. But in these works the way of a construction of this formula is not clear and, moreover, the uniqueness of this formula as a formula of a semidirect product satisfying the conditions mentioned above was not shown.

2000 Mathematics Subject Classification: 20N15
Keywords: group, loop, transversal, permutation, semidirect product

The author of this article want to show the natural way of constructing of above mentioned product by the help of the concept of transversal in a group. The uniqueness of the formula (7) of semidirect product satisfying the conditions mentioned above immediately follows from the method of constructing.

1. Necessary definitions and notations

Definition 1. A system $\langle E, \cdot \rangle$ is called a *left* (*right*) *quasigroup*, if for arbitrary $a, b \in E$ the equation $x \cdot a = b$ (respectively: $a \cdot y = b$) has a unique solution in the set E. If $\langle E, \cdot \rangle$ in the same times is a left and right quasigroup, then it is called a *quasigroup*. A quasigroup containing an element e satisfying the identity $x \cdot e = e \cdot x = e$ is called a *loop*.

Definition 2. (cf. [1]) Let G be a group and H its subgroup. A complete system $T = \{t_i\}_{i \in E}$ of representatives of the left (right) cosets of H in G ($e = t_1 \in H$) is called a *left* (*right*) *transversal in G to H*.

Let $T = \{t_i\}_{i \in E}$ be a left transversal in G to H. We can define correctly (see [1, 7]) the following operation on the set E (E is an index set; left cosets in G to H are numbered by indexes from E):

$$x \overset{(T)}{\cdot} y = z \quad \overset{def}{\Longleftrightarrow} \quad t_x t_y = t_z h, \quad h \in H.$$

In [7] it is proved that $\langle E, \cdot \rangle$ is a left quasigroup with two-sided unit 1.

Below we assume (for simplicity) that $Core_G(H) = e$ and we study a permutation representation $\hat{G}$ of a group G by its left cosets of a subgroup H. According to [5], we have $\hat{G} \cong G$, where

$$\hat{g}(x) = y \quad \overset{def}{\Longleftrightarrow} \quad g t_x H = t_y H.$$

Note that $\hat{H} = St_1(\hat{G})$.

Lemma 1. ([6], Lemma 4) *Let T be an arbitrary left transversal in G to H. Then the following statements are true:*

1. $\hat{h}(1) = 1 \quad \forall h \in H.$

2. *For any $x, y \in E$* $\hat{t}_x(y) = x \overset{(T)}{\cdot} y; \quad \hat{t}_1(x) = \hat{t}_x(1) = x;$

$$\hat{t}_x^{-1}(y) = x \overset{(T)}{\backslash} y; \quad \hat{t}_x^{-1}(1) = x \overset{(T)}{\backslash} 1; \quad \hat{t}_x^{-1}(x) = 1,$$

where $\overset{(T)}{\backslash}$ *is the left division in* $< E, \overset{(T)}{\cdot}, 1 >$ (*i.e.* $x \overset{(T)}{\backslash} y = z \Longleftrightarrow x \overset{(T)}{\cdot} z = y$).

Since an arbitrary element $g \in G$ is contained in some left coset of H in G, then it can be a uniquely represented in the form:

$$g = t_u h, \tag{1}$$

where $t_u \in T$, $h \in H$.

Let $g_1 g_2 = g_3$ be the product of two arbitrary elements of G. According to the representation (1) we have

$$t_x h_1 t_y h_2 = t_z h_3. \tag{2}$$

Let $x \overset{(T)}{\cdot} y = x \bullet y$. In view of Lemma 1 we have

$$z = \hat{t}_z(1) = \hat{t}_z \hat{h}_3(1) = \hat{t}_x \hat{h}_1 \hat{t}_y \hat{h}_2(1) = \hat{t}_x \hat{h}_1 \hat{t}_y(1) = \hat{t}_x \hat{h}_1(y) = x \bullet \hat{h}_1(y). \tag{3}$$

Applying (2) and (3) we obtain

$$h_3 = t_z^{-1} t_x h_1 t_y h_2 = t^{-1}_{x \bullet \hat{h}_1(y)} t_x h_1 t_y h_2 = (t^{-1}_{x \bullet \hat{h}_1(y)} t_x t_{\hat{h}_1(y)})(t^{-1}_{\hat{h}_1(y)} h_1 t_y h_1^{-1}) h_1 h_2,$$

which implies

$$t_x h_1 t_y h_2 = t_{x \bullet \hat{h}_1(y)} (t^{-1}_{x \bullet \hat{h}_1(y)} t_x t_{\hat{h}_1(y)})(t^{-1}_{\hat{h}_1(y)} h_1 t_y h_1^{-1}) h_1 h_2 \,. \tag{4}$$

Now let

$$\begin{aligned} l_{a,b} &\rightleftharpoons t^{-1}_{a \bullet b} t_a t_b, \\ \varphi(u,h) &\rightleftharpoons t^{-1}_{\hat{h}(u)} h t_u h^{-1} \end{aligned}$$

(for details see [10]).

Lemma 2. *The following sentences are true:*

1) $\hat{l}_{a,b} \in \hat{H}$ *for any* $a, b \in E$.

2) $\hat{\varphi}(u,h) \in \hat{H}$ *for any* $u \in E$ *and* $h \in H$.

Proof. 1) For any $a, b \in E$ we have

$$\hat{l}_{a,b}(1) = \hat{t}^{-1}_{a \bullet b} \hat{t}_a \hat{t}_b(1) = \hat{t}^{-1}_{a \bullet b} \hat{t}_a(b) = \hat{t}^{-1}_{a \bullet b}(a \bullet b) = (a \bullet b) \backslash (a \bullet b) = 1,$$

i.e. $\hat{l}_{a,b} \in St_1(\hat{G}) = \hat{H}$.

2) For any $u \in E$ and $h \in H$ we obtain

$$\begin{aligned} \hat{\varphi}(u,h)(1) &= \hat{t}^{-1}_{\hat{h}(u)} \hat{h}\, \hat{t}_u \hat{h}^{-1}(1) = \hat{t}^{-1}_{\hat{h}(u)} \hat{h}\, \hat{t}_u(1) \\ &= \hat{t}^{-1}_{\hat{h}(u)} \hat{h}\,(u) = (\hat{h}\,(u)) \backslash (\hat{h}\,(u)) = 1, \end{aligned}$$

i.e. $\hat{\varphi}(u,h) \in St_1(\hat{G}) = \hat{H}$. □

Remark 1. All permutations $\hat{l}_{a,b}$ generate the group

$$LI(\langle E,\cdot,1\rangle) \rightleftharpoons \langle \hat{l}_{a,b} | a,b \in E\rangle,$$

which is called a *left inner mapping group* of operation $\langle E,\cdot,1\rangle$. In view of Lemma 2 we have

$$LI(\langle E,\cdot,1\rangle) \subseteq \hat{H}. \tag{5}$$

Remark 2. In [10] it is shown that $\hat{\varphi}(u, LI(\langle E,\cdot,1\rangle)) \subset LI(\langle E,\cdot,1\rangle)$, for any $u \in E$, i.e. all elements of the group $LI(\langle E,\cdot,1\rangle)$ satisfy both the conditions of Lemma 2.

2. Semidirect products

The investigations in the previous chapter lead us in the natural way to the definition of a product of the left quasigroup $\langle E,\bullet,1\rangle$ with two-sided unit 1 and a group H (satisfying some conditions connected with the operation in $\langle E,\bullet,1\rangle$).

Let $\langle E,\bullet,1\rangle$ be a left quasigroup with two-sided unit 1 and let H be a permutation group on the set E $(H \subseteq St_1(S_E))$ such that

$$\begin{array}{cc} \forall a,b \in E & l_{a,b} = L^{-1}_{a\bullet b} L_a L_b \in H, \\ \forall u \in E,\ \forall h \in H & \varphi(u,h) = L^{-1}_{h(u)} h L_u h^{-1} \in H, \end{array} \tag{6}$$

where L_a is the left translation by a in $\langle E,\bullet,1\rangle$. In the set

$$E \times H = \{(u,h) |\, u \in E,\, h \in H\}$$

we define the operation

$$(u,h_1) * (v,h_2) \stackrel{def}{=} (u \bullet h_1(v), l_{u,h_1(v)} \varphi(v,h_1) h_1 h_2) \tag{7}$$

(see [10]). In view of (6) this definition is correct.

On the set E we define the function:

$$\begin{array}{c} (u,h) : E \to E, \\ (u,h)(x) \stackrel{def}{=} u \bullet h(x). \end{array} \tag{8}$$

Lemma 3. *The following sentences are true:*

1. *The function $(u,h) : E \to E$ is an action, i.e.*
   (a) *it is a permutation on the set E,*

(*b*) *if* $(u,h_1)(x)=(v,h_2)(x)$ *for all* $x\in E$, *then* $u=v$ *and* $h_1=h_2$,

2. $(u,h_1)((v,h_2)(x))=((u,h_1)*(v,h_2))(x)$ *for any* $x\in E$, *where* $*$ *is defined by* (7),

3. $(1,id)$ *is an unit of* $\langle E\times H,*\rangle$,

4. $(\,h^{-1}(u\backslash 1),\,(L_uhL_{h^{-1}(u\backslash 1)})^{-1}\,)$ *is an inverse element of* (u,h) *in* $\langle E\times H,*,(1,id)\rangle$,

5. $G=\langle E\times H,*,(1,id)\rangle$ *is a group.*

Proof. 1a. According to (8), we have $(u,h)(x)=u\bullet h(x)=L_uh(x)$. Because L_u is a permutation of the set E, then also L_uh is a permutation of E. Obviously $(1,id)(x)=x$.

1b. If $(u,h_1)(x)=(v,h_2)(x)$ for all $x\in E$, then $L_uh_1(x)=L_vh_2(x)$. This for $x=1$ gives $L_u=L_v$. Thus $u=v$. Hence $h_1(x)=h_2(x)$ for all $x\in E$, and, in the consequence, $h_1=h_2$.

2. For $\alpha=(u,h_1)$ and $\beta=(v,h_2)$ we have

$$\begin{aligned}\alpha(\beta(x))&=(u,h_1)((v,h_2)(x))=(u,h_1)(v\bullet h_2(x))\\&=u\bullet h_1(v\bullet h_2(x))=L_uh_1L_vh_2(x)\,.\end{aligned}$$

But on the other hand

$$\begin{aligned}((u,h_1)*(v,h_2))(x)&=(u\bullet h_1(v),l_{u,h_1(v)}\varphi(v,h_1)h_1h_2)(x)\\&=(u\bullet h_1(v))\bullet L^{-1}_{u\bullet h_1(v)}L_uL_{h_1(v)}L^{-1}_{h_1(v)}h_1L_vh_1^{-1}h_1h_2(x)\\&=L_{u\bullet h_1(v)}L^{-1}_{u\bullet h_1(v)}L_uh_1L_vh_2(x)=L_uh_1L_vh_2(x)\,.\end{aligned}$$

So $(u,h_1)((v,h_2)(x))=((u,h_1)*(v,h_2))(x)$.

3. According to the previous paragraph we have

$$((u,h_1)*(v,h_2))(x)=L_uh_1L_vh_2(x),\tag{9}$$

which gives

$$((1,id)*(u,h))(x)=L_1id\,L_uh(x)=L_uh(x)=(u,h)(x)$$

for any $x\in E$. Thus $(1,id)*(u,h)=(u,h)$.

We obtain also

$$((u,h)*(1,id))(x)=L_uhL_1id\,(x)=L_uh(x)=(u,h)(x)\,.$$

Hence $(u,h)*(1,id)=(u,h)$, which proves that $(1,id)$ is a two-sided unit.

4. According to the general properties of $\{L_u\}_{u\in E}$ in $LM(\langle E,\bullet,1\rangle)$ to $LI(\langle E,\bullet,1\rangle)\subseteq H$ we have $L_u^{-1}=L_{u\backslash 1}h'$ for some $h'\in H$. So

$$(h^{-1}(u\backslash 1),(L_uhL_{h^{-1}(u\backslash 1)})^{-1})=(h^{-1}(u\backslash 1),L^{-1}_{h^{-1}(u\backslash 1)}h^{-1}L_u^{-1})$$
$$=(h^{-1}(u\backslash 1),L^{-1}_{h^{-1}(u\backslash 1)}h^{-1}L_{u\backslash 1}hh'')=(h^{-1}(u\backslash 1),\varphi(u\backslash 1,h^{-1})h'')\in E\times H.$$

But by (9) we have also

$$((u,h)*(h^{-1}(u\backslash 1),(L_uhL_{h^{-1}(u\backslash 1)})^{-1})(x)$$
$$=L_uhL_{h^{-1}(u\backslash 1)}L^{-1}_{h^{-1}(u\backslash 1)}h^{-1}L_u^{-1}(x)=x,$$

which proves $(u,h)*(h^{-1}(u\backslash 1),(L_uhL_{h^{-1}(u\backslash 1)})^{-1}=(1,id)$.

In the same way

$$((h^{-1}(u\backslash 1),(L_uhL_{h^{-1}(u\backslash 1)})^{-1}*(u,h))(x)$$
$$=L_{h^{-1}(u\backslash 1)}L^{-1}_{h^{-1}(u\backslash 1)}h^{-1}L_u^{-1}L_uh(x)=x$$

implies $(h^{-1}(u\backslash 1),(L_uhL_{h^{-1}(u\backslash 1)})^{-1}*(u,h)=(1,id)$.

5. It is a simple consequence of 2, 3 and 4. □

Lemma 4. *Let $G=\langle E\times H,*,(1,id)\rangle$ be a group. Then*

1. *$\hat{H}=\langle H^*,*,(1,id)\rangle$ (where $H^*\rightleftharpoons\{(1,h)|\,h\in H\}$) is a subgroup of G and it is isomorphic to the group H.*
2. *$\hat{T}\rightleftharpoons\{(u,id)|\,u\in E\}$ is a left transversal in G to its subgroup $\hat{H}$ and the operation of $\langle E,\overset{(\hat{T})}{\bullet},1\rangle$ coincides with the operation of $\langle E,\bullet,1\rangle$.*

Proof. 1. According to (9) we have

$$((1,h_1)*(1,h_2))(x)=h_1h_2(x)=(1,h_1h_2)(x),$$

which proves that $\hat{H}=\langle H^*,*,(1,id)\rangle$ is a subgroup of G. Moreover, the bijection $\psi: H^*\to H,\quad \psi((1,h))=h$ defines an isomorphism between groups $\hat{H}$ and H.

2. In view of (9) we have

$$((u,id)*(1,h))(x)=L_uid\,L_1h(x)=L_uh(x)=(u,h)(x),$$

which gives $(u,id)*(1,h)=(u,h)$. Then for any $u\in E$ the set

$$H_u\rightleftharpoons(u,id)*H^*=\{(u,h)|\,h\in H\}$$

is a left coset of $\hat{H}$ in G. Obviously $(u, id) \in H_u$ and $(1, id) \in H_1 = \hat{H}$.

So, $\hat{T} \rightleftharpoons \{(u, id) | \, u \in E\}$ is a left transversal in G to its subgroup $\hat{H}$. Moreover, for $\langle E, \overset{(\hat{T})}{\bullet}, 1\rangle$ we have $u \overset{(\hat{T})}{\bullet} v = z$, $(u, id) * (v, id) = (z, h)$, $z = u \bullet v$ and $h = l_{u,v}$, which implies $u \overset{(\hat{T})}{\bullet} v = u \bullet v$. □

3. The case of a left A_l-loop

Note that if in the previous part of this work the permutation $h \in H$ is an automorphism of $\langle E, \bullet, 1\rangle$, then any $u, x \in E$ we have

$$hL_u h^{-1}(x) = h(u \bullet h^{-1}(x)) = h(u) \bullet x = L_{h(u)}(x).$$

Thus $hL_u h^{-1} = L_{h(u)}$ and $\varphi(u, h) = L^{-1}_{h(u)} hL_u h^{-1} = L^{-1}_{h(u)} L_{h(u)} = id$.

This means that the study of the general construction of a semidirect product from the previous chapter can be interesting in the case when

$$LI(\langle E, \bullet, 1\rangle) \subseteq H \subseteq Aut\,(\langle E, \bullet, 1\rangle).$$

In this case the left loop $\langle E, \bullet, 1\rangle$ is a left special loop (left A_l-loop) and (7) can be written in the form

$$(u, h_1) * (v, h_2) = (u \bullet h_1(v), l_{u,h_1(v)} h_1 h_2). \tag{10}$$

Obviously such defined product has all properties mentioned in Lemmas 3 and 4.

Remark 3. By Lemma 3, for any $u \in E$ and $h \in H$ we have

$$(u, h)^{-1} = (h^{-1}(u\backslash 1), (L_u L_{u\backslash 1} h)^{-1}),$$

and, in the consequence, $(u, id)^{-1} = (u\backslash 1, (L_u L_{u\backslash 1})^{-1})$.

Remark 4. Formula (10) coincides with the formula of a gyrosemidirect product of a left gyrogroup and its gyroautomorphism group (see [11, 4]).

References

[1] **R. Baer**: *Nets and groups. 1.* Trans. Amer. Math. Soc. **46** (1939), 110 – 141.

[2] **I. Burdujan**: *Some remarks about geometry of quasigroups*, (Russian), Mat. Issled. **39** (1976), 40 – 53.

[3] **V. D. Belousov**: *Foundations of quasigroup and loop theory*, (Russian), Nauka, Moscow 1967.

[4] **T. Foguel and A. Ungar**: *Transversals, loops and gyrogroups*, Preprint of NDSY, 1998.

[5] **M. I. Kargapolov and Yu. I. Merzlyakov**: *Foundations of group theory*, (Russian), 3rd edition, Nauka, Moscow 1982.

[6] **E. A. Kuznetsov**: *Transversals in groups. 1. Elementary properties*, Quasigroups and Related Systems **1** (1994), 22 – 42.

[7] **E. A. Kuznetsov**: *Transversals in groups. 2. Loop transversals in a group by the same subgroup*, Quasigroups and Related Systems **6** (1999), 1 – 12.

[8] **L. V. Sabinin**: *About equivalence of the categories of loops and homogeneous spaces*, (Russian), Dokl. AN SSSR, **205** (1972), 533 – 537.

[9] **L. V. Sabinin**: *About geometry of loops*, (Russian), Mat. zametki, **12** (1972), 605 – 616.

[10] **L. V. Sabinin and O. I. Mikheev**: *Quasigroups and differential geometry*, Chapter XII in the book *Quasigroups and loops: Theory and Applications*, Helderman-Verlag, Berlin 1990, 357 – 430.

[11] **A. Ungar**: *Thomas Precession: Its underlying gyrogroup axioms and their use in hyperbolic geometry and relativistic physics*, Foundations of Physics, **27** (1997), 881 – 951.

Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
str. Academiei 5
MD-2028 Chishinau
MOLDOVA
e-mail: ecuz@math.md

Received August 20, 2001

Quasigroups and Related Systems **8** (2001), 45 – 65

Subtree-counting loops

François Lemieux, Cristopher Moore and Denis Thérien

Abstract

An important objective of the algebraic theory of languages is to determine the combinatorial properties of the languages recognized by finite groups and semigroups. In [20], finite nilpotent groups are characterized as those groups that have the ability to count subwords. In this paper, we attempt to generalize this result to finite loops. We introduce the notion of *subtree-counting* and define subtree-counting loops. We prove a number of algebraic results. In particular, we show that all subtree-counting loops and their multiplication groups are nilpotent. We conclude with several small examples and a number of open questions related to computational complexity.

1. Introduction

A body of recent work focuses on the computational complexity of various problems involving algebraic structures, such as evaluating circuits and expressions [2, 3, 4], predicting cellular automata [15, 16], solving equations [11], and communication complexity [19]. While these algebraic problems are interesting in their own right, they also offer elegant characterizations of some low-lying complexity classes, and may even help us prove new separations between them.

Most of this work has dealt with associative structures, namely groups, semigroups and monoids, largely because the idea of a syntactic monoid is familiar from the theory of finite-state automata. However, some progress has been made in the non-associative case as well [5, 6, 13, 10, 17]. Here, concepts such as solvability generalize in several competing ways, and finding the appropriate one for a given problem can be difficult. For instance, the complexity of circuit evaluation and expression evaluation over loops

2000 Mathematics Subject Classification: 20N05, 68Q70
Keywords: finite loop, nilpotency, formal language, tree, subtree.

is determined by two different generalizations of solvability, which we call polyabelianness (being a certain kind of product of Abelian groups) and $\mathcal{M}$-solvability (having a solvable multiplication group) [17].

In this paper, we attempt to generalize the concept of nilpotence, by building on Thérien's result that nilpotent groups are characterized by counting subwords up to some constant size [20]. In the non-associative case, we expect subwords to become subtrees, and so we explore loops which count subtrees of constant size. We find that many of the properties of nilpotent groups hold true for these loops as well.

The paper is structured as follows. After defining some terms in algebra, we review the properties of nilpotent groups and their ability to count subwords. We then introduce the notion of subtree counting and define subtree-counting loops. We prove a number of algebraic results relating these to nilpotent and $\mathcal{M}$-nilpotent loops. We conclude with several small examples and a number of open questions related to computational complexity.

2. Algebraic definitions

For the theory of quasigroups and loops, we refer the reader to [1, 7, 8, 18]. We will use the following terms, and additional definitions are given in the text.

By a *groupoid* $(G, \cdot)$ is mean a binary operation $f : G \times G \to G$, written $f(a, b) = a \cdot b$ or simply ab. The *order* of a groupoid is the number of elements in G, written $|G|$.

A *quasigroup* is a groupoid whose multiplication table is a *Latin square*, in which each symbol occurs once in each row and each column. Equivalently, for every a, b there are unique elements a/b and $a\backslash b$ such that $(a/b) \cdot b = a$ and $a \cdot (a\backslash b) = b$; thus the left (right) *cancellation property* holds, that $bc = bd$ (resp. $cd = bd$) implies $c = d$.

An *identity* is an element 1 such that $1 \cdot a = a \cdot 1 = a$ for all a. A *loop* is a quasigroup with an identity.

A groupoid is *associative* if $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all a, b, c. A *semigroup* is an associative groupoid, and a *monoid* is a semigroup with identity. A *group* is an associative quasigroup; groups have inverses and an identity. In a group, the *order* of an element a is the smallest $p > 0$ such that $a^p = 1$ (or $pa = 0$ in an Abelian group).

Two elements a, b *commute* if $a \cdot b = b \cdot a$. A groupoid is *commutative* if all pairs of elements commute. Commutative groups are also called *Abelian*.

We will use + instead of · for products in an Abelian group, and call the identity 0 instead of 1. The simplest Abelian group is the *cyclic group* $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, the set of integers with addition mod p.

A *subgroupoid* (*subquasigroup*, *subloop*, etc.) of a finite groupoid G is a subset $H \subseteq G$ such that $b_1 \cdot b_2 \in H$ for all $b_1, b_2 \in H$. The subgroupoid generated by a set S, consisting of all possible products of elements in S, is written $\langle S \rangle$.

A *homomorphism* is a function φ from one groupoid $(A, \cdot)$ to another $(B, \star)$ such that $\varphi(a \cdot b) = \varphi(a) \star \varphi(b)$. An *isomorphism* is a one-to-one and onto homomorphism; we will write $A \cong B$ if A and B are isomorphic.

An *equivalence relation* is a relation $\sim$ that is reflexive and transitive. Its *index* is the number of equivalence classes. An equivalence relation is a *congruence* with respect to G if $a \sim b$ and $c \sim d$ implies that $ac \sim bd$. (For infinite quasigroups, we also demand that $a/c \sim b/d$ and $a\backslash c \sim b\backslash d$.) We can then define a groupoid $G/\!\sim$ whose elements are $\sim$'s equivalence classes, and the obvious map from G to $G/\!\sim$ is a homomorphism. Conversely, for any homomorphism φ we can define a congruence $a \sim b$ if $\varphi(a) = \varphi(b)$. The groupoid $G/\!\sim$ is called a *quotient* or *factor* of G. A groupoid is *simple* if it has no factors other than $\{1\}$ and itself.

A *divisor* is a factor of a subgroupoid. Since a sub of a factor is the factor of a sub, the divisor relation is the transitive closure of the sub and factor relations.

The *left (right) cosets* of a subloop $H \subseteq G$ are the sets

$$aH = \{ah \,|\, h \in H\} \quad \text{and} \quad Ha = \{ha \,|\, h \in H\}$$

for each $a \in G$. A subloop H is *normal* if the following hold for all $a, b \in G$:

$$aH = Ha, \quad a(bH) = (ab)H, \quad \text{and} \quad (aH)b = a(Hb)$$

Then the relation

$$a \sim b \quad \text{if} \quad a = bh \quad \text{for some} \quad h \in H$$

is a congruence, the left and right cosets coincide, and the cosets form a quotient subloop G/H.

The *commutator* of two elements in a loop is $[a, b] = ab \,/\, ba$, i.e. the unique element such that $ab = [a, b](ba)$. The *associator* of three elements is $[a, b, c] = (ab)c \,/\, a(bc)$, i.e. the unique element such that $(ab)c = [a, b, c](a(bc))$. The subloop $\langle [G, G], [G, G, G] \rangle$ generated by all possible commutators and associators in a loop G is called the *commutator-associator*

subloop or *derived subloop* G'. It is normal, and it is the smallest subloop such that the quotient G/G' is an Abelian group.

The *derived series* of a loop G is the series of normal subloops

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots$$

where $G_{i+1} = G_i'$. A loop is *solvable of degree* k if $G_k = \{1\}$.

The *center* of a loop is the set of elements that associate and commute with everything,

$$Z(G) = \{c \,|\, cx = xc,\ c(xy) = (xc)y = x(yc) \text{ for all } x, y \in G\}.$$

It is a normal subloop of G, and is always an Abelian group.

The *upper central series* of a loop is $\{1\} = Z_0 \subset Z_1 \subset \cdots$ where Z_{i+1}/Z_i is the center of G/Z_i. The *lower central series* is $G = \Gamma_0 \supset \Gamma_1 \supset \cdots$ where $\Gamma_{i+1} = \langle [G, \Gamma_i], [G, G, \Gamma_i] \rangle$ is generated by the commutators and associators of Γ_i with elements of G. A loop is *nilpotent of class* k if $Z_k = G$ or if $\Gamma_k = \{1\}$; these turn out to be equivalent and k is the same in either case.

In a groupoid G, we can define left and right multiplication as functions $L_a(b) = a \cdot b$ and $R_a(b) = b \cdot a$, namely the rows and columns of the multiplication table. The *left (right) multiplication semigroup* $\mathcal{M}_L(G)$ (resp. $\mathcal{M}_R(G)$) is the set of functions on G generated by the L_a (resp. the R_a), and the *multiplication semigroup* is the set of functions generated by both. If G is a quasigroup, the L_a and R_a are permutations, so $\mathcal{M}_L(G)$, $\mathcal{M}_R(G)$ and $\mathcal{M}(G)$ are groups.

A *pseudovariety* is a class of groupoids V such that subgroups, factors, and finite direct products of groupoids in V are also in V. The solvable and nilpotent loops both form pseudovarieties.

For a given alphabet A, we define the groupoid $A^{(+)}$ as the smallest set that includes A and such that whenever f and g belong to $A^{(+)}$ then their formal product (fg) also belongs to $A^{(+)}$. It is isomorphic to the set of non-empty binary trees whose leaves are labelled with elements of A, or the set of parenthesized words generated by the grammar $S \to (S \cdot S)$, $S \to A$. The *free groupoid over* A is the set $A^{(*)} = A^{(+)} \cup \{1\}$, where 1 is the empty tree. The *free monoid over* A is the associative version of this, namely the set A^* of finite words over A, where the product is by concatenation and 1 is the empty word.

The *yield* of a labelled tree is the word formed by reading its leaves from left to right, which is clearly a homomorphism from $A^{(*)}$ to A^*. Thus free monoids are factors of free groupoids under the congruence that identifies trees with the same yield, and so removes the non-associativity of the groupoid.

Moreover, every finite groupoid (monoid) is a divisor of the free groupoid (monoid) over some finite alphabet, i.e. it can be derived from a free object by imposing some congruence with a finite index.

The length of a word w, or the number of leaves in a tree w, is denoted $|w|$. Except for the free algebras, all loops used in this paper are finite.

3. Nilpotence and subword counting

Counting subwords is a well-known operation in combinatorial algebra (e.g. Ch. 6 of [14]). If x and w are two words over some alphabet A, then $|x|_w$ is the number of ways that x can be written

$$x = y_0 w_1 y_1 w_2 \cdots w_k y_k$$

where $w_1 w_2 \cdots w_k = w$ and $y_i \in A^*$. For instance, $|abab|_{ab} = 3$. (Note that many authors write $\binom{x}{w}$ instead of $|x|_w$.) If x and y are both words over A, we can define the subword counts of their product recursively:

$$|xy|_w = \sum_{\substack{u,v \in A^* \\ uv = w}} |x|_u |y|_v \tag{1}$$

summing over all the ways to break w into a pair of words.

In a group or monoid, we can define two words as equivalent if they evaluate to the same element. It is interesting to ask what exactly about a long word makes it evaluate to one element or another; different groups are 'sensitive' to different properties of the word. To make this precise, we say that a language $L \subset A^*$ is *recognized* by a monoid M if there is a homomorphism h from A^* to M, and a subset $K \subset M$, such that $L = h^{-1}(K)$. In other words, h maps each symbol of A to an element of M, and L is the set of words where the resulting string evaluates to an accepting element of M.

In the associative case, Thérien [20] showed that nilpotent groups are exactly those that are sensitive to counting subwords up to a certain fixed length. Specifically, define an equivalence class $\sim_k^p$ that counts, $\bmod p$, subwords of length up to k:

$$x \sim_k^p y \quad \text{if} \quad |x|_u \equiv |y|_u \bmod p \quad \text{for all} \quad |u| \leqslant k$$

It is easy to show from Equation 1 that this is a congruence. Then we have

Theorem 1 (Thérien). *If a group G has order p and is generated by m elements, it is nilpotent of class k if and only if it is a divisor of $A^*/\sim_k^p$ where A is the free monoid on m symbols. Therefore, any language recognized by G is a union of equivalence classes of $\sim_k^p$.*

Thus nilpotent groups can be characterized completely by the combinatorics of subwords.

For instance, if we take the free group with two generators a and b and count the subwords a, b, ab and ba mod 2, we get an 8-element group

$$\{1, a, b, ab, ba, aba, bab, abab\}$$

Note, for instance, that $abab = baba$ since (mod 2) both have zero a's, zero b's, one ab, and one ba. Furthermore, $abab$ commutes with every element. The reader can check that this is isomorphic to the dihedral group D_4, the symmetries of the square, where a and b correspond to reflections around axes 45° apart, and $abab$ is a 180° rotation.

Similarly, if we have two generators i and j and we count i's and j's mod 2, but combine the counts of ii, jj and ji by adding them together mod 2, we get the quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. The combined count of ii, jj and ji gives the sign if $ij = k$ is defined as positive, which makes sense since $i^2 = j^2 = -1$ and $ji = -k$.

To put it differently, $\{a, b\}^*/\sim_2^2$ is a 32-element group, of which both D_4 and Q_8 are factors. (Since there are six subwords of length $\leqslant 2$, namely a, b, aa, ab, ba and bb, in principle this group could have 64 elements. However, subword counts are not independent of each other.)

4. Subtree-counting loops

In the non-associative case, subwords presumably become subtrees. Counting subtrees is actually simpler than counting subwords, since there is only one way to divide a binary tree into smaller ones. The intuitive definition seems to be the following, where x, y, u, v are elements of the free groupoid $A^{(*)}$ and $a, b \in A$ are generators:

$$\begin{aligned} |1|_a &= 0 \\ |a|_1 &= 0 \\ |a|_a &= 1 \\ |a|_b &= 0 \\ |(xy)|_a &= |x|_a + |y|_a \\ |(xy)|_{(uv)} &= |x|_{(uv)} + |y|_{(uv)} + |x|_u |y|_v \end{aligned}$$

Given $p \geqslant 2$ and $k \geqslant 0$, define $x \sim_k^p y$ iff $|x|_u \equiv |y|_u \pmod{p}$ for all $u \in A^{(*)}$ of size at most k. The following lemma follows directly from the definition:

Lemma 2. *The relation $\sim_k^p$ is a congruence of finite index.*

Define $D_k^p = \{x \in A^{(*)} \mid x \sim_k^p 1\}$

Lemma 3. *$A^{(*)}/\sim_k^p$ is a finite loop with identity D_k^p*

Proof. We want to prove that $(xy) \sim_k^p (xz)$ implies $y \sim_k^p qz$ (the proof of left cancellation is symmetric). It suffices to show that for all $s \in A^{(*)}$ of size less than k, $|(xy)|_s = |(xz)|_s$ implies that $|y|_s = |z|_s$.

The proof is by mathematical induction on $|s|$. This is clear when $|s| \leqslant 1$. Otherwise $s = (uv)$ and

$$\begin{aligned} |(xy)|_s &\equiv |x|_s + |y|_s + |x|_u|y|_v \\ &\equiv |x|_s + |z|_s + |x|_u|z|_v \\ &\equiv |(xz)|_s \,(\mathrm{mod}\, p) \end{aligned}$$

Hence, there exists some constant $c = |x|_u$ such that

$$|y|_s + c|y|_v \equiv \quad |z|_s + c|z|_v \,(\mathrm{mod}\, p)$$

By the inductive hypothesis, we have that $|y|_v \equiv |z|_v$. So, we obtain $|y|_{(uv)} \equiv |z|_{(uv)}$ and $y \sim_k^p z$. □

Definition 1. Loops that divide $A^{(*)}/\sim_k^p$ are called *subtree-counting loops of class k.*

When a subtree-counting loop is express as an algebra $(G, \cdot, \backslash, /)$, we can deduce how to count subtrees in quotients x/y and $y\backslash x$:

Lemma 4.

a) $|x/y|_a \equiv |y\backslash x|_a \equiv |x|_a - |y|_a$ if $a \in A$

b) $|x/y|_{uv} \equiv |x|_{uv} - |y|_{uv} - |x/y|_u\,|y|_v$

c) $|y\backslash x|_{uv} \equiv |x|_{uv} - |y|_{uv} - |y|_u\,|y\backslash x|_v$

Proof.

$$|x|_a \equiv |(x/y)y|_a \equiv |x/y|_a + |y|_a$$

$$|x|_{uv} \equiv |(x/y)y|_{uv} \equiv |x/y|_{uv} + |y|_{uv} + |x/y|_u\,|y|_v$$

and similarly for $y\backslash x$. □

The definition of $A^{(*)}/\sim_k^p$ implies that for any $s,t \in A^{(+)}$ satisfying $s \sim_k^p t$, we have that s and t evaluate to the same element in $A^{(*)}/\sim_k^p$. This property is generalized in the following lemma.

Lemma 5. *A loop G is subtree-counting if and only if there exists two positive integers k and p such that for any $s,t \in G^{(+)}$ satisfying $s \sim_k^p t$, we have that s and t evaluate to the same element in G.*

Proof. Let G be a subtree counting loop and consider first the special case where $G = A^{(*)}/\sim_k^p$. Without loss of generality, we can assume that $A \subseteq G$, which means that A is a basis for G. By definition, we know that for all $x,y \in A^{(+)}$, if $x \sim_k^p y$, then x and y evaluate to the same element in G.

Let $h : G \to A^{(+)}$ be any mapping such that $h(g)$ evaluates to g, for all $g \in G$ and such that $h(a) = a$ for all $a \in A$. We can extend h in the natural way to a groupoid morphism $h : G^{(+)} \to A^{(+)}$. Thus, for any $t \in G^{(+)}$, we have that t and $h(t)$ evaluate to the same element in G.

Let $u \in G^{(+)}$ be such that $|u| \leqslant k$, let $X(u)$ be the set of all leaves of u that are in A, and let $Y(u)$ be the set of all other leaves. Given $v \in A^{(+)}$, we are interested by the occurrences of v in $h(u)$ that contains all the leaves from $X(u)$ and at least one leaf from $h(g)$, for each $g \in Y(u)$. We denote the number of such occurrences with $\|h(u)\|_v$. We have

$$|h(s)|_v = \sum_{\substack{u \in G^{(+)} \\ |u| \leqslant |v|}} |s|_u \cdot \|h(u)\|_v$$

Hence, $s \sim_k^p t$ implies that $h(s) \sim_k^p h(t)$ and that s and t evaluate to the same element in G.

Consider now the general case where G divides $A^{(*)}/\sim_k^p$. Let S be a subloop of G and let $h : S \to G$ be a loop morphism. Define the function $h^{-1} : G \to S$ by choosing $h^{-1}(g)$ to be any element in S such that $h(h^{-1}(g)) = g$ and extend it in the natural way to a groupoid morphism $h^{-1} : G^{(+)} \to (h^{-1}(G))^{(+)}$.

Let $x,y \in G^{(+)}$ be such that $x \sim_k^p y$. Then, we must have $h^{-1}(x) \sim_k^p h^{-1}(y)$ and, since $h^{-1}(x)$ and $h^{-1}(y)$ belong to $A^{(*)}/\sim_k^p$, they both evaluate to the same element in S. Since h is a morphism, x and y must evaluate to the same element in G.

The other direction of the proof is immediate. □

5. Properties of subtree-counting loops

Let $G = A^{(*)}/\sim_k^p$ where $p \geqslant 2$ and $k \geqslant 1$. Let $\eta : A^{(*)} \to A^{(*)}/\sim_k^p$ be the natural morphism. For $0 \leqslant i \leqslant k$, let $D_i^p = \{x \in A^{(*)} \mid x \sim_i^p 1\}$ and define $\Delta_i^p = \eta(D_i^p)$, a normal subloop of G. We can then define the following descending series of normal subloops, which we call the *subtree series:*

$$G = \Delta_0^p \supseteq \Delta_1^p \supseteq \cdots \supseteq \Delta_k^p = \{1\}$$

This series can still be defined if G is a proper divisor of $A^{(*)}/\sim_k^p$. In this case, there exists a subloop $S \subseteq A^{(*)}/\sim_k^p$ and a loop morphism $h : S \to G$. Hence, it suffices to define $\Delta_i^p = h(\eta(D_i^p) \cap S)$.

Commutators and associators are contained in various Δ_j^p because their counts of small subtrees cancel out, as the next two lemmas show.

Lemma 6. *If $x \in \Delta_k^p$ and $y \in \Delta_l^p$, then their commutator $[x, y] \in \Delta_{k+l+1}^p$.*

Proof. Let S be defined as above. We observe that any commutator y of G is the morphic image of a commutator x in S. Hence, if $x \in \eta(D_i^p)$ then $y \in \Delta_i^p$. Consequently, it suffices to consider the case where $G = A^{(*)}/\sim_k^p$. The reader can show that $|[x, y]|_a = 0 \pmod p$ for all $a \in A$, and that

$$|[x, y]|_{uv} \equiv |x|_u\,|y|_v - |y|_u\,|x|_v - |[x, y]|_u\,|yx|_v \,(\mathrm{mod}\, p)$$

If $|[x, y]|_w \equiv 0$ for all words shorter than uv, then the last term is zero, and the first two terms are also zero unless $|u| > k$ and $|v| > l$ or vice versa. Thus the shortest subword with nonzero count in $[x, y]$ has length at least $k + l + 2$, so $[x, y] \in \Delta_{k+l+1}$. □

Lemma 7. *If $x \in \Delta_k^p$, $y \in \Delta_l^p$, and $z \in \Delta_m^p$, then their associator $[x, y, z] \in \Delta_{k+l+m+2}^p$.*

Proof. Again, it is sufficient to consider the case where $G = A^{(*)}/\sim_k^p$. As in the previous lemma, $|[x, y, z]|_a \equiv 0$ for all $a \in A$. If $u = rs$ and $v = tw$, then

$$|[x, y, z]|_{uv} \equiv |x|_r\,|y|_s\,|z|_{tw} - |x|_{rs}\,|y|_t\,|z|_w - |[x, y, z]|_u\,|(xy)z|_v \,(\mathrm{mod}\, p)$$

(the first and second terms, respectively, disappear if $|u| = 1$ or $|v| = 1$). So the shortest word with nonzero count must be the product of three words of length greater than k, l and m respectively; its length is then at least $k + l + m + 3$, so $[x, y, z] \in \Delta_{k+l+m+2}$. □

Thérien's result [20] shows that in the associative case, subtree-counting and nilpotence are the same thing. In the non-associative case, this is still true in one direction:

Theorem 8. *If a loop G is subtree-counting of class k, it is nilpotent of class k.*

Proof. Assume G divides $A^{(*)}/\sim_k^p$ for some p and k. Recall the definition of the lower central series Γ_i. We have $\Delta_0^p = \Gamma_0 = G$, and $\Gamma_i \subset \Delta_i^p$ follows by induction from lemmas 3 and 4 for all $i \geqslant 0$. Therefore, if $\Delta_k^p = \{1\}$, then $\Gamma_k = \{1\}$. □

If the loop is commutative, we can make this stronger:

Theorem 9. *If a loop G is commutative and subtree-counting of class k, it is nilpotent of class $\lceil k/2 \rceil$.*

Proof. $\Delta_0^p = \Gamma_0 = G$, and if all commutators are the identity, then $\Gamma_i \subset \Delta_{2i}^p$ follows by induction from lemma 4 for all $i \geq 0$. Therefore, if $\Delta_k^p = \{1\}$, then $\Gamma_j = \{1\}$ where $2j \geqslant i$. □

Nilpotence implies solvability [7], but we can show that a loop's solvability degree is exponentially smaller than its subtree-counting class:

Theorem 10. *If a loop G is subtree-counting of class k, it is solvable of degree $\lceil \log_2(k+1) \rceil$. If it is also commutative, it is solvable of degree $\lceil \log_3(k+1) \rceil$.*

Proof. Recall the definition of the derived series G_i. We have $\Delta_0^p = G_0 = G$, and $G_j \subset \Delta_i^p$ implies $G_{j+1} \subset \Delta_{2i+1}^p$ by lemmas 3 and 4. Therefore, $G_i \subset \Delta_{2^i-1}^p$ for all $i \geq 0$, so if $\Delta_k^p = \{1\}$ then $\Gamma_j = \{1\}$ where $2^j \geq k+1$. If all commutators are the identity, then $G_j \subset \Delta_i^p$ implies $G_{j+1} \subset \Delta_{3i+2}^p$ by lemma 4. Therefore $G_i \subset \Delta_{3^i-1}^p$, so if $\Delta_k^p = \{1\}$ then $\Gamma_j = \{1\}$ where $3^j \geq k+1$. □

We close this section with a characterization of the first few classes of subtree-counting loops. Recall that the *center* of a loop is the set of elements that commute and associate with all other elements. We also say that a loop is *associator-distributive* if $[wx, y, z] = [w, y, z]\,[x, y, z]$ and similarly on the other two variables. Then:

Theorem 11. *Suppose a loop is subtree-counting of class k. If $k = 1$, it is an Abelian group. If $k = 2$, it is a group and nilpotent of class 2. If $k = 3$, it is associator-distributive and its associators are in its center.*

Proof. If $k = 1$, all commutators and associators are the identity by lemmas 3 and 4. If $k = 2$, all associators are the identity by lemma 4, so it is a group and is subword-counting of class 2. If $k = 3$, we can check that an associator $[u, v, w]$ commutes with any element x by counting subtrees. If $|s| \leqslant 3$,

$$|x\,[u, v, w]|_s \equiv |x|_s + |[u, v, w]|_s \equiv |[u, v, w]\,x|_s \,(\mathrm{mod}\, p)$$

since $[u, v, w]$ contains no subtrees of size 1 or 2 by Lemma 7. A similar argument shows that an associator associates with any pair of elements. To show associator-distributivity, since $[wx, y, z]$ contains no subtrees of size 1 or 2, we just have to count subtrees of size 3. If $a, b, c \in A$, then

$$\begin{aligned} |[wx, y, z]|_{(ab)c} &\equiv |wx|_a\, |y|_b\, |z|_c \,(\mathrm{mod}\, p) \\ &\equiv (|w|_a + |x|_a)\, |y|_b\, |z|_c \,(\mathrm{mod}\, p) \\ &\equiv |[w, y, z]|_{(ab)c} + |[x, y, z]|_{(ab)c} \,(\mathrm{mod}\, p) \\ &\equiv |[w, y, z][x, y, z]|_{(ab)c} \,(\mathrm{mod}\, p) \end{aligned}$$

and similarly for $a(bc)$. □

6. $\mathcal{M}$-nilpotence and nilpotence

If we think of left and right multiplication as functions $L_a(b) = ab$ and $R_a(b) = ba$, the L_a and R_a are permutations given by the rows and columns of the multiplication table. Recall that the left (right) multiplication group of a loop G is the group generated by the L_a (resp. R_a), and the multiplication group $\mathcal{M}(G)$ is generated by both.

In [17], we used the idea of $\mathcal{M}$-solvability, the property of having a solvable multiplication group, to address the complexity of expression evaluation in loops. Here, we will say that a loop is *$\mathcal{M}$-nilpotent of class k* if its multiplication group is nilpotent of class k, and *left* (*right*) *$\mathcal{M}$-nilpotent* if its left (right) multiplication group is.

The following inclusions are known [7, 21]:

$$\mathcal{M}\text{-nilpotent} \Rightarrow \text{nilpotent} \Rightarrow \mathcal{M}\text{-solvable} \Rightarrow \text{solvable}$$

For groups, $\mathcal{M}(G)$ is in the variety generated by G, so $\mathcal{M}$-nilpotence and nilpotence coincide. In the non-associative case, however, the $\mathcal{M}$-nilpotent loops are a proper subclass of the nilpotent ones. For instance, the following

loop is nilpotent of class 2:

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

Its derived subloop $\{1, 2\}$ is also its center. However, its left, right and full multiplication groups are all equal to a 24-element group which is solvable of degree 2 but not nilpotent.

Then we can show that subtree-counting loops are $\mathcal{M}$-nilpotent:

Theorem 12. *If a loop G is subtree-counting of class k, then it is $\mathcal{M}$-nilpotent of class k.*

Proof. Define a *spine* as a tree where every node has at most one child which is not a leaf. An element of $\mathcal{M}(G)$ is characterized by its action on the elements of G. Since the multiplications L_a and R_a add leaves on the left and right, an element of $\mathcal{M}(G)$ corresponds to $|G|$ spines of the same shape, one for each element. For instance, $L_a R_b L_c$ corresponds to the spines $a((cx)b)$ for each $x \in G$ as shown in figure 1.

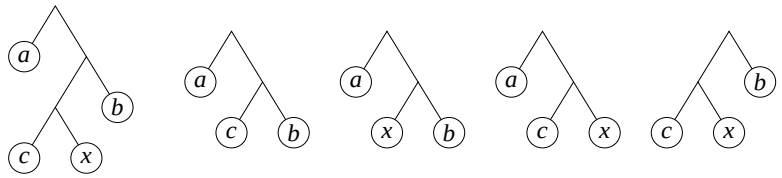


Figure 1: A spine corresponding to $m = L_a R_b L_c$ and its subtrees of size 3.

Let $m \in \mathcal{M}(G)$, and call these spines $m(x)$ for each $x \in G$. For each x, the spines $m(x)$ have two kinds of subtrees, namely those that don't include x and those that do. If a subtree of $m(x)$ of size k doesn't include x, it corresponds to a subword of m of size k. If it does include x, it corresponds to a subword of m of size $k - 1$. In either case, the subtrees of $m(x)$ are dictated by the subwords of m of the same size or smaller.

Therefore, if $m_1, m_2 \in \mathcal{M}(G)$ have the same subword counts of size k or less, then for all x their spines $m_1(x)$ and $m_2(x)$ have the same subtree counts of size k or less. Since G is subtree-counting of class k, $m_1(x) = m_2(x)$ for all $x \in G$, but this means that $m_1 = m_2$. Thus $\mathcal{M}(G)$ is subword-counting of class k, and by theorem 1 it is nilpotent of class k. □

We can also obtain a partial converse to the last part of theorem 11, with a purely algebraic corollary. Recall the notion of associator-distributivity from the previous section. Then:

Theorem 13. *If a loop G has the following properties:*

- *G is associator-distributive, and*
- *all of G's associators are in its center, and*
- *there is a set of generators A for G such that the subgroup of $\mathcal{M}_R(G)$ generated by their right multiplications, $\langle \{R_a \mid a \in A\} \rangle$ is nilpotent of class k,*

then it is subtree-counting of class $\max(3, k)$. *Therefore, G is $\mathcal{M}$-nilpotent of class* $\max(3, k)$.

Proof. If we are given a tree in $G^{(*)}$, we start by rewriting it as a tree in $A^{(*)}$ by replacing elements of G with products of elements of A. Now define a (*left*) *comb* in $A^{(*)}$ as a tree where every node's right child, if it has one, is a leaf. Inductively, the empty tree is a comb, and ca is a comb if c is a comb and $a \in A$. Since the parenthesization of a comb is fixed, we can denote it without ambiguity by its yield, e.g. $((ab)c)d$ is simply denoted $abcd$.

Then we start by converting an arbitrary tree to a comb with the same yield which is equivalent with respect to G, keeping track of the associators as we do so. We do this inductively, first transforming subtrees of depth 2, then subtrees of depth 3, and so on. Suppose that at some point in this process we are about to transform a subtree t. If t is already a comb, there is nothing to do. Otherwise, $t = ba$ where $b = b_1 \cdots b_k$ and $a = a_1 \cdots a_l$ are two combs of size $k \geqslant 1$ and $l \geqslant 2$, where $b_j, a_i \in A$ for all j, i. To apply the transformation, we use the following:

$$\begin{aligned} ba &= b(a_1 \cdots a_l) \\ &= (b(a_1 \cdots a_{l-1}))\, a_l\, [b, a_1 \cdots a_{l-1}, a_l] \\ &\vdots \\ &= (b_1 \cdots b_k a_1 \cdots a_l)\, \textstyle\prod_{i=2}^{l} [b, a_1 \cdots a_{i-1}, a_i] \end{aligned}$$

Since associators are in the center of G, each one can be moved to the side of the expression as it is created.

Now since G is associator-distributive, we can write this product of associators as

$$\prod_{j=1}^{k} \prod_{i=2}^{l} \prod_{h=1}^{i-1} [b_j, a_h, a_i]$$

There is a bijection between the associators $[b_j, a_h, a_i]$ in this product and the subtrees $b_j(a_h a_i)$ of size 3 rooted at the node where b and a meet. By induction, the transformation of a tree into a left comb creates precisely one associator $[a, b, c]$ for each subtree $a(bc)$ where $a, b, c \in A$.

Thus we can convert a tree into an equivalent comb, and the product of associators it takes to do this is a function only of subtrees of size 3. Since a left comb in $A^{(*)}$ is formed by composing a series of right multiplications R_a for $a \in A$, and since these generate a nilpotent group of class k, we can evaluate the comb by counting subcombs of size k. Since the comb has the same yield as the original tree, this is the same as counting subtrees of size k in the original tree and combining subtrees of the same yield.

Thus the value of the tree is determined by counting subtrees of size $\max(3, k)$, so G is subtree-counting of this class. Finally, G is $\mathcal{M}$-nilpotent of class $\max(3, k)$ by Theorem 12. □

Obviously, the third condition of Theorem 13 is satisfied whenever G is right-$\mathcal{M}$-nilpotent of class k. For instance, consider the octonion loop O_{16}, which consists of 16 elements $\{\pm 1, \pm i, \pm j, \pm k, \pm E, \pm I, \pm J, \pm K\}$. Its multiplication table is

1	i	j	k	E	I	J	K
i	-1	k	$-j$	I	$-E$	$-K$	J
j	$-k$	-1	i	J	K	$-E$	$-I$
k	j	$-i$	-1	K	$-J$	I	$-E$
E	$-I$	$-J$	$-K$	-1	i	j	k
I	E	$-K$	J	$-i$	-1	$-k$	j
J	K	E	$-I$	$-j$	k	-1	$-i$
K	$-J$	I	E	$-k$	$-j$	i	-1

which we extend to elements with minus signs in the obvious way. Just as the quaternions are commutative up to a sign, the octonions are associative up to a sign. Since all commutators and associators are in the center $\{\pm 1\}$, O_{16} is nilpotent of class 2. Moreover, the reader can check that it is associator-distributive and its right multiplication group (which has 128 elements) is nilpotent of class 2. Therefore, it is subtree-counting of class 3, and its full multiplication group (which has 1024 elements) is nilpotent of class 3.

The reader might hope that all nilpotent loops of class 2 are associator-distributive. This is not the case, as we will show below.

7. Examples

If we take the free groupoid on one generator $\{1, a, aa, a(aa), (aa)a, \ldots\}$ and consider equivalence classes that count subtrees up to size 3 (mod 2), then $\{a\}^{(*)}/\sim_3^2$ is a subtree-counting loop of class 3 with 8 elements. It is an extension of $\mathbb{Z}_2$ by $\mathbb{Z}_4$, and its multiplication table is

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \\ 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \\ 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \\ 5 & 6 & 8 & 7 & 3 & 4 & 2 & 1 \\ 6 & 5 & 7 & 8 & 4 & 3 & 1 & 2 \\ 7 & 8 & 6 & 5 & 1 & 2 & 4 & 3 \\ 8 & 7 & 5 & 6 & 2 & 1 & 3 & 4 \end{array} \tag{2}$$

The eight elements can be represented by 1, $2 = a((aa)a)$, $3 = aa$, $4 = a(a(a((aa)a)))$, $5 = a$, $6 = a(a((aa)a))$, $7 = (aa)a$, and $8 = a(aa)$. In fact, there are no non-associative subtree-counting loop with fewer than 8 elements, since the smallest non-associative nilpotent loops have 6 elements, and these all have a multiplication group $\mathbb{Z}_2 \wr \mathbb{Z}_3$ of order 24 that is solvable but not nilpotent (here $\wr$ is the wreath product [12]).

Counting subtrees of size 3 mod p for larger p gives class 3 loops of size cp^2 where c appears to depend only on $p(\mathrm{mod}\,6)$:

$$c = \begin{cases} 1 & \text{if} \quad p(\mathrm{mod}\,6) = 1 \text{ or } 5 \\ 2 & \text{if} \quad p(\mathrm{mod}\,6) = 2 \text{ or } 4 \\ 3 & \text{if} \quad p(\mathrm{mod}\,6) = 3 \\ 6 & \text{if} \quad p(\mathrm{mod}\,6) = 0 \end{cases}$$

We have checked this for $p \leqslant 25$, and we conjecture it is true for all p. Counting subtrees up to size $4(\mathrm{mod}\,2)$ gives a subtree-counting loop of class 4 with $128 = 2^7$ elements, and counting mod 3 gives $729 = 3^6$ elements.

All of these loops are generated by a single element, like the free groupoid of which they are factors. For an example with two generators, if we take the free groupoid on two generators a, b and impose the relations $a^2 = b^2 = 1$ and $xy = yx$ for all x, y, we get a subtree-counting loop of class 3 with 16

elements. Its multiplication table is

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	1	4	3	6	5	8	7	10	9	12	11	14	13	16	15
3	4	1	2	7	8	5	6	11	12	9	10	15	16	13	14
4	3	2	1	8	7	6	5	12	11	10	9	16	15	14	13
5	6	7	8	1	2	3	4	13	14	15	16	10	9	12	11
6	5	8	7	2	1	4	3	14	13	16	15	9	10	11	12
7	8	5	6	3	4	1	2	15	16	13	14	12	11	10	9
8	7	6	5	4	3	2	1	16	15	14	13	11	12	9	10
9	10	11	12	13	14	15	16	1	2	3	4	7	8	5	6
10	9	12	11	14	13	16	15	2	1	4	3	8	7	6	5
11	12	9	10	15	16	13	14	3	4	1	2	5	6	7	8
12	11	10	9	16	15	14	13	4	3	2	1	6	5	8	7
13	14	15	16	10	9	12	11	7	8	5	6	1	2	3	4
14	13	16	15	9	10	11	12	8	7	6	5	2	1	4	3
15	16	13	14	12	11	10	9	5	6	7	8	3	4	1	2
16	15	14	13	11	12	9	10	6	5	8	7	4	3	2	1

where the generators are (say) $5 = a$ and $9 = b$. Counting (mod 3), (mod 4), and mod 5 gives loops of 81, 256, and 625 elements respectively.

Going back to a one-symbol alphabet and counting (mod 2) the five subtrees of *depth* 2 or less, a, aa, $(aa)a$, $a(aa)$ and $(aa)(aa)$, gives a 16-element loop

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	1	4	3	6	5	8	7	10	9	12	11	14	13	16	15
3	4	5	6	9	10	11	12	1	2	14	13	15	16	8	7
4	3	6	5	10	9	12	11	2	1	13	14	16	15	7	8
5	6	7	8	2	1	4	3	13	14	16	15	10	9	11	12
6	5	8	7	1	2	3	4	14	13	15	16	9	10	12	11
7	8	1	2	13	14	15	16	6	5	9	10	12	11	3	4
8	7	2	1	14	13	16	15	5	6	10	9	11	12	4	3
9	10	11	12	4	3	6	5	15	16	7	8	2	1	14	13
10	9	12	11	3	4	5	6	16	15	8	7	1	2	13	14
11	12	14	13	16	15	9	10	7	8	1	2	4	3	6	5
12	11	13	14	15	16	10	9	8	7	2	1	3	4	5	6
13	14	15	16	8	7	2	1	12	11	4	3	5	6	9	10
14	13	16	15	7	8	1	2	11	12	3	4	6	5	10	9
15	16	10	9	11	12	14	13	3	4	6	5	7	8	2	1
16	15	9	10	12	11	13	14	4	3	5	6	8	7	1	2

Here $\{1,2\}$ is a normal subloop, and dividing it out gives the 8-element loop (2) above.

If we count just the balanced trees a, aa and $(aa)(aa)$ up to depth 2, we get another 8-element loop,

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

where the generator is (say) $2 = a$. This loop is not isomorphic to (2) since only two elements give the identity when squared. It is commutative but not associative, since $(22)3 = 5$ but $2(23) = 1$. However, like (2) it is an extension of $\mathbb{Z}_2$ by $\mathbb{Z}_4$.

In fact, all loop extensions of $\mathbb{Z}_2$ by $\mathbb{Z}_4$ are nilpotent and $\mathcal{M}$-nilpotent, since $\mathbb{Z}_2 \wr \mathbb{Z}_4$ is nilpotent of class 4. Similarly, all loop extensions of $\mathbb{Z}_2$ by $\mathbb{Z}_2^2$ are $\mathcal{M}$-nilpotent, since $\mathbb{Z}_2 \wr Z_2^2$ is nilpotent of class 3. We do not know if all of these are subtree-counting.

This loop also shows that, unlike the derived series and the central lower series, the subtree series can halt for a while and then continue downward. $\Delta_1 = \{1,3,5,7\}$ is generated by $3 = a^2$ and is isomorphic to $\mathbb{Z}_4$, while Δ_2 and Δ_3 coincide and are both $\{1, 5 = (aa)(aa)\}$. Finally, $\Delta_4 = \{1\}$. Thus

$$\Delta_0 \supset \Delta_1 \supset \Delta_2 = \Delta_3 \supset \Delta_4.$$

In general, counting (mod 2) balanced trees with one generator up to depth k gives a subtree-counting loop of class 2^k and size 2^{k+1}. Thus, in the non-associative case, a loop of size n can have a subtree-counting degree linear in n, whereas the nilpotence degree of a loop can be at most logarithmic in n. This suggests that determining when a given loop is *not* subtree-counting may require exponentially more computation than telling when a loop is not nilpotent.

As these examples show, we can choose to count some subset S of the set of trees of size less than or equal to k, instead of all of them. This will be a congruence, and so will give a well-defined loop, if and only if S is closed under subtrees, i.e. $uv \in S$ implies $u \in S$ and $v \in S$. For instance, we can choose to count subtrees up to a certain depth rather than a certain size;

balanced subtrees up to a certain depth; left or right combs of a certain depth; and so on.

If we define loops as (*balanced*) *subtree-counting of depth* k in the obvious way, we have

Lemma 14. *If a loop is subtree-counting of class* k*, then it is* (*balanced*) *subtree-counting of depth* k*. If it is* (*balanced*) *subtree-counting of depth* d*, then it is subtree-counting of class* 2^d*.*

Proof. A subtree of size k is contained in a balanced subtree of depth at most k, and a subtree of depth d has size at most 2^d. □

However, a tree which is not a comb is not contained in a comb of any size, so the *subcomb-counting* loops might be a proper subclass of the subtree-counting ones.

8. Open questions

We have introduced the class of subtree-counting loops and show that it is a subclass of the M-nilpotent loops. However, we still don't know if this inclusion is strict. If so, it would be interesting to have some examples and investigate their combinatorial properties.

A more basic problem is that we have no decision algorithm to determine if a finite loop G of order g is subtree-counting. This is equivalent to determining if there exist p and k such that G divides $A^{(*)}/\sim_k^p$ for some alphabet A. If G is subtree-counting, then we can take $p = g$ and $A = G$ since it must be a morphic image of $H = G^{(*)}/\sim_k^p$. Since G/Δ_1^p is an abelian group divided by $\mathbb{Z}_p$, then g must be a multiple of p. This implies that G divides $G^{(*)}/\sim_k^g$.

Finding k seems to be more difficult. However, we observe that in order to compute the number of subtrees of depth $d > 1$, it seems necessary to have some information about the number of subtrees of depth $d - 1$. This suggests that the number of elements in a subtree-counting loop G of class k must be at least $\log k$ and that G must divide $G^{(*)}/\sim_{2^g}^g$. We conjecture that this is true, in which case a decision algorithm would exist.

Another set of open questions come from the theory of computational complexity, especially low-level parallel complexity classes. For instance,

expressions and circuits over solvable groups can be evaluated in the classes $\mathbf{ACC}^0$ and $\mathbf{ACC}^1$, while over non-solvable groups these problems are $\mathbf{NC}^1$-complete and $\mathbf{P}$-complete respectively (see [3, 4, 15] for definitions of these classes and proofs of these results). Similarly, equations over nilpotent groups can be solved in polynomial time, while for non-solvable groups this problem is $\mathbf{NP}$-complete [11] and for solvable groups quasipolynomial time is believed to suffice. Finally, languages defined over groups have constant multiplayer communication complexity if and only if they are nilpotent [19].

Subtree-counting loops can be shown to have many of the same complexity properties as nilpotent groups, suggesting that subtree-counting may play the same role for loops that nilpotence does for groups. However, we have not yet been able to prove the converse computational hardness results for non-subtree-counting loops. In particular, we would like to know if any expressions or programs over non-subtree-counting loops can always express the logical AND of an arbitrary number of variables. We hope that techniques from loop theory can be applied to this and other complexity-theoretic questions.

Acknowledgements. F.L and D.T. where supported by grants from FCAR (Québec) and NSERC (Canada). D.T where also supported by a grant from the von Humbolt Foundation. C.M. is grateful to McGill University for a delightful visit to Montréal, and to Molly Rose and Spootie the Cat for their support. We also thank William C. Waterhouse and Michael Kinyon for helpful conversations.

References

[1] **A. A. Albert**: *Quasigroups I*, Trans. Amer. Math. Soc. **54** (1943), 507 – 519, and *Quasigroups II*, Trans. Amer. Math. Soc. **55** (1944), 401 – 419.

[2] **D. A. Barrington**: *Bounded-width polynomial-size branching programs recognize exactly those languages in* $\mathbf{NC}^1$, J. Comput. System Sci. **38** (1989), 150 – 164.

[3] **D. A. Mix Barrington and D. Thérien**: *Finite monoids and the fine structure of* $\mathbf{NC}^1$, Journal of the ACM **35** (1988), 941 – 952.

[4] **M. Beaudry, P. McKenzie, P. Péladeau, and D. Thérien**: *Circuits with monoidal gates*, Proc. STACS (1993), 555 – 565.

[5] **M. Beaudry and P. McKenzie**: *Circuits, matrices, and nonassociative computation*, J. Comput. System Sci. **50** (1995), 441 – 455.

[6] **M. Beaudry, F. Lemieux, and D. Thérien**: *Finite loops recognize exactly the regular open languages*, Proc. 24th International Colloquium on Automata, Languages and Programming, Lecture Notes in Computer Science 1256, Springer-Verlag 1997, 110 – 120.

[7] **R. H. Bruck**: *Contributions to the theory of loops*, Trans. Amer. Math. Soc. **60** (1946), 245 – 354.

[8] **R. H. Bruck**: *A survey of binary systems*, Springer-Verlag 1966.

[9] **S. R. Buss**: *The Boolean formula value problem is in* ALOGTIME, Proc. 18th ACM Symp. on the Theory of Computing (1987), 123–131.

[10] **H. Caussinus and F. Lemieux**: *The complexity of computing over quasigroups*, Proc. 14th annual FST&TCS (1994), 36 – 47.

[11] **M. Goldman and A. Russell**: *The complexity of solving equations over finite groups*, Proc. 14th Annual IEEE Conference on Computational Complexity 1999.

[12] **P. Hall**: *The theory of groups*, Macmillan 1959.

[13] **F. Lemieux**: *Finite groupoids and their applications to computational complexity*, Ph. D. Thesis, School of Computer Science, McGill University, Montréal 1996.

[14] **M. Lothaire**: *Combinatorics on words*, Encyclopedia of Mathematics and its applications, (G.-C. Rota, Ed.) Addison-Wesley 1983.

[15] **C. Moore**: *Predicting non-linear cellular automata quickly by decomposing them into linear ones*, Physica D **111** (1998), 27 – 41.

[16] **C. Moore**: *Quasi-linear cellular automata*, Proceedings of the International Workshop on Lattice Dynamics, *Physica D* **103** (1997), 100–132.

[17] **C. Moore, D. Thérien, F. Lemieux, J. Berman, and A. Drisko**: *Circuits and expressions with non-associative gates*, J. Comput. System Sci. (to appear)

[18] **H. O. Pflugfelder**: *Quasigroups and loops: An Introduction*, Heldermann Verlag 1990.

[19] **J.-F. Raymond, P. Tesson and D. Thérien**: *An algebraic approach to communication complexity*: Proc. 25th International Colloquium on Automata, Languages and Programming, Lecture Notes in Computer Science 1443, Springer-Verlag 1998, 29 – 40.

[20] **D. Thérien**: *Subword counting and nilpotent groups*, Combinatorics on Words, Progress and Perspectives, (Larry Cummings, Ed.) Academic Press 1983, 297 – 306.

[21] **A. Vesanen**: *Solvable groups and loops*, J. Algebra **180** (1996), 862 – 876.

Received November 1, 2001

François Lemieux
Département d'informatique et de mathématique, Université du Québec à Chicoutimi, 555 boulevard de l'Université, Chicoutimi (Québec), Canada G7H 2B1
e-mail: flemieux@uqac.ca

Cristopher Moore
Computer Science Department, University of New Mexico, Farris Engineering Center, Room 157, Albuquerque (NM), USA 87131 and the Santa Fe Institute, 1399 Hyde Park Road, Santa Fe (NM) USA 87501
e-mail: moore@cs.unm.edu

Denis Thérien
School of Computer Science, McGill University, 3480 University Street, McConnell Engineering Building Room 318, Montréal (Québec), Canada H3A 2A7
e-mail: denis@cs.mcgill.ca

Quasigroups and Related Systems **8** (2001), 67 – 72

On quadratic B-algebras

Hee Kon Park and Hee Sik Kim

Abstract

In this paper we introduce the notion of quadratic B-algebra which is a medial quasigroup, and obtain that every quadratic B-algebra on a field X with $|X| \geqslant 3$, is a BCI-algebra.

1. Introduction

Y. Imai and K. Iséki introduced two classes of abstract algebras: BCK-algebras and BCI-algebras ([6, 7]). It is known that the class of BCK-algebras is a proper subclass of the class of BCI-algebras. In [4, 5] Q. P. Hu and X. Li introduced a wide class of abstract algebras: BCH-algebras. They have shown that the class of BCI-algebras is a proper subclass of the class of BCH-algebras. J. Neggers and H. S. Kim ([10]) introduced the notion of d-algebras, i.e. algebras $(X; *, e)$ defined by (i) $x * x = e$, (v) $e * x = e$, (vi) $x * y = e$ and $y * x = e$ imply $x = y$, which is another useful generalization of BCK-algebras, and then they investigated several relations between d-algebras and BCK-algebras as well as some other interesting relations between d-algebras and oriented digraphs. Y. B. Jun, E. H. Roh and H. S. Kim introduced in [8] a new notion, called an BH-algebra, i.e. algebras $(X; *, e)$ satisfying (i), (ii) $x * e = x$ and (vi), which is a generalization of $BCH/BCI/BCK$-algebras. They also defined the notions of ideals and boundedness in BH-algebras, and showed that there is a maximal ideal in bounded BH-algebras. J. Neggers, S. S. Ahn and H. S. Kim (cf. [10]) introduced the notion of a Q-algebra, and generalized some theorems discussed in BCI-algebras. Recently, J. Neggers and H. S. Kim introduced and investigated a class of algebras, called a B-algebra ([12, 13]), which is related to several classes of algebras of interest such as $BCH/BCI/BCK$-algebras and which seems to have rather nice

2000 Mathematics Subject Classification: 06F35
Keywords: B-algebra, Q-algebra, BCI-algebra

properties without being excessively complicated otherwise. B-algebras are also unipotent quasigroups which plays an important role in the theory of Latin squares (cf. [3]).

In this paper we introduce the notion of quadratic B-algebra which is a medial quasigroup, and obtain that every quadratic B-algebra on a field X with $|X| \geqslant 3$, is a BCI-algebra.

2. B-algebras

A *B-algebra* (cf. [12]) is a non-empty set X with a constant e and a binary operation $*$ satisfying the following axioms:

(i) $x * x = e$,

(ii) $x * e = x$,

(iii) $(x * y) * z = x * (z * (e * y))$

for all $x, y, z \in X$.

Example 2.1. (cf. [12]) Let X be the set of all real numbers except for a negative integer $-n$. Define a binary operation $*$ on X by

$$x * y = \frac{n(x-y)}{n+y}.$$

Then $(X; *, 0)$ is a B-algebra with $e = 0$.

Example 2.2. (cf. [13]) Let $X = \{0, 1, 2, 3, 4, 5\}$ be a set with the following table:

$*$	0	1	2	3	4	5
0	0	2	1	3	4	5
1	1	0	2	4	5	3
2	2	1	0	5	3	4
3	3	4	5	0	2	1
4	4	5	3	1	0	2
5	5	3	4	2	1	0

Then $(X; *, 0)$ is a B-algebra with $e = 0$.

In [2] the following result is proved.

Lemma 2.3. *Let $(X;*,e)$ be a B-algebra. Then we have the following statements.*

(a) *If $x*y=e$ then $x=y$ for any $x,y\in X$.*

(b) *If $e*x=e*y$, then $x=y$ for any $x,y\in X$.*

(c) *$e*(e*x)=x$ for any $x\in X$.*

J. Neggers, S. S. Ahn and H. S. Kim introduced in [10] the notion of Q-algebra, as an algebra $(X,;*,e)$ satisfying (i), (ii) and

(iv) $(x*y)*z=(x*z)*y$

for any $x,y,z\in X$. It is easy to see that B-algebras and Q-algebras are different notions. For example, $X=\{0,1,2,3\}$ with $*$ defined by the following table:

$*$	0	1	2	3
0	0	0	0	0
1	1	0	0	0
2	2	0	0	0
3	3	3	3	0

is a Q-algebra ([10]), but not a B-algebra, since $(3*2)*1=0\neq 3=3*(1*(0*2))$. Example 2.2 is a B-algebra ([13]), but not a Q-algebra, since $(5*3)*4=3\neq 4=(5*4)*3$.

Theorem 2.4. (cf. [10]) *Every Q-algebra satisfying the conditions (iv) and*

(vii) $(x*y)*(x*z)=z*y$

for any $x,y,z\in X$, is a BCI-algebra.

3. Quadratic B-algebras

Let X be a field with $|X|\geqslant 3$. An algebra $(X;*)$ is said to be *quadratic* if $x*y$ is defined by

$$x*y=a_1x^2+a_2xy+a_3y^2+a_4x+a_5y+a_6\,,$$

where $a_1,\ldots,a_6\in X$ are fixed.

A quadratic algebra $(X;*)$ is said to be a *quadratic B-algebra* if for some fixed $e\in X$ it satisfies the conditions (i), (ii) and (iii). Similarly, a quadratic algebra $(X;*)$ is said to be a *quadratic Q-algebra* if for some fixed $e\in X$ it satisfies the conditions (i), (ii) and (iv).

In [10] it is proved that in every quadratic Q-algebra $(X; *, e)$ the operation $*$ has the form $x * y = x - y + e$.

We prove that the similar result is true for quadratic B-algebras.

Theorem 3.1. *Let X be a field with $|X| \geqslant 3$. Then every quadratic B-algebra $(X; *, e)$, $e \in X$, has the form $x * y = x - y + e$, where $x, y \in X$.*

Proof. Let

$$x * y = Ax^2 + Bxy + Cy^2 + Dx + Ey + F \tag{1}$$

for some fixed $A, B, C, D, E, F \in X$.

Consider (i). Then

$$e = x * x = (A + B + C)x^2 + (D + E)x + F. \tag{2}$$

Let $x = 0$ in (2). Then we obtain $F = e$. Hence (1) turns out to be

$$x * y = Ax^2 + Bxy + Cy^2 + Dx + Ey + e \tag{3}$$

If $y = x$ in (3), then

$$e = x * x = (A + B + C)x^2 + (D + E)x + e,$$

for any $x \in X$, and hence we obtain $A+B+C = 0 = D+E$, i.e. $E = -D$ and $B = -A - C$. Hence (3) turns out to be

$$x * y = (x - y)(Ax - Cy + D) + e. \tag{4}$$

Let $y = e$ in (4). Then by (ii) we have

$$x = x * e = (x - e)(Ax - Ce + D) + e,$$

i.e. $(Ax - Ce + D - 1)(x - e) = 0$. Since X is a field, either $x - e = 0$ or $Ax - Ce + D - 1 = 0$. Since $|X| \geqslant 3$, we have $Ax - Ce + D - 1 = 0$, for any $x \in X$. This means that $A = 0$, $1 - D + Ce = 0$. Thus (4) turns out to be

$$x * y = (x - y) + C(x - y)(e - y) + e. \tag{5}$$

To satisfy the condition (iv) we need to determine the constant C, but its computation is so complicated that we use Lemma 2.3 (iii) instead. If we replace e by x, and x by y respectively in (5), then

$$e * x = (e - x) + C(e - x)(e - x) + e. \tag{6}$$

It follows that

$$\begin{aligned} e * (e * x) &= e * [(e - x) + C(e - x)^2 + e] \\ &= x - C(e - x)^2 + C(e - x)\{1 + C(e - x)\}^2 \\ &= x + C^3(e - x)^4 + 2C^2(e - x)^3 . \end{aligned}$$

Since $x = e * (e * x)$, we obtain

$$C^2(e - x)^3\{-Cx + 2 + Ce\} = 0.$$

Since X is a field with $|X| \geqslant 3$, we obtain $C = 0$. This means that every quadratic B-algebra $(X; *, e)$ has the form $x * y = x - y + e$, where $x, y \in X$, completing the proof. □

It follows from Theorem 3.1 that the quadratic B-algebras are medial quasigroups (cf. [1]).

Example 3.2. Let $\mathcal{R}$ be the set of all real numbers. Define $x * y = x - y + \sqrt{2}$. Then $(\mathcal{R}; *, \sqrt{2})$ is a quadratic B-algebra.

Example 3.3. Let $\mathcal{K} = GF(p^n)$ be a Galois field. Define $x * y = x - y + e$, $e \in \mathcal{K}$. Then $(\mathcal{K}; *, e)$ is a quadratic B-algebra.

As a simple consequence of Theorem 3.1 and results proved in [10] we obtain:

Proposition 3.4. *Let X be a field with $|X| \geqslant 3$. Then every quadratic B-algebra on X is a Q-algebra, and conversely.*

Proposition 3.5. *Let X be a field with $|X| \geqslant 3$. If $(X; *, e)$ is a quadratic B-algebra, then $(x * y) * (x * z) = z * y$ for any $x, y, z \in X$.*

Proof. Straightforward. □

Theorem 3.6. *Let X be a field with $|X| \geqslant 3$. Then every quadratic B-algebra on X is a BCI-algebra.*

Proof. It is an immediate consequence of Proposition 3.5 and Theorem 2.4. □

References

[1] **V. D. Belousov**: *Foundations of the theory of quasigroups and loops*, (Russian), Nauka, Moscov 1967.

[2] **J. R. Cho and H. S. Kim**: *On B-algebras and quasigroups*, Quasigroups and Related Systems **8** (2001), 1 – 6.

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

[4] **Q. P. Hu and X. Li**: *On BCH-algebras*, Math. Seminar Notes **11** (1983), 313 – 320.

[5] **Q. P. Hu and X. Li**: *On proper BCH-algebras*, Math. Japonica **30** (1985), 659 – 661.

[6] **K. Iséki and S. Tanaka**: *An introduction to the theory of BCK-algebras*, Math. Japonica **23** (1978), 1 – 26.

[7] **K. Iséki**: *On BCI-algebras*, Math. Seminar Notes **8** (1980), 125−130.

[8] **Y. B. Jun, E. H. Roh and H. S. Kim**: *On BH-algebras*, Scientiae Math. **1** (1998), 347 – 354.

[9] **J. Meng and Y. B. Jun**: *BCK-algebras*, Kyung Moon Sa Co., Seoul 1994.

[10] **J. Neggers, S. S. Ahn and H. S. Kim**: *On Q-algebras*, Int. J. Math. and Math. Sci. **27** (2001), 749 – 757.

[11] **J. Neggers and H. S. Kim**: *On d-algebras*, Math. Slovaca **49** (1999), 19 – 26.

[12] **J. Neggers and H. S. Kim**: *On B-algebras*, (submitted)

[13] **J. Neggers and H. S. Kim**: *A fundamental theorem of B-homomorphism for B-algebras*, Intern. Math. J. **2** (2002), (to appear)

Received April 19, 2001

Hee Kon Park, Department of Engineering Sciences, Hanyang University, Seoul 133-791, Korea

Hee Sik Kim, Department of Mathematics, Hanyang University, Seoul 133-791, Korea, e-mail: heekim@hanyang.ac.kr

Quasigroups and Related Systems **8** (2001), 73 – 85

Algebras of vector-valued functions

Valentin S. Trokhimenko

Abstract

Superpositions (compositions) of multiplace functions have various applications in the modern mathematics, especially in the algebraic theory of automata [1], [3], [4]. It is known that any automaton with n entrances and m exits can be defined by some functions of the form $f : A^n \to A^m$, which are called multiplace vector-valued functions. There are two types of compositions of such functions: serial $\circ$ and parallel $\star$ which were considered by B. Schweizer and A. Sklar in [5], [6], [7]. In this paper we find the abstract characterization of algebras of the form $(\Phi, \circ, \star, \Delta, F)$, where Φ is the set of multiplace vector-valued functions stable for compositions $\circ, \star$ and containing two functions $\Delta(x) = x$, $F(x, y) = y$. We also describe the case when Φ contains all vector-valued functions defined on a fixed set A. Automorphisms of such algebra are described too.

1. Introduction

Any mapping $f : A^n \to A^m$, where $n, m \in \mathbb{N}$ are fixed and A is a non-empty set, is called a *multiplace vector-valued function* (or simply *vector-function*) of *degree* n and *rank* m (cf. [5]). The degree and the rank of the multiplace vector-valued function f is denoted by αf and βf, respectively. $\gamma f = \alpha f - \beta f$ is called the *index* of f. The set of all multiplace vector-valued functions of degree n and rank m defined on a fixed set A is denoted by $\mathcal{T}(A^n, A^m)$.

According to [5], [6] and [7], on the set $\mathcal{T}(A) = \bigcup_{n,m \in \mathbb{N}} \mathcal{T}(A^n, A^m)$ we consider two binary operations: the serial composition $\circ$ and the parallel composition $\star$, which are defined in the following way:

2000 Mathematics Subject Classification: 20N15, 08N05
Keywords: vector valued function

Definition 1. The *serial composition* $f \circ g$ of vector-functions $f, g \in \mathcal{T}(A)$ is defined by

$$(f \circ g)(a_1, \ldots, a_d) = f(b_1, \ldots, b_{\alpha f}) b_{\alpha f+1} \ldots b_{d-\gamma g}\,, \tag{1}$$

where $a_1, \ldots, a_d \in A$, $d = \max\{\alpha f + \gamma g, \alpha g\}$, $b_1, \ldots, b_{d-\gamma g} \in A$ and $b_1 \ldots b_{d-\gamma g} = g(a_1, \ldots, a_{\alpha g}) a_{\alpha g+1} \ldots a_d$.

Definition 2. The *parallel composition* of vector-functions $f, g \in \mathcal{T}(A)$ is a vector-function $f \star g$ defined by

$$(f \star g)(a_1, \ldots, a_d) = f(a_1, \ldots, a_{\alpha f}) g(a_1, \ldots, a_{\alpha g})\,, \tag{2}$$

where $a_1, \ldots, a_d \in A$ and $d = \max\{\alpha f, \alpha g\}$.

It is easy to see that these operations are associative. Moreover, in the case $\alpha f = \beta g$, serial composition reduces to ordinary composition of functions.

Let I_i^n, where $n \in \mathbb{N}$, $1 \leqslant i \leqslant n$, be an *n-place i-th projection* of A, i.e. $I_i^n(a_1, \ldots, a_n) = a_i$ for all $a_1, \ldots, a_n \in A$. Obviously $\alpha I_i^n = n$, $\beta I_i^n = 1$ for all $1 \leqslant i \leqslant n \in \mathbb{N}$. Putting $\Delta(x) = I_1^1(x) = x$ and $F(x, y) = I_2^2(x, y) = y$, we can verify that

$$I_i^n = (F \circ (F \star \Delta))^{n-i} \circ F^{i-1}$$

for any $n \in \mathbb{N}$, $1 \leqslant i \leqslant n$ and $f \in \mathcal{T}(A)$, where $f^0 = \Delta$ and $f^{n+1} = f \circ f^n$.

If the subset Φ of $\mathcal{T}(A)$ contains Δ, F and is closed under operations $\circ, \star$, then a system $(\Phi, \circ, \star, \Delta, F)$ is called an *algebra of vector-functions*. In the case $\Phi = \mathcal{T}(A)$ we say that this algebra is *symmetrical*.

2. The main result

In this section we find an abstract characterization of algebras of vector valued-functions.

First we consider an algebra $(G, \circ, \star, e, f)$ of type $(2, 2, 0, 0)$ satisfying the following six axioms:

Axiom 1. *$(G, \circ)$ and $(G, \star)$ are semigroups and e is the unit of $(G, \circ)$.*

Let e_i^p denotes the expression $(f \circ (f \star e))^{p-i} \circ f^{i-1}$, where $p \in \mathbb{N}$, $1 \leqslant i \leqslant p$ and $(f \circ (f \star e))^0 = f^0 = e$.

Axiom 2. *For each* $g \in G$ *there exist* $m, n \in \mathbb{N}$ *such that*

$$g \circ (e^p \star \cdots \star e^p_p) = g\,, \quad (e^q_1 \star \cdots \star e^q_q) \circ g = g$$

for all $p \leqslant n$, $q \leqslant m$, $p, q \in \mathbb{N}$ *and*

$$g \circ (e^p \star \cdots \star e^p_p) \neq g\,, \quad (e^q_1 \star \cdots \star e^q_q) \circ g \neq g$$

for any $p > n$, $q > m$.

The numbers n and m are called *degree* and *rank* of g and are denoted by αg, βg, respectively.

Axiom 3. *For any* $g_1, g_2 \in G$ *the following conditions*

(*a*) $\alpha e = \beta e = \beta f = 1$, $\alpha f = 2$,

(*b*) $\alpha(g_1 \star g_2) = \max\{\alpha g_1, \alpha g_2\}$, $\beta(g_1 \star g_2) = \beta g_1 + \beta g_2$,

(*c*) $\alpha(g_1 \circ g_2) = \max\{\alpha g_1 + \gamma g_2, \alpha g_2\}$, $\beta(g_1 \circ g_2) = \max\{\beta g_1, \beta g_2 - \gamma g_1\}$,

where $\gamma g = \alpha g - \beta g$, *hold.*

Axiom 4. $f \circ (g_1 \star g_2) = g_2$ *for all* $g_1, g_2 \in G$ *such that* $\alpha g_1 = \alpha g_2$ *and* $\beta g_1 = \beta g_2 = 1$.

Axiom 5. *For all* $g_1, g_2, g_3 \in G$

(*a*) $g_1 \circ (g_2 \star g_3) = (g_1 \circ g_2) \star g_3$, *if* $\alpha g_1 \leqslant \beta g_2$,

(*b*) $(g_1 \star g_2) \circ g_3 = (g_1 \circ g_3) \star (g_2 \circ g_3)$, *if* $\beta g_3 \leqslant \min\{\alpha g_1, \alpha g_2\}$.

Axiom 6. *For all* $g_1, g_2, g_3, g_4 \in G$

(*a*) $(g_1 \star g_2) \circ (g_3 \star g_4) = (g_1 \circ g_3) \star (g_2 \circ (g_3 \star g_4))$, *if* $\alpha g_1 < \alpha g_2$, $\alpha g_1 = \beta g_3$, $\alpha g_2 = \beta(g_3 \star g_4)$,

(*b*) $(g_1 \star g_2) \circ (g_3 \star g_4) = (g_1 \circ (g_3 \star g_4)) \star (g_2 \circ g_3)$, *if* $\alpha g_1 > \alpha g_2$, $\alpha g_2 = \beta g_3$, $\alpha g_1 = \beta(g_3 \star g_4)$.

Now we can prove some auxiliary results on the algebra $(G, \circ, \star, e, f)$.

Proposition 1. *For all* $g_1, g_2 \in G$ *we have*

(*a*) $\gamma(g_1 \circ g_2) = \gamma g_1 + \gamma g_2$,

(*b*) $\gamma(g_1 \star g_2) = \gamma g_1 + \gamma g_2 - \min\{\alpha g_1, \alpha g_2\}$.

Proof. By simple application of the above Axiom 3(c). □

Proposition 2. *For each* $n \in \mathbb{N}$ *and all* $1 \leqslant i \leqslant n$ *the equations* $\alpha e_i^n = n$, $\beta e_i^n = 1$ *are true.*

Proof. Indeed, let g be an element of G such that $\beta g = 1$. Then, by Axiom 3(c), we obtain $\alpha g^n = n\alpha g - n + 1$ and $\beta g^n = 1$. Further

$$\alpha e_i^n = \alpha((f \circ (f \star e))^{n-i} \circ f^{i-1}) = \max\{\alpha((f \circ (f \star e))^{n-i}) + \gamma f^{i-1},\, \alpha f^{i-1}\}.$$

But $\alpha(f \circ (f \star e)) = 2$ and $\beta(f \circ (f \star e)) = 1$ by our Axiom 3. Thus $\alpha((f \circ (f \star e))^{n-i}) = n - i + 1$, $\beta((f \circ (f \star e))^{n-i}) = 1$, $\alpha f^{i-1} = i$, $\beta f^{i-1} = 1$. Hence $\alpha e_i^n = \max\{n, i\} = n$.

Similarly we can prove $\beta e_i^n = 1$. □

Proposition 2 implies that the equation

$$e_i^n \circ (e_1^n \star \cdots \star e_n^n) = e_i^n \tag{3}$$

is satisfied for all $n \in \mathbb{N}$ and $1 \leqslant i \leqslant n$.

Proposition 3. *For all* $g_1, \ldots, g_n \in G$ *such that* $\alpha g_1 = \cdots = \alpha g_n$ *and* $\beta g_1 = \cdots = \beta g_n = 1$, *the equation*

$$e_i^n \circ (g_1 \star \cdots \star g_n) = g_i \tag{4}$$

is satisfied for all $n \in \mathbb{N}$ *and* $1 \leqslant i \leqslant n$.

Proof. First let $n = 2$. If $i = 2$, then, according to Axiom 4, we have

$$e_2^2 \circ (g_1 \star g_2) = f \circ (g_1 \star g_2) = g_2\,.$$

If $i = 1$, then $e_1^2 \circ (g_1 \star g_2) = f \circ (f \star e) \circ (g_1 \star g_2)$. Hence by Axioms 6(b) and 4 we obtain

$$e_1^2 \circ (g_1 \star g_2) = f \circ \Big(\Big(f \circ (g_1 \star g_2)\Big) \star (e \circ g_1)\Big) = f \circ (g_2 \star g_1) = g_1.$$

Now let $n > 2$, $1 \leqslant i \leqslant n$. Then

$$\begin{aligned} e_i^n \circ (g_1 \star \cdots \star g_n) &= (e_1^2)^{n-i} \circ f^{i-1} \circ (g_1 \star \cdots \star g_n) \\ &= (e_1^2)^{n-i} \circ f^{i-2} \circ \Big(\Big(f \circ (g_1 \star g_2)\Big) \star g_3 \star \cdots \star g_n\Big) \\ &= (e_1^2)^{n-i} \circ f^{i-2} \circ (g_2 \star \cdots \star g_n). \end{aligned}$$

Repeating this procedure we obtain

$$\begin{aligned} e_i^n \circ (g_1 \star \cdots \star g_n) &= (e_1^2)^{n-i} \circ (g_i \star \cdots \star g_n) \\ &= (e_1^2)^{n-i-1} \circ \Big(\Big(e_1^2 \circ (g_i \star g_{i+1}) \Big) \star g_{i+2} \star \cdots \star g_n \Big) \\ &= (e_1^2)^{n-i-1} \circ (g_i \star g_{i+2} \star \cdots \star g_n) = \cdots \\ &= e_1^2 \circ (g_i \star g_n) = g_i. \end{aligned}$$

This completes the proof. □

Proposition 4. *If* $x_1, \ldots, x_k \in G$ *are such that*

$$n = \beta x_1 + \cdots + \beta x_k \quad \textit{and} \quad m = \max\{\alpha x_1, \ldots, \alpha x_k\},$$

then

$$e_i^n \circ (x_1 \star \cdots \star x_k) = e_s^{\beta x_p} \circ x_p \circ (e_1^m \star \cdots \star e_{\alpha x_p}^m) \tag{5}$$

for all $1 \leqslant i \leqslant n$, *where* $\sum\limits_{j=1}^{p-1} \beta x_j < i \leqslant \sum\limits_{j=1}^{p} \beta x_j$ *and* $s = i - \sum\limits_{j=1}^{p-1} \beta x_j$.

Proof. Let $n_i = \beta x_i$ for all $x_i \in G$, $i = 1, \ldots, k$. By Axiom 3(b) we have $\alpha(x_1 \star \cdots \star x_k) = \max\{\alpha x_1, \ldots, \alpha x_k\} = m$. Applying Axiom 2 we obtain

$$\begin{aligned} &e_i^n \circ (x_1 \star \cdots \star x_k) = \\ &e_i^n \circ \Big(\Big((e_1^{n_1} \star \cdots \star e_{n_1}^{n_1}) \circ x_1 \Big) \star \cdots \star \Big((e_1^{n_k} \star \cdots \star e_{n_k}^{n_k}) \circ x_k \Big) \Big) \circ (e_1^n \star \cdots \star e_m^m). \end{aligned}$$

Further, by Axiom 5(b)

$$\begin{aligned} e_i^n \circ (x_1 \star \cdots \star x_k) = e_i^n \circ \Big(&(e_1^{n_1} \circ x_1) \star \cdots \star (e_{n_1}^{n_1} \circ x_1) \star \cdots \star \\ &\star (e_1^{n_k} \circ x_k) \star \cdots \star (e_{n_k}^{n_k} \circ x_k) \Big) \circ (e_1^m \star \cdots \star e_m^m)\,. \end{aligned}$$

This, together with Axiom 6 and Proposition 3, implies

$$\begin{aligned} &e_i^n \circ (x_1 \star \cdots \star x_k) = e_i^n \circ \Big(\Big(e_1^{n_1} \circ x_1 \circ (e_1^m \star \cdots \star e_{\alpha x_1}^m) \Big) \star \cdots \star \\ &\star \Big(e_{n_k}^{n_k} \circ x_1 \circ (e_1^m \star \cdots \star e_{\alpha x_k}^m) \Big) \Big) = e_s^{\beta x_p} \circ x_p \circ (e_1^m \star \cdots \star e_{\alpha x_p}^m)\,, \end{aligned}$$

which completes the proof. □

Theorem 1. *An algebra* $(G, \circ, \star, e, f)$ *of type* $(2, 2, 0, 0)$ *is isomorphic to some algebra of vector-functions if and only if it satisfies Axioms* $1 - 6$.

Proof. The necessity of Theorem is evident. We prove the sufficiency. For this let $(G, \circ, \star, e, f)$ be an algebra satisfying Axioms $1-6$ and let G_n be the set of all elements $g \in G$ such that $\alpha g = n$ and $\beta g = 1$. It is clear that $G_n \neq \emptyset$ for every $n \in \mathbb{N}$, because $e_i^n \in G_n$ for all $1 \leqslant i \leqslant n$. Note that $G_n \cap G_m = \emptyset$ for $n \neq m$. Let $\overline{G} = \bigtimes\limits_{n\in\mathbb{N}} G_n$ be the Cartesian power of the family sets $(G_n)_{n\in\mathbb{N}}$.

For each $g \in G$ we define the vector-function $P_g : \overline{G}^{\,n} \to \overline{G}^{\,m}$, where $n = \alpha g$, $m = \beta g$, putting $P_g(\bar{x}_1, \ldots, \bar{x}_n) = \bar{y}_1 \ldots \bar{y}_m$ if and only if

$$\bar{y}_i(k) = e_i^m \circ g \circ \Big(\bar{x}_1(k) \star \cdots \star \bar{x}_n(k)\Big) \tag{6}$$

for every $1 \leqslant i \leqslant m$ and $k = 1, 2, \ldots$

We prove that the mapping $P : g \mapsto P_g$ is an isomorphism between algebras $(G, \circ, \star, e, f)$ and $(\Phi, \circ, \star, \Delta, F)$, where $\Phi = \{P_g \,|\, g \in G\}$.

First observe that $P_e = \Delta$ and $P_f = F$. Indeed, if $P_e(\bar{x}) = \bar{y}$ for some $\bar{x}, \bar{y} \in \overline{G}$, then $\bar{y}(k) = e_1^1 \circ e \circ \bar{x}(k) = \bar{x}(k)$ for all $k = 1, 2, \ldots$, because $e_1^1 = e$ is the unit of $(G, \circ)$. Thus $\bar{y}(k) = \bar{x}(k)$, $k = 1, 2, \ldots$ So, $P_e(\bar{x}) = \bar{x}$. Hence $P_e = \Delta$. Analogously, from Axiom 4, we deduce $P_f = F$.

Now prove that $P(g_1 \circ g_2) = P(g_1) \circ P(g_2)$ for all $g_1, g_2 \in G$, i.e.

$$P_{g_1 \circ g_2} = P_{g_1} \circ P_{g_2}\,. \tag{7}$$

Let $n_i = \alpha g_i$, $m_i = \beta g_i$, $i = 1, 2$, $n = \max\{n_1 + \gamma g_2, n_2\}$ and $m = \max\{m_1, m_2 - \gamma g_1\}$. By Axiom 3(c) $n = \alpha(g_1 \circ g_2)$, $m = \beta(g_1 \circ g_2)$. Thus the degree and the rank of the function $P_{g_1 \circ g_2}$ are equal n and m, respectively. Let

$$\bar{y}_1 \ldots \bar{y}_m = P_{g_1 \circ g_2}(\bar{x}_1, \ldots, \bar{x}_n)$$

for some $\bar{x}_1, \ldots, \bar{x}_n, \bar{y}_1, \ldots, \bar{y}_m \in \overline{G}$. If $n_1 > m_2$ then $m = m_1$. Therefore, by (6), we have

$$\bar{y}_i(k) = e_i^m \circ g_1 \circ g_2 \circ \Big(\bar{x}_1(k) \star \cdots \star \bar{x}_n(k)\Big)$$

for all $1 \leqslant i \leqslant m$ and $k = 1, 2, \ldots$ Since the equation

$$n_2 = \beta\Big(\bar{x}_1(k) \star \cdots \star \bar{x}_{n_2}(k)\Big)$$

is true, Axiom 5(a) gives

$$\bar{y}_i(k) = e_i^{m_1} \circ g_1 \circ \Big(\Big(g_2 \circ \Big(\bar{x}_1(k) \star \cdots \star \bar{x}_{n_2}(k)\Big)\Big) \star \bar{x}_{n_2+1}(k) \star \cdots \star \bar{x}_n(k)\Big).$$

Applying to this equation Axioms 2 and 6, we obtain

$$\begin{aligned}\bar{y}_i(k) &= e_i^{m_1} \circ g_1 \circ \Big(\Big(\Big(e_1^{m_2} \star \cdots \star e_{m_2}^{m_2}\Big) \circ g_2 \circ \Big(\bar{x}_1(k) \star \cdots \star \bar{x}_{n_2}(k)\Big)\Big) \star \\ &\qquad \star\ \bar{x}_{n_2+1}(k) \star \cdots \star \bar{x}_n(k)\Big) \\ &= e_i^{m_1} \circ g_1 \circ \Big(\Big(e_1^{m_2} \circ g_2 \circ \Big(\bar{x}_1(k) \star \cdots \star \bar{x}_{n_2}(k)\Big)\Big) \star \cdots \star \\ &\quad \star \Big(e_{m_2}^{m_2} \circ g_2 \circ \Big(\bar{x}_1(k) \star \cdots \star \bar{x}_{n_2}(k)\Big)\Big) \star \bar{x}_{n_2+1}(k) \star \cdots \star \bar{x}_n(k)\Big).\end{aligned}$$

Let $\bar{z}_1 \ldots \bar{z}_{m_2} = P_{g_2}(\bar{x}_1, \ldots, \bar{x}_{n_2})$, i.e.

$$\bar{z}_i(k) = e_i^{m_2} \circ g_2 \circ (\bar{x}_1(k) \star \cdots \star \bar{x}_{n_2}(k))$$

for all $1 \leqslant i \leqslant m_2$ and $k = 1, 2, \ldots$ Then

$$\bar{y}_i(k) = e_i^{m_1} \circ g_1 \circ \Big(\bar{z}_1(k) \star \cdots \star \bar{z}_{m_2}(k) \star \bar{x}_{n_2+1}(k) \star \cdots \star \bar{x}_n(k)\Big)$$

for all $1 \leqslant i \leqslant m_1$ and $k = 1, 2, \ldots$ Thus

$$\bar{y}_1 \ldots \bar{y}_{m_1} = P_{g_1}(\bar{z}_1, \ldots, \bar{z}_{m_2}, \bar{x}_{n_2+1}, \ldots, \bar{x}_n).$$

Therefore

$$\bar{y}_1 \ldots \bar{y}_{m_1} = P_{g_1}(P_{g_2}(\bar{x}_1, \ldots, \bar{x}_{n_2}), \bar{x}_{n_2+1}, \ldots, \bar{x}_n),$$

i.e. $\bar{y}_1 \ldots \bar{y}_m = (P_{g_1} \circ P_{g_2})(\bar{x}_1, \ldots, \bar{x}_n)$, which proves (7) for $n_1 > m_2$, $m = m_1$.

Now let $n_1 \leqslant m_2$. Then $n = n_2$ and $m = m_2 - \gamma g_1$. Hence, for all $1 \leqslant i \leqslant m$, $k = 1, 2, \ldots$ we have

$$\begin{aligned}\bar{y}_i(k) &= e_i^m \circ g_1 \circ g_2 \circ \Big(\bar{x}_1(k) \star \cdots \star \bar{x}_n(k)\Big) \\ &= e_i^m \circ g_1 \circ \Big(e_1^{m_2} \star \cdots \star e_{m_2}^{m_2}\Big) \circ g_2 \circ \Big(\bar{x}_1(k) \star \cdots \star \bar{x}_{n_2}(k)\Big) \\ &= e_i^m \circ g_1 \circ \Big(\Big(e_1^{m_2} \circ g_2 \circ \Big(\bar{x}_1(k) \star \cdots \star \bar{x}_{n_2}(k)\Big)\Big) \star \cdots \star \\ &\qquad \star\ \Big(e_{m_2}^{m_2} \circ g_2 \circ \Big(\bar{x}_1(k) \star \cdots \star \bar{x}_{n_2}(k)\Big)\Big)\Big) \\ &= e_i^m \circ g_1 \circ \Big(\bar{z}_1(k) \star \cdots \star \bar{z}_{m_2}(k)\Big).\end{aligned}$$

Now applying Axiom 5(a) we obtain

$$\bar{y}_i(k) = e_i^m \circ \Big(\Big(g_1 \circ \Big(\bar{z}_1(k) \star \cdots \star \bar{z}_{n_1}(k)\Big)\Big) \star \bar{z}_{n_1+1}(k) \star \cdots \star \bar{z}_{m_2}(k)\Big). \quad (8)$$

If $1 \leqslant i \leqslant m_1$, then applying Proposition 4 to (8) we get

$$\bar{y}_i(k) = e_i^{m_1} \circ g_1 \circ \Big(\bar{z}_1(k) \star \cdots \star \bar{z}_{n_1}(k)\Big)$$

for $k = 1, 2, \ldots$ Therefore

$$\bar{y}_1 \ldots \bar{y}_{m_1} = P_{g_1}(\bar{z}_1, \ldots, \bar{z}_{n_1}).$$

For $m_1 < i \leqslant m$ we have $\bar{y}_i(k) = \bar{z}_{i+\gamma g_1}(k)$, where $k = 1, 2, \ldots$ Whence $\bar{y}_{m_1+1} \ldots \bar{y}_m = \bar{z}_{n_1+1} \ldots \bar{z}_{m_2}$. So,

$$\bar{y}_1 \ldots \bar{y}_m = P_{g_1}(\bar{z}_1, \ldots, \bar{z}_{n_1})\bar{z}_{n_1+1} \ldots \bar{z}_{m_2}\,,$$

which, by Definition 1, gives $\bar{y}_1 \ldots \bar{y}_m = (P_{g_1} \circ P_{g_2})(\bar{x}_1, \ldots, \bar{x}_n)$. Thus

$$P_{g_1 \circ g_2}(\bar{x}_1, \ldots, \bar{x}_n) = (P_{g_1} \circ P_{g_2})(\bar{x}_1, \ldots, \bar{x}_n)$$

for all $\bar{x}_1, \ldots, \bar{x}_n \in \overline{G}$. This proves (7).

To verify $P(g_1 \star g_2) = P(g_1) \star P(g_2)$, i.e.

$$P_{g_1 \star g_2} = P_{g_1} \star P_{g_2} \tag{9}$$

for all $g_1, g_2 \in G$, assume that $n_i = \alpha g_i$, $m_i = \beta g_i$ for $i = 1, 2$, and $n = \max\{n_1, n_2\}$, $m = m_1 + m_2$. By Axiom 3(b), $n = \alpha(g_1 \star g_2) = \alpha(P_{g_1 \star g_2})$, $m = \beta(g_1 \star g_2) = \beta(P_{g_1 \star g_2})$. Let

$$\bar{y}_1 \ldots \bar{y}_m = P_{g_1 \star g_2}(\bar{x}_1, \ldots, \bar{x}_n)$$

for some $\bar{x}_1, \ldots, \bar{x}_n, \bar{y}_1, \ldots, \bar{y}_m \in \overline{G}$. Then, according to (6),

$$\bar{y}_i(k) = e_i^m \circ (g_1 \star g_2) \circ (\bar{x}_1(k) \star \cdots \star \bar{x}_n(k)) \tag{10}$$

for all $1 \leqslant i \leqslant m$ and $k = 1, 2, \ldots$

Assume that $n_1 \leqslant n_2$. Then $n = n_2$. Therefore, by Axiom 6, the equation (10) can be written in the form

$$\bar{y}_i(k) = e_i^m \circ \Big(\Big(g_1 \circ \Big(\bar{x}_1(k) \star \cdots \star \bar{x}_{n_1}(k)\Big)\Big) \star \Big(g_2 \circ \Big(\bar{x}_1(k) \star \cdots \star \bar{x}_n(k)\Big)\Big)\Big). \tag{11}$$

For $1 \leqslant i \leqslant m_1$ the above equation and Proposition 4 imply

$$\bar{y}_i(k) = e_i^{m_1} \circ g_1 \circ \Big(\bar{x}_1(k), \ldots, \bar{x}_{n_1}(k)\Big), \quad k = 1, 2, \ldots$$

Hence $\bar{y}_1 \dots \bar{y}_{m_1} = P_{g_1}(\bar{x}_1, \dots, \bar{x}_{n_1})$.

In the same manner, for $m_1 + 1 \leqslant i \leqslant m$, we obtain

$$\bar{y}_i(k) = e^{m_2}_{i-m_1} \circ g_2 \circ \Big(\bar{x}_1(k) \star \cdots \star \bar{x}_n(k)\Big), \quad k = 1, 2, \dots$$

and $\bar{y}_{m_1+1} \dots \bar{y}_m = P_{g_2}(\bar{x}_1, \dots, \bar{x}_n)$. Thus $\bar{y}_1 \dots \bar{y}_m = (P_{g_1} \star P_{g_2})(\bar{x}_1, \dots, \bar{x}_n)$. Hence

$$P_{g_1 \star g_2}(\bar{x}_1, \dots, \bar{x}_n) = (P_{g_1} \star P_{g_2})(\bar{x}_1, \dots, \bar{x}_n)$$

for all $\bar{x}_1, \dots, \bar{x}_n \in \overline{G}$. This proves (9) in the case $n_1 \leqslant n_2$.

The case $n_2 \leqslant n_1$ is analogous.

Now we prove that P is one-to-one. Let $P_{g_1} = P_{g_2}$ for some $g_1, g_2 \in G$. Then $\alpha g_1 = \alpha g_2$, $\beta g_1 = \beta g_2$. Therefore

$$e^m_i \circ g_1 \circ \Big(\bar{x}_1(k) \star \cdots \star \bar{x}_n(k)\Big) = e^m_i \circ g_2 \circ \Big(\bar{x}_1(k) \star \cdots \star \bar{x}_n(k)\Big) \qquad (12)$$

for all $1 \leqslant i \leqslant m = \beta g_1$, $\bar{x}_1, \dots, \bar{x}_n \in \overline{G}$, where $n = \alpha g_1$ and $k = 1, 2, \dots$

This for $\bar{x}_j = \bar{e}_j = (e^1_1, e^2_2, \dots, e^i_i, e^{i+1}_i, e^{i+2}_i, \dots) \in \overline{G}$, $j = 1, \dots, n$ and $k = n$, gives

$$e^m_i \circ g_1 \circ (e^n_1 \star \cdots \star e^n_n) = e^m_i \circ g_2 \circ (e^n_1 \star \cdots \star e^n_n)\,.$$

Thus $e^m_i \circ g_1 = e^m_i \circ g_2$ for all $1 \leqslant i \leqslant m$, and in the consequence

$$(e^m_1 \circ g_1) \star \cdots \star (e^m_m \circ g_1) = (e^m_1 \circ g_2) \star \cdots \star (e^m_m \circ g_2)\,.$$

Hence $(e^m_1 \star \cdots \star e^m_m) \circ g_1 = (e^m_1 \star \cdots \star e^m_m) \circ g_2$, which implies $g_1 = g_2$.

This completes the proof that $P : g \mapsto P_g$ is an isomorphism between algebras $(G, \circ, \star, e, f)$ and $(\Phi, \circ, \star, \Delta, F)$, where $\Phi = \{P_g \,|\, g \in G\}$. □

3. Symmetrical algebras

An algebra $(G, \circ, \star, e, f)$ of type $(2, 2, 0, 0)$ satisfying Axioms $1 - 6$ is called a *V-algebra*.

Let $\mathcal{G} = (G, \circ, \star, e, f)$ be a fixed V-algebra and let $\mathcal{G}' = (G', \circ, \star, e', f')$ be some other algebra of type $(2, 2, 0, 0)$.

Definition 3. A homomorphism $P : \mathcal{G} \to \mathcal{G}'$ is called a *v-homomorphism*, if $g \neq g \circ (e^n_1 \star \cdots \star e^n_n)$ implies $P(g) \neq P(g \circ (e^n_1 \star \cdots \star e^n_n))$ for any $g \in G$ and $n \in \mathbb{N}$.

It is easy to see that if P is a v-homomorphism of a V-algebra $\mathcal{G}$ onto an algebra $\mathcal{G}'$, then $\mathcal{G}'$ is a V-algebra too. In this case $\alpha g = \alpha P(g)$ and $\beta g = \beta P(g)$ for any $g \in G$. Conversely, if P is a homomorphism of a V-algebra $\mathcal{G}$ onto a V-algebra $\mathcal{G}'$ such that $\alpha g = \alpha P(g)$ and $\beta = \beta P(g)$ for all $g \in G$, then P is a v-homomorphism.

Definition 4. A subset H of a V-algebra $\mathcal{G}$ is called a *v-ideal*, if for all $x \in G, h_1, \ldots, h_n \in H, 1 \leqslant i \leqslant n$, where $n = \alpha x$ and $m = \beta x$, the condition $e_i^m \circ x \circ (h_1 \star \cdots \star h_n) \in H$ is satisfied.

Generalizing the concept of dense ideals in semigroups (cf. [2]), we say that an ideal H of a V-algebra $\mathcal{G}$ is *dense* if and only if

(a) any v-homomorphism of $\mathcal{G}$, which is not an isomorphism, induces on H a homomorphism, which is not an isomorphism,

(b) if $\mathcal{G}$ is a V-subalgebra of V-algebra $\mathcal{G}' \neq \mathcal{G}$ and H is a v-ideal of $\mathcal{G}'$, then there exists a v-homomorphism of $\mathcal{G}'$, which is not an isomorphism, but induces on H an isomorphism.

Now consider the symmetrical algebra of vector-functions

$$\mathfrak{T} = (\mathcal{T}(A), \circ, \star, \Delta, F).$$

It is easy to verify that it satisfies Axioms $1 - 6$, i.e. it is a V-algebra.

By H_A we denote the set of all functions φ_a such that $a \in A$ and $\varphi_a(x) = a$ for all $x \in A$. Clearly, $\alpha\varphi_a = \beta\varphi_a = 1$ for all $a \in A$ and $(H_A, \circ)$ is a semigroup of left zeros.

The following three theorems are generalizations of similar results proved for transformation semigroups [2].

Theorem 2. *The set H_A is a dense v-ideal of $\mathfrak{T} = (\mathcal{T}(A), \circ, \star, \Delta, F)$.*

Proof. Let $\psi \in \mathcal{T}(A)$, $\varphi_{a_1}, \ldots, \varphi_{a_n} \in H_A$, where $n = \alpha\psi$ and $a_1, \ldots, a_n$ are elements of A. Suppose that

$$\psi(a_1, \ldots, a_n) = b_1 \ldots b_m$$

for some $b_1, \ldots, b_m \in A$, where $m = \beta\psi$. We have $(I_i^m \circ \psi)(a_1, \ldots, a_n) = b_i$ for $1 \leqslant i \leqslant m$, because $I_i^m(b_1, \ldots, b_m) = b_i$. If $c \in A$, then

$$(I_i^m \circ \psi)(\varphi_{a_1}(c), \ldots, \varphi_{a_n}(c)) = \varphi_{b_i}(c),$$

i.e. $(I_i^m \circ \psi \circ (\varphi_{a_1} \star \cdots \star \varphi_{a_n}))(c) = \varphi_{b_i}(c)$. So,

$$I_i^m \circ \psi \circ (\varphi_{a_1} \star \cdots \star \varphi_{a_n}) = \varphi_{b_i} \in H_A.$$

This proves that H_A is a v-ideal of $\mathfrak{T}$.

Now let P be a v-homomorphism of $\mathfrak{T}$, which is not an isomorphism. Hence, there are $\psi_1, \psi_2 \in \mathcal{T}(A)$ such that $\psi_1 \neq \psi_2$ and $P(\psi_1) = P(\psi_2)$. The last equation gives $\alpha P(\psi_1) = \alpha P(\psi_2)$ and $\beta P(\psi_1) = \beta P(\psi_2)$. So, there are elements $a_1, \ldots, a_n \in A$ such that

$$\psi_1(a_1, \ldots, a_n) \neq \psi_2(a_1, \ldots, a_n).$$

Let $\psi_1(a_1, \ldots, a_n) = b_1 \ldots b_m$ and $\psi_2(a_1, \ldots, a_n) = c_1 \ldots c_m$, where n, m are degree and rank of functions ψ_1, ψ_2 respectively. Thus $b_1 \neq c_i$ for some $1 \leqslant i \leqslant m$, because $b_1 \ldots b_m \neq c_1 \ldots c_m$. Whence $\varphi_{b_i} \neq \varphi_{c_i}$. But

$$\begin{aligned} P(\varphi_{b_i}) &= P(I_i^m \circ \psi_1 \circ (\varphi_{a_1} \star \cdots \star \varphi_{a_n})) \\ &= P(I_i^m) \circ P(\psi_1) \circ (P(\varphi_{a_1}) \star \cdots \star P(\varphi_{a_n})) \\ &= P(I_i^m) \circ P(\psi_2) \circ (P(\varphi_{a_1}) \star \cdots \star P(\varphi_{a_n})) \\ &= P(I_i^m \circ \psi_2 \circ (\varphi_{a_1} \star \cdots \star \varphi_{a_n})) = P(\varphi_{c_i}). \end{aligned}$$

Thus, P induces on H_A a homomorphism, which is not isomorphism.

Now assume that H_A is a v-ideal of V-algebra $\mathcal{G} = (G, \circ, \star, \Delta, F)$ and $\mathfrak{T}$ is a proper subalgebra of $\mathcal{G}$. For each element $g \in G$ we consider the function $\lambda_g \in \mathcal{T}(A)$ defined in the following way:

$$b_1 \ldots b_m = \lambda_g(a_1, \ldots, a_n) \Longleftrightarrow \bigwedge_{i=1}^{m} I_i^m \circ g \circ (\varphi_{a_1} \star \cdots \star \varphi_{a_n}) = \varphi_{b_i}\,, \quad (13)$$

where $n = \alpha g,\ m = \beta g,\ a_1, \ldots, a_n, b_1, \ldots, b_m \in A$. It is not difficult to see that the mapping $P : g \mapsto \lambda_g$ is a v-homomorphism of $\mathcal{G}$ into $\mathfrak{T}$. Since $\mathcal{T}(A) \subset G$ and $\mathcal{T}(A) \neq G$, for $g \in G \setminus \mathcal{T}(A)$ we have $g \neq P(g) = \lambda_g$. But $P(\lambda_g) = \lambda_g$, by (13). Therefore $P(g) = P(\lambda_g)$. Thus, P is a v-homomorphism, which is not an isomorphism, and which induces on H_A an identical isomorphism. □

Theorem 3. *A V-algebra $\mathcal{G} = (G, \circ, \star, e, f)$ is isomorphic to some symmetrical algebra of vector-functions if and only if it contains a dense v-ideal H, which is a semigroup of left zeros under the operation $\circ$ and $\alpha h = \beta h = 1$ for all $h \in H$.*

Proof. The necessity follows from Theorem 2. To prove the sufficiency we consider the mapping $P : G \to \mathcal{T}(H)$ defined by the formula

$$y_1 \dots y_m = P(g)(x_1, \dots, x_n) \iff \bigwedge_{i=1}^{m} y_i = e_i^m \circ g \circ (x_1 \star \dots \star x_n) \qquad (14)$$

for all $g \in G$ and $x_1, \dots, x_n, y_1, \dots, y_m \in H$, where $n = \alpha g$, $m = \beta g$. From (14) it follows that $P(e) = \Delta$, $P(f) = F$. It is not difficult to verify that P is a v-homomorphism, which induces on H an isomorphism. But H is a dense v-ideal of $\mathcal{G}$, therefore, according to the definition of a dense v-ideal, P must be an isomorphism. Hence, a v-ideal H_H is a dense v-ideal of a homomorphic image of $(G, \circ, \star, e, f)$, i.e. $(P(G), \circ, \star, \Delta, F)$, because $(H_H, \circ)$ is isomorphic to $(H, \circ)$. But, by Theorem 2, a v-ideal H_H is a dense v-ideal of $(\mathcal{T}(H), \circ, \star, \Delta, F)$, therefore $P(G) \subset \mathcal{T}(H)$ implies $P(G) = \mathcal{T}(H)$. This proves that $\mathcal{G}$ is isomorphic to a symmetrical algebra of vector-functions. $\square$

Let $f : A \to A$ be some one-to-one mapping. By P_f we denote the mapping $\mathcal{T}(A) \to \mathcal{T}(A)$ defined by the condition

$$P_f(\varphi)(a_1, \dots, a_n) = b_1 \dots b_m \iff$$
$$f^{-1}(b_1) \dots f^{-1}(b_m) = \varphi(f^{-1}(a_1), \dots, f^{-1}(a_n))$$

for all $\varphi \in \mathcal{T}(A)$ and $a_1, \dots, a_n, b_1, \dots, b_m \in A$, where $n = \alpha\varphi$, $m = \beta\varphi$. It is easy to see that P_f is an automorphism of $\mathfrak{T} = (\mathcal{T}(A), \circ, \star, \Delta, F)$. Such defined automorphism is called *inner*.

Theorem 4. *Every automorphism of* $\mathfrak{T} = (\mathcal{T}(A), \circ, \star, \Delta, F)$ *is inner.*

Proof. Let λ be some automorphism of $\mathfrak{T} = (\mathcal{T}(A), \circ, \star, \Delta, F)$, then $\lambda(\Delta) = \Delta$ and $\lambda(F) = F$. Therefore $\lambda(I_i^n) = I_i^n$ for $n \in \mathbb{N}$ and any $1 \leqslant i \leqslant n$. This implies $\alpha\varphi = \alpha\lambda(\varphi)$ and $\beta\varphi = \beta\lambda(\varphi)$ for every $\varphi \in \mathcal{T}(A)$.

We have also $\lambda(\varphi_a) \in H_A$ for all $a \in A$. Indeed, for any $\psi \in \mathcal{T}(A)$ such that $\alpha\psi = \beta\psi = 1$, holds $\varphi_1 \circ \psi = \varphi_a$, where $a \in A$. Therefore $\varphi_a \circ \lambda^{-1}(\varphi_b) = \varphi_a$, where $b \in A$. Thus, $\lambda(\varphi_a \circ \lambda^{-1}(\varphi_b)) = \lambda(\varphi_a)$, i.e. $\lambda(\varphi_a) \circ \varphi_b = \lambda(\varphi_a)$. Since H_A is a v-ideal of $\mathfrak{T}$, then $\lambda(\varphi_a) \circ \varphi_b \in H_A$, i.e. $\lambda(\varphi_a) \in H_A$.

Now consider the one-to-one correspondence $f_\lambda : A \to A$ such that

$$(a, b) \in f_\lambda \iff (\varphi_a, \varphi_b) \in \lambda$$

for any $a, b \in A$.

Evidently $\lambda(\varphi_a) = \varphi_{f_\lambda(a)}$ and $\lambda^{-1}(\varphi_a) = \varphi_{f_\lambda^{-1}(a)}$ for each $a \in A$. Thus, for all $\varphi \in \mathcal{T}(A)$ and $a_1, \dots, a_n, b_1, \dots, b_m \in A$, where $n = \alpha\varphi$, $m = \beta\varphi$, we have

$$\begin{aligned}
& b_1 \dots b_m = \lambda(\varphi)(a_1, \dots, a_n) \\
\iff & \bigwedge_{i=1}^{m} \varphi_{b_i} = I_i^m \circ \lambda(\varphi) \circ (\varphi_{a_1} \star \dots \star \varphi_{a_n}) \\
\iff & \bigwedge_{i=1}^{m} \varphi_{f_\lambda^{-1}(b_i)} = I_i^m \circ \varphi \circ (\varphi_{f_\lambda^{-1}(a_1)} \star \dots \star \varphi_{f_\lambda^{-1}(a_n)}) \\
\iff & f_\lambda^{-1}(b_1) \dots f_\lambda^{-1}(b_m) = \varphi(f_\lambda^{-1}(a_1), \dots, f_\lambda^{-1}(a_n)) \\
\iff & b_1 \dots b_m = P_{f_\lambda}(\varphi)(a_1, \dots, a_n).
\end{aligned}$$

So, $\lambda = P_{f_\lambda}$, i.e. λ is an inner automorphism. □

References

[1] **V. M. Glushkov, G. E. Tseytlin, E. L. Yuschenko**: *Algebras, languages, programming*, (Russian) Naukova Dumka, Kiev 1974.

[2] **E. S. Lyapin**: *Semigroups*, (Russian), Fizmatgiz, Moscow 1960.

[3] **A. I. Mal'tsev**: *Iterative Post algebras*, (Russian), Novosibirsk State University 1976.

[4] **R. Pöschel, L. A. Kalužnin**: *Funktionen und Relationenalgebren*, VEB Deutscher Verlag der Wissenschaften, Berlin 1979.

[5] **B. Schweizer, A. Sklar**: *The algebra of vector–valued functions*, Bull. Amer. Math. Soc. **73** (1967), 510 – 515.

[6] **B. Schweizer, A. Sklar**: *A grammar of functions, I*, Aequat. Math. **2** (1968), 62 – 85.

[7] **B. Schweizer, A. Sklar**: *A grammar of functions, II*, Aequat. Math. **3** (1969), 15 – 43.

Department of Mathematics
Pedagogical University
21100 Vinnitsa
Ukraine
e-mail: vtrokhim@sovauma.com

Received September 12, 2001

Quasigroups and Related Systems **8** (2001), 87 – 96

Representations of positional algebras

Valentin S. Trokhimenko

Abstract

In the paper we consider representations of positional algebras in the sense of V. D. Belousov [1] by partial multiplace functions. We prove that any such representation has a special construction.

On the sets of multiplace functions of several arities one often considers the binary operations of superpositions, which are called positional superpositions. Such operations are used in the theory of functional equations and in the theory of n-ary quasigroups [1]. Thus the study of positional algebras and their representations by multiplace functions has the particular interest. For descriptions of such representations we use the generalization of the method of determining pairs, which B. M. Schein considered for semigroups of transformations [2].

A *positional algebra* is a partial algebra of the form

$$\mathfrak{G} = (G; \overset{1}{+}, \overset{2}{+}, \dots, \overset{n}{+}, \dots),$$

where $\overset{1}{+}, \overset{2}{+}, \dots, \overset{n}{+}, \dots$ are partial binary operations on a set G satisfying the Axioms $\mathbf{A_1} - \mathbf{A_5}$.

$\mathbf{A_1}$ $\{x\} \overset{1}{+} \{y\} \neq \emptyset$ for all $x, y \in G$.

$\mathbf{A_2}$ For every $x \in G$ there exists $n \in \mathbb{N}$ such that

$$i \leqslant n \Longleftrightarrow \{x\} \overset{n}{+} \{y\} \neq \emptyset$$

for all $i \in \mathbb{N}$ and $y \in G$.

2000 Mathematics Subject Classification: 20N15, 08N05
Keywords: vector valued function
The main result of this paper was announced on the Third International Algebraic Conference in Ukraine, Sumy, 2 – 8 July 2001.

Let α be the binary relation on $G\times\mathbb{N}$ such that $(x,n)\in\alpha$ if and only if

$$(\forall i\in\mathbb{N})\,(\forall y\in G)\ (\,i\leqslant n\Longleftrightarrow\{x\}\overset{i}{+}\{y\}\neq\emptyset\,). \tag{1}$$

Proposition 1. *The relation α is single valued.*

Proof. Let $(x,n)\in\alpha$ and $(x,m)\in\alpha$ for some $x\in G$, $n,m\in\mathbb{N}$. Assume that $n\neq m$, then we suppose, without restricting generality, that $n<m$. According to (1) we have

$$(\forall i\in\mathbb{N})\,(\forall y\in G)\ (\,i\leqslant n\Longleftrightarrow\{x\}\overset{i}{+}\{y\}\neq\emptyset\,), \tag{2}$$

$$(\forall i\in\mathbb{N})\,(\forall y\in G)\ (\,i\leqslant m\Longleftrightarrow\{x\}\overset{i}{+}\{y\}\neq\emptyset\,). \tag{3}$$

As it is not difficult to see (2) is equivalent to

$$(\forall i\in\mathbb{N})\,(\forall y\in G)\ (\,i>n\Longleftrightarrow\{x\}\overset{i}{+}\{y\}=\emptyset\,). \tag{4}$$

From (3) it follows $\{x\}\overset{m}{+}\{y\}\neq\emptyset$ for all $y\in G$. Since $m>n$, then, from (4), for each $y\in G$ we obtain $\{x\}\overset{m}{+}\{y\}=\emptyset$. The obtained contradiction proves that $n=m$. □

Further by the arity of an element $x\in G$ we mean the value $\alpha(x)$ and we denote it by $|x|$. Thus, $|x|=\alpha(x)$. From the definition of α it follows that for $x,y\in G$ and $i\in\mathbb{N}$ the result of $x\overset{i}{+}y$ is defined if and only if $i\leqslant|x|$.

$\mathbf{A_3}$ For all $x,y\in G$, $i\in\mathbb{N}$, if $i\leqslant|x|$, then

$$|x\overset{i}{+}y|=|x|+|y|-1.$$

$\mathbf{A_4}$ For $x,y,z\in G$ and $n,m\in\mathbb{N}$ such that $n\leqslant|x|$, $m\leqslant|y|$, we have

$$x\overset{n}{+}(y\overset{m}{+}z)=(x\overset{n}{+}y)\overset{n+m-1}{+}z\,.$$

$\mathbf{A_5}$ For $x,y,z\in G$ and $n,m\in\mathbb{N}$ such that $m<n\leqslant|x|$, holds

$$(x\overset{n}{+}y)\overset{m}{+}z=(x\overset{m}{+}z)\overset{n+|z|-1}{+}y.$$

Let $\mathcal{T}_n(A) = \mathcal{T}(A^n, A)$ be the set of all full multiplace functions (i.e. operations) on a set A. For all $f, g \in \mathcal{T}(A) = \bigcup_{n\in\mathbb{N}} \mathcal{F}_n(A)$ such that $|f| = n,\ |g| = m$ we define a *positional superposition* $\overset{i}{+}$ $(i \in \mathbb{N})$ putting:

$$(f \overset{i}{+} g)(a_1^{n+m-1}) = f(a_1^{i-1}, g(a_i^{i+m-1}), a_{i+m}^{n+m-1}) \tag{5}$$

where $a_1, \ldots, a_{n+m-1} \in A$ and a_i^j denotes the sequence $a_i, a_{i+1}, \ldots, a_j$ if $i \leqslant j$, and the empty symbol if $i > j$.

An algebra $(\mathcal{T}(A), \overset{1}{+}, \overset{2}{+}, \ldots)$ is called a *symmetrical positional algebra of operations*, its subalgebras – *positional algebras of operations*.

Let $\mathcal{F}_n(A)$ be the set of all partial n-place transformations on A and let Θ_n be an empty mapping from A^n into A. On the set

$$\mathcal{F}(A) = \bigcup_{n\in\mathbb{N}} \mathcal{F}_n(A) \cup \{\Theta_n\}$$

we consider partial binary operations $\overset{i}{+}$ $(i \in \mathbb{N})$ defined for $f \in \mathcal{F}_n(A)$, $g \in \mathcal{F}_m(A)$ and $a_1, \ldots, a_{n+m-1}, b, c \in A$ by the formula

$$(a_1^{n+m-1}, c) \in f \overset{i}{+} g \iff (\exists b)\Big((a_i^{i+m-1}, b) \in g \wedge (a_1^{i-1} b a_{i+m}^{n+m-1}, c) \in f\Big). \tag{6}$$

If $f \overset{i}{+} g$ is an empty transformation, then we put $f \overset{i}{+} g = \Theta_{n+m-1}$.

We assume that $\Theta_n \overset{i}{+} \Theta_m = \Theta_{n+m-1}$ for all $n, m \in \mathbb{N}$ and $i \leqslant n$. We assume also that $f \overset{i}{+} \Theta_m = \Theta_n \overset{i}{+} g = \Theta_{n+m-1}$. It is clear that the system $(\mathcal{F}(A), \overset{1}{+}, \overset{2}{+}, \ldots)$ is a positional algebra. This algebra is called a *symmetrical positional algebra of multiplace functions*, its subalgebras – *positional algebras of multiplace functions*.

Let $\mathfrak{G}_1 = (G_1, \overset{1}{+}, \overset{2}{+}, \ldots)$ and $\mathfrak{G}_2 = (G_2, \overset{1}{+}, \overset{2}{+}, \ldots)$ be two positional algebras. The mapping $P : G_1 \to G_2$ such that

1. $|g| = |P(g)|$ for each $g \in G_1$,

2. $P(g_1 \overset{i}{+} g_2) = P(g_1) \overset{i}{+} P(g_2)$ for all $g_1, g_2 \in G_1$ and $i \leqslant |g_1|$,

---

We put $n = |f|$ if and only if $f \in \mathcal{T}(A^n, A)$.

Analougously we define the operations $\overset{i}{+}$ on the set of all relations.

is called a *strong homomorphism of* $\mathfrak{G}_1$ *into* $\mathfrak{G}_2$. A strong homomorphism of a positional algebra $\mathfrak{G}$ into a symmetrical positional algebra of operations (multiplace functions) is called a *representation of* $\mathfrak{G}$ *by operations* (or *by multiplace functions*). A representation which is an isomorphism is called *faithful* (or *isomorphic*).

Let $\mathfrak{G} = (G, \overset{1}{+}, \overset{2}{+}, \ldots)$ be a positional algebra, e – an element not belonging to G, $G^* = G \cup \{e\}$. We put $|e| = 1$, $e \overset{1}{+} e = e$, $e \overset{1}{+} g = g$, $g \overset{i}{+} e = g$ for every $g \in G$ and $i \leqslant |g|$. It is not difficult to see that $\mathfrak{G}^* = (G^*, \overset{1}{+}, \overset{2}{+}, \ldots)$ is a positional algebra.

The following theorem was proved by V. D. Belousov (cf. [1]).

Theorem 1. *Every positional algebra is isomorphic to some positional algebra of operations.*

Corollary 1. *Every positional algebra is isomorphic to some positional algebra of multiplace functions and to some positional algebra of relations.*

Let $\mathfrak{G} = (G, \overset{1}{+}, \overset{2}{+}, \ldots)$ be a positional algebra, A – a non-empty set, $\Omega(A)$ – the set of all words on it. If $\omega_1, \ldots, \omega_n \in \Omega(A)$, then the word $\omega = \omega_1\omega_2 \ldots \omega_n$ is the sum of words $\omega_1, \omega_2, \ldots, \omega_n$. By $l(\omega)$ we denote the length of $\omega \in \Omega(A)$. For each word $\omega \in \Omega(A)$ of length $l(\omega) = n$ by ε^ω we denote some equivalence relation on $G_n = \{g \in G \,|\, |g| = n\}$, which corresponds to ω. So, $\varepsilon^\omega \subset G_{l(\omega)} \times G_{l(\omega)}$.

Let $\mathcal{E} = (\varepsilon^\omega)^{\omega \in B}$, where $B \subset \Omega(A)$, be a family of equivalence relations.

Definition 1. A family $\mathcal{E}$ is called *permissible* for positional algebra $\mathfrak{G}$, if for all $g, x_i, y_i \in G$, $i = 1, \ldots, n$ and $n = |g|$

$$x_1 \equiv y_1(\varepsilon^{\omega_1}) \wedge \ldots \wedge x_n \equiv y_n(\varepsilon^{\omega_n}) \implies g \underset{n}{\overset{1}{+}} x_n^1 \equiv g \underset{n}{\overset{1}{+}} y_n^1(\varepsilon^{\omega_1 \cdots \omega_n}),$$

where $g \underset{n}{\overset{1}{+}} x_n^1$ denotes $(\ldots((g \overset{n}{+} x_n) \overset{n-1}{+} x_{n-1}) \ldots) \overset{1}{+} x_1$.

Definition 2. A family $\mathcal{W} = (W^\omega)^{\omega \in B}$, where W^ω is a subset of $G_{l(\omega)}$, is an *l-ideal*, if for all $g, x_k \in G$, $k \neq i$, $k, i = 1, \ldots, n$, where $|g| = n$ and $l(\omega_1) = l(\omega) + \sum_{k=1, k\neq i}^{n} |x_k|$ the following implication is valid:

$$h \in W^\omega \implies ((g \underset{n}{\overset{i+1}{+}} x_n^{i+1}) \overset{i}{+} h) \underset{i-1}{\overset{1}{+}} x_{i-1}^1 \in W^{\omega_1}.$$

Definition 3. By a *determining pair* of a positional algebra $\mathfrak{G}$ we mean an ordered pair $(\mathcal{E},\mathcal{W})$, where $\mathcal{E}$ is a family of equivalence relations permissible for a positional algebra $\mathfrak{G}^*$, $\mathcal{W}$ is an l-ideal of a family of subsets W^ω such that W^ω is either empty or an ε^ω-class.

By $(H_a^\omega)_{a\in I_\omega}$, where $W^\omega \neq H_a^\omega$ for all $a \in I_\omega$, we denote the family of all ε^ω-classes (uniquely indexed by elements of some fixed set I_ω) such that the following implication, where $n = |g|$, holds

$$\left.\begin{aligned}(\dots((g \overset{n}{+} H_{a_n}^{\omega_n}) \overset{n-1}{+} H_{a_{n-1}}^{\omega_{n-1}})\dots) \overset{1}{+} H_{a_1}^{\omega_1} \subset H_b^{\omega_1\cdots\omega_n},\\ (\dots((g \overset{n}{+} H_{a_n}^{\omega'_n}) \overset{n-1}{+} H_{a_{n-1}}^{\omega'_{n-1}})\dots) \overset{1}{+} H_{a_1}^{\omega'_1} \subset H_c^{\omega'_1\cdots\omega'_n}\end{aligned}\right\} \Longrightarrow b = c\,. \quad (7)$$

Obviously for $I_\omega \cap I_{\omega'} = \emptyset$ the condition (7) is satisfied.

For every $g \in G$, $|g| = n$, we define the partial n-place function $P_{(\mathcal{E},\mathcal{W})}(g)$, where $(\mathcal{E},\mathcal{W})$ is a determining pair of a positional algebra $\mathfrak{G}$, putting

$$(a_1^n, b) \in P_{(\mathcal{E},\mathcal{W})}(g) \Longleftrightarrow (\dots((g \overset{n}{+} H_{a_n}^{\omega_n}) \overset{n-1}{+} H_{a_{n-1}}^{\omega_{n-1}})\dots) \overset{1}{+} H_{a_1}^{\omega_1} \subset H_b^{\omega_1\cdots\omega_n} \quad (8)$$

for some $\omega_1,\dots,\omega_n \in \Omega(A)$.

Theorem 2. *If $(\mathcal{E},\mathcal{W})$ is a determining pair of a positional algebra*

$$\mathfrak{G} = (G; \overset{1}{+}, \overset{2}{+}, \dots, \overset{n}{+}, \dots),$$

then the mapping $P_{(\mathcal{E},\mathcal{W})} : g \longmapsto P_{(\mathcal{E},\mathcal{W})}(g)$, where $g \in G$, is its representation by multiplace functions.

Proof. Let g_1, g_2 be arbitrary elements of G such that $|g_1| = n$, $|g_2| = m$. Assume that $(a_1^{n+m-1}, c) \in P_{(\mathcal{E},\mathcal{W})}(g_1 \overset{i}{+} g_2)$ for $i \leqslant n$. Then, by (8), we obtain

$$(\dots((g_1 \overset{i}{+} g_2) \overset{n+m-1}{+} H_{a_{n+m-1}}^{\omega_{n+m-1}}) \overset{n-1}{+} \dots) \overset{1}{+} H_{a_1}^{\omega_1} \subset H_c^{\omega_1\cdots\omega_{n+m-1}}.$$

If $x_i \in H_{a_i}^{\omega_i}$, $i = 1,\dots,n+m-1$, then

$$(g_1 \overset{i}{+} g_2) \underset{n+m-1}{\overset{1}{+}} x_{n+m-1}^1 \in H_c^{\omega_1\dots\omega_{n+m-1}},$$

which, by the axioms of a positional algebra, gives

$$(g_1 \overset{i}{+} g_2) \underset{n+m-1}{\overset{1}{+}} x_{n+m-1}^1 = \left(\left(g_1 \underset{n}{\overset{i+1}{+}} x_{n+m-1}^{i+m}\right) \overset{i}{+} \left(g_2 \underset{m}{\overset{1}{+}} x_{i+m-1}^i\right)\right) \underset{i-1}{\overset{1}{+}} x_{i-1}^1\,.$$

Therefore

$$\left(\left(g_1 \overset{i+1}{\underset{n}{+}} x_{n+m-1}^{i+m}\right) \overset{i}{+} \left(g_2 \overset{1}{\underset{m}{+}} x_{i+m-1}^{i}\right)\right) \overset{1}{\underset{i-1}{+}} x_{i-1}^{1} \in H_c^{\omega_1 \dots \omega_{n+m-1}}. \tag{9}$$

Hence

$$\left(\left(g_1 \overset{i+1}{\underset{n}{+}} x_{n+m-1}^{i+m}\right) \overset{i}{+} \left(g_2 \overset{1}{\underset{m}{+}} x_{i+m-1}^{i}\right)\right) \overset{1}{\underset{i-1}{+}} x_{i-1}^{1} \notin W^{\omega_1 \dots \omega_{n+m-1}}.$$

Since the family $\mathcal{W}$ is an l-ideal, then from the last condition follows that $g_2 \overset{1}{\underset{m}{+}} x_{i+m-1}^{i} \notin W^{\omega_i \dots \omega_{i+m-1}}$.

Suppose that

$$g_2 \overset{1}{\underset{m}{+}} x_{i+m-1}^{i} \in H_b^{\omega_i \dots \omega_{i+m-1}}. \tag{10}$$

This, by the permissibility of $\mathcal{E}$, gives

$$\left(\dots \left(g_2 \overset{m}{+} H_{a_{i+m-1}}^{\omega_{i+m-1}}\right) \overset{m-1}{+} \dots\right) \overset{1}{+} H_{a_i}^{\omega_i} \subset H_b^{\omega_i \dots \omega_{i+m-1}},$$

which implies

$$(a_i^{i+m-1}, b) \in P_{(\mathcal{E},\mathcal{W})}(g_2). \tag{11}$$

Thus (9) together with (10) proves that

$$g_1 \overset{n}{+} H_{a_{n+m-1}}^{\omega_{n+m-1}} \overset{n-1}{+} \cdots \overset{i+1}{+} H_{a_{i+m}}^{\omega_{i+m}} \overset{i}{+} H_b^{\omega_i \dots \omega_{i+m-1}} \overset{i-1}{+} H_{a_{i-1}}^{\omega_{i-1}} \overset{i-2i-2}{+} \cdots \overset{1}{+} H_{a_1}^{\omega_1}$$

is contained in $H_c^{\omega_1 \dots \omega_{n+m-1}}$. Hence

$$(a_1^{i-1} b\, a_{i+m}^{n+m-1}, c) \in P_{(\mathcal{E},\mathcal{W})}(g_1). \tag{12}$$

Now, comparing (11) with (12) we obtain

$$(a_1^{n+m-1}, c) \in P_{(\mathcal{E},\mathcal{W})}(g_1) \overset{i}{+} P_{(\mathcal{E},\mathcal{W})}(g_2).$$

So, we have proved that

$$P_{(\mathcal{E},\mathcal{W})}(g_1 \overset{i}{+} g_2) \subset P_{(\mathcal{E},\mathcal{W})}(g_1) \overset{i}{+} P_{(\mathcal{E},\mathcal{W})}(g_2).$$

The converse inclusion can be proved in the similar way. Thus

$$P_{(\mathcal{E},\mathcal{W})}(g_1 \overset{i}{+} g_2) = P_{(\mathcal{E},\mathcal{W})}(g_1) \overset{i}{+} P_{(\mathcal{E},\mathcal{W})}(g_2)$$

for all $g_1, g_2 \in G$ and $i \leqslant n$. Hence $P_{(\mathcal{E},\mathcal{W})}$ is a representation of the positional algebra $\mathfrak{G}$.

The fact that $P_{(\mathcal{E},\mathcal{W})}(g)$ is a function is a consequence of the permissibility of $\mathcal{E}$. □

We say that a *representation* P of a given positional algebra *is generated by a determining pair* if there exists a determining pair $(\mathcal{E},\mathcal{W})$ of this algebra such that $P = P_{(\mathcal{E},\mathcal{W})}$.

Theorem 3. *Every representation of a positional algebra by multiplace functions is generated by some of its determining pair.*

Proof. Let P be a representation of a positional algebra $\mathfrak{G} = (G; \overset{1}{+}, \overset{2}{+}, \ldots)$ by multiplace functions on a set A. For each vector $a_1^n = (a_1, \ldots, a_n) \in A^n$ we define the binary relation $\varepsilon^{a_1^n} \subset G_n \times G_n$ and the subset $W^{a_1^n} \subset G_n$ putting (for $g, g_1, g_2 \in G_n$)

$$g_1 \equiv g_2(\varepsilon^{a_1^n}) \iff P(g_1)\langle a_1^n\rangle = P(g_2)\langle a_1^n\rangle\,,$$
$$g \in W^{a_1^n} \iff P(g)\langle a_1^n\rangle = \emptyset.$$

Moreover, let

$$I(G) = \{n \in \mathbb{N} \mid (\exists g \in G)\, n = |g|\}\,,$$
$$\mathcal{E}_P = \{\varepsilon^{a_1^n} \mid a_1^n \in A^n, n \in I(G)\}\,,$$
$$\mathcal{W}_P = \{W^{a_1^n} \mid a_1^n \in A^n, n \in I(G)\}\,.$$

We prove that $(\mathcal{E}_P, \mathcal{W}_P)$ is a determining pair of the positional algebra $\mathfrak{G}$ such that $P = P_{(\mathcal{E}_P,\mathcal{W}_P)}$.

It is clear that $\varepsilon^{a_1^n}$ is an equivalence relation on G_n. To prove that $\mathcal{E}_P$ is permissible for the positional algebra $\mathfrak{G}^*$, let $g \in G$, $|g| = n$ and

$$x_1 \equiv y_1(\varepsilon^{a_1^{m_1}}),\ x_2 \equiv y_2(\varepsilon^{b_1^{m_2}})\,, \ldots,\ x_n \equiv y_n(\varepsilon^{c_1^{m_n}})\,.$$

This, by the definition, implies

$$P(x_1)\langle a_1^{m_1}\rangle = P(y_1)\langle a_1^{m_1}\rangle,$$
$$P(x_2)\langle b_1^{m_2}\rangle = P(y_2)\langle b_1^{m_2}\rangle,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$P(x_n)\langle c_1^{m_n}\rangle = P(y_n)\langle c_1^{m_n}\rangle,$$

which gives

$$P(g)\Big(P(x_1)\langle a_1^{m_1}\rangle, P(x_2)\langle b_1^{m_2}\rangle, \dots, P(x_n)\langle c_1^{m_n}\rangle\Big)$$
$$= P(g)\Big(P(y_1)\langle a_1^{m_1}\rangle, P(y_2)\langle b_1^{m_2}\rangle, \dots, P(y_n)\langle c_1^{m_n}\rangle\Big).$$

That is equivalent to

$$\Big(P(g) \overset{n}{+} P(x_n) \overset{n-1}{+} \cdots \overset{1}{+} P(x_1)\Big)\langle a_1^{m_1} b_1^{m_2} \dots c_1^{m_n}\rangle$$
$$= \Big(P(g) \overset{n}{+} P(y_n) \overset{n-1}{+} \cdots \overset{1}{+} P(y_1)\Big)\langle a_1^{m_1} b_1^{m_2} \dots c_1^{m_n}\rangle.$$

Since P is a homomorphism, we have

$$P(g \overset{1}{+}_n x_n^1)\langle a_1^{m_1} \dots c_1^{m_n}\rangle = P(g \overset{1}{+}_n y_n^1)\langle a_1^{m_1} \dots c_1^{m_n}\rangle,$$

i. e.

$$g \overset{1}{+}_n x_n^1 \equiv g \overset{1}{+}_n y_n^1(\varepsilon^{a_1^{m_1} \dots c_1^{m_n}}).$$

So, $\mathcal{E}_P$ is permissible for the positional algebra $\mathfrak{G}^*$.

To prove that $\mathcal{W}_P$ is an l-ideal, consider $g, x_i \in G$, $|g| = n$, $|x_i| = m_i$, $i = 1, \dots, n$. By the definition $|g \overset{1}{+}_n x_n^1| = \sum\limits_{i=1}^{n} m_i = m$.

If $g \overset{1}{+}_n x_n^1 \notin W^{a_1^{n_1}}$, then $P(g \overset{1}{+}_n x_n^1)\langle a_1^m\rangle \neq \emptyset$, whence

$$\Big(P(g) \overset{n}{+} P(x_n) \overset{n-1}{+} \cdots \overset{i}{+} P(x_i) \overset{i-1}{+} \cdots \overset{1}{+} P(x_1)\Big)\langle a_1^m\rangle \neq \emptyset,$$

therefore

$$P(g)\Big(P(x_1)\langle a_1^{m_1}\rangle, \dots, P(x_i)\langle a_{s_{i-1}+1}^{s_{i-1}+m_i}\rangle, \dots, P(x_n)\langle a_{s_{n-1}}^{m}\rangle\Big) \neq \emptyset,$$

where $s_{i-1} = \sum\limits_{k=1}^{i-1} m_k$. Hence $P(x_i)\langle a_{s_{i-1}+1}^{s_{i-1}+m_i}\rangle \neq \emptyset$, i.e. $x_i \notin W^{\omega_i^{i+m_i}}$ for each $i = 1, \dots, n$. So, $\mathcal{W}_P$ is an l-ideal and, in the consequence, $(\mathcal{E}_P, \mathcal{W}_P)$ is a determining pair of the positional algebra $\mathfrak{G}$.

To prove that $P = P_{(\mathcal{E}_P, \mathcal{W}_P)}$, let $a_1^n \in A^n$, $b \in A$ and

$$H_b^{a_1^n} = \{g \in G_n \mid P(g)\langle a_1^n\rangle = \{b\}\},$$

i. e.

$$g \in H_b^{a_1^n} \Longleftrightarrow (a_1^n, b) \in P(g).$$

It is clear that $e \in H_a^a$ for any $a \in A$. Also it is not difficult to see that $\{H_b^{a_1^n} \mid b \in A\}$ is the set of $\varepsilon^{a_1^n}$-classes, which are disjoint with $W^{a_1^n}$.

The set of all such classes satisfies (7). Indeed, if

$$g \overset{n}{+} H_{b_n}^{c_1^{m_n}} \overset{n-1}{+} \cdots \overset{1}{+} H_{b_1}^{a_1^{m_1}} \subset H_c^{a_1^{m_1} \ldots c_1^{m_n}}$$

and

$$g \overset{n}{+} H_{b_n}^{c'^{m'_n}_1} \overset{n-1}{+} \cdots \overset{1}{+} H_{b_1}^{a'^{m'_1}_1} \subset H_d^{a'^{m'_1}_1 \ldots c'^{m'_n}_1},$$

then

$$g \underset{n}{\overset{1}{+}} x_n^1 \in H_c^{a_1^{m_1} \ldots c_1^{m_n}} \quad \text{and} \quad g \underset{n}{\overset{1}{+}} y_n^1 \in H_c^{a'^{m'_1}_1 \ldots c'^{m'_n}_1},$$

where $x_i \in H_{b_i}^{d_1^{m_i}}$, $y_i \in H_{b_i}^{d'^{m'_i}_1}$, $i = 1, \ldots, n$, $d \in \{a, \ldots, c\}$. Since P is a homomorphism

$$\begin{aligned} c &= P(g)\Big(P(x_1)(a_1^{m_1}), \ldots, P(x_n)(c_1^{m_n})\Big) = P(g)(b_1, \ldots, b_n) \\ &= P(g)\Big(P(y_1)(a'^{m'_1}_1), \ldots, P(y_n)(c'^{m'_n}_1)\Big) = d, \end{aligned}$$

i.e. $c = d$. So, the condition (7) is satisfied.

Now let $(b_1^n, c) \in P(g)$, where $|g| = n$. Therefore $g \in H_c^{b_1^n}$. But $e \in H_{b_i}^{b_i}$, $i = 1, \ldots, n$, and $g = g \underset{n}{\overset{1}{+}} e$ imply

$$g \overset{n}{+} H_{b_n}^{b_n} \overset{n-1}{+} H_{b_{n-1}}^{b_{n-1}} \overset{n-1}{+} \cdots \overset{1}{+} H_{b_1}^{b_1} \subset H_c^{b_1^n},$$

which gives

$$(b_1^n, c) \in P_{(\mathcal{E}_P, \mathcal{W}_P)}(g). \tag{13}$$

Conversely, if (13) holds, then for some $a_1^{m_1}, \ldots, c_1^{m_n}$ we have

$$g \overset{n}{+} H_{b_n}^{c_1^{m_n}} \overset{n-1}{+} \cdots \overset{1}{+} H_{b_1}^{a_1^{m_1}} \subset H_c^{a_1^{m_1} \ldots c_1^{m_n}}.$$

This means that $g \underset{n}{\overset{1}{+}} x_n^1 \in H_c^{a_1^{m_1} \ldots c_1^{m_n}}$ for $x_1 \in H_{b_1}^{a_1^{m_1}}, \ldots, x_n \in H_{b_n}^{c_1^{m_n}}$. Thus $P(x_1)(a_1^{m_1}) = b_1$,..., $P(x_n)(c_1^{m_n}) = b_n$ and $(a_1^{m_1} \ldots c_1^{m_n}, c) \in P(g \underset{n}{\overset{1}{+}} x_n^1)$.

But P is a homomorphism, hence

$$(a_1^{m_1} \ldots c_1^{m_n}, c) \in P(g) \overset{n}{+} P(x_n) \overset{n-1}{+} \cdots \overset{1}{+} P(x_1).$$

Therefore

$$c = P(g)\Big(P(x_1)(a_1^{m_1}), \ldots, P(x_n)(c_1^{m_n})\Big) = P(g)(b_1, \ldots, b_n) = P(g)(b_1^n),$$

whence $(b_1^n, c) \in P(g)$.

So, $P(g) = P_{(\mathcal{E}_P, \mathcal{W}_P)}(g)$ for all $g \in G$, which proves $P = P_{(\mathcal{E}_P, \mathcal{W}_P)}$. $\square$

Problems

1. *Describe all representations of positional algebras by n-ary relations.*

2. *Find an abstract characterization of symmetrical positional algebras of operations (multiplace functions, n-ary relations).*

3. *Find an abstract characteristic of the class of all positional algebras of multiplace functions ordered by the relation of the set-theoretical inclusion.*
(For n-ary relations this problem was solved by F. M. Sokhatsky in [3].)

4. *Describe all automorphisms of the symmetrical positional algebra of operations (multiplace functions, n-ary relations).*

References

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

[2] **B. M. Schein**: *Lectures on transformation semigroups*, (Russian), Special course. Izdat. Saratov. Univ., Saratov 1970. (English translation: *Lectures on semigroups of transformations*, Amer. Math. Soc. Translations, II ser. **113** (1979), 123 – 181.)

[3] **F. M. Sokhatsky**: *On positional algebras*, (Russian), Mat. Issled. **71**, (1983), 104 – 117.

Department of Mathematics
Pedagogical University
21100 Vinnitsa
Ukraine
e-mail: vtrokhim@sovauma.com

Received September 29, 2001

Quasigroups and Related Systems **8** (2001), 97 – 104

The abstract groups (3, 3 | 3, p), their subgroup structure, and their significance for Paige loops

Petr Vojtěchovský

Abstract

For most (and possibly all) non-associative finite simple Moufang loops, three generators of order 3 can be chosen so that each two of them generate a group isomorphic to $(3,3\,|\,3,p)$. The subgroup structure of $(3,3\,|\,3,p)$ depends on the solvability of a certain quadratic congruence, and it is described here in terms of generators.

1. Introduction

Moufang loops and, more generally, diassociative loops are usually an abundant source of two-generated groups. In the end, this is what diassociativity is all about: every two elements generate an associative subloop, i.e. a group. (We refer the reader not familiar with the theory of loops to [5].) This short paper emerged as an offshoot of our larger-scale program to fully describe the subloop structure of all non-associative finite simple Moufang loops, sometimes called *Paige loops*.

Let $M^*(q)$ denote the Paige loop constructed over $F = GF(q)$ as in [4]. That is, $M^*(q)$ consists of vector matrices

$$M = \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix},$$

where $a,\ b \in F$, $\alpha,\ \beta \in F^3$, $\det M = ab - \alpha \cdot \beta = 1$, and where M is identified with $-M$. The multiplication in $M^*(q)$ coincides with the Zorn

2000 Mathematics Subject Classification: 20D30, 20N10
Keywords: non-associative finite simple Moufang loop, Paige loop, the abstract group (3, 3 | 3, p), loop generator, quadratic congruence

matrix multiplication

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}\begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac+\alpha\cdot\delta & a\gamma+d\alpha-\beta\times\delta \\ c\beta+b\delta+\alpha\times\gamma & \beta\cdot\gamma+bd \end{pmatrix},$$

where $\alpha\cdot\beta$ (resp. $\alpha\times\beta$) is the standard dot product (resp. cross product).

We have shown in [6, Theorem 1.1] that every $M^*(q)$ is three-generated, and when $q\neq 9$ is odd or $q=2$ then the generators can be chosen as

$$g_1=\begin{pmatrix} 1 & e_1 \\ 0 & 1 \end{pmatrix},\ g_2=\begin{pmatrix} 1 & e_2 \\ 0 & 1 \end{pmatrix},\ g_3=\begin{pmatrix} 0 & ue_3 \\ -u^{-1}e_3 & 1 \end{pmatrix}, \quad (1)$$

where u is a primitive element of F (cf. [6, Proposition 4.1]). In particular, note that g_1, g_2 and g_3 generate $M^*(p)$ for every prime p. We find it more convenient to use another set of generators.

Proposition 1. *Let $q\neq 9$ be an odd prime power or $q=2$. Then $M^*(q)$ is generated by three elements of order three.*

Proof. Let us introduce

$$\begin{aligned} g_4=g_3g_1 &= \begin{pmatrix} 0 & (0,0,u) \\ (0,u,-u^{-1}) & 1 \end{pmatrix}, \\ g_5=g_3g_2 &= \begin{pmatrix} 0 & (0,0,u) \\ (-u,0,-u^{-1}) & 1 \end{pmatrix}. \end{aligned}$$

It follows from (1) that $M^*(q)$ is generated by g_3, g_4, and g_5. One easily verifies that these elements are of order 3. □

The groups $\langle g_3,\, g_4\rangle$, $\langle g_3,\, g_5\rangle$ and $\langle g_4,\, g_5\rangle$ play therefore a prominent role in the lattice of subloops of $M^*(q)$. As we prove in Section 3, each of them is isomorphic to the group $(3,\, 3 \mid 3,\, p)$, defined below.

2. The abstract groups (3, 3 | 3, p)

The two-generated abstract groups $(l,\, m \mid n,\, k)$ defined by presentations

$$(l,\, m \mid n,\, k)=\langle x,\, y \mid x^l=y^m=(xy)^n=(x^{-1}y)^k\rangle \quad (2)$$

were first studied by Edington [3], for some small values of l, m, n and k. The notation we use was devised by Coxeter [1] and Moser [2], and has a

deeper meaning that we will not discuss here. From now on, we will always refer to presentation (2) when speaking about $(l,\, m \mid n,\, k)$.

The starting point for our discussion is Theorem 2, due to Edington [3, Theorem IV and pp. 208–210]. (Notice that there is a typo concerning the order of $(3,\, 3 \mid 3,\, n)$, and a misprint claiming that $(3,\, 3 \mid 3,\, 3)$ is isomorphic to A_4.). For the convenience of the reader, we give a short, contemporary proof.

Theorem 2 (Edington). *The group $G = (3,\, 3 \mid 3,\, n)$ exists for every $n \geqslant 1$, is of order $3n^2$, and is non-abelian when $n > 1$. It contains a normal subgroup $H = \langle x^2y,\, xy^2\rangle \cong C_n \times C_n$. In particular, $G \cong C_3$ when $n = 1$, $G \cong A_4$ when $n = 2$, and G is the unique non-abelian group of order 27 and exponent 3 when $n = 3$.*

Proof. Verify that $(3,\, 3 \mid 3,\, 1)$ is isomorphic to C_3. Let $n > 1$. Since $x(x^2y)x^{-1} = yx^{-1} = y(x^2y)y^{-1} \in H$, and $x^{-1}(xy^2)x = y^2x = y^{-1}(xy^2)y \in H$, the subgroup H is normal in G. It is an abelian group of order at most n^2 since $x^2y \cdot xy^2 = x(xy)^2y = x(xy)^{-1}y = xy^2 \cdot x^2y$. Clearly, $G/H \cong C_3$ (enumeration of cosets works fine), and hence $|G| = 3|H| \leqslant 3n^2$.

Let $N = \langle a\rangle \times \langle b\rangle \cong C_n \times C_n$, and $K = \langle f\rangle \leqslant \mathrm{Aut}(N)$, where f is defined by $f(a) = a^{-1}b$, $f(b) = a^{-1}$. Let E be the semidirect product of N and K via the natural action of K on N. We claim that E is non-abelian, and isomorphic to $(3,\, 3 \mid 3,\, n)$ with generators $x = (1,\, f)$ and $y = (a,\, f)$. We have $(a,\, f)^2 = (af(a),\, f^2) = (b,\, f^2)$, $(b,\, f^2)(1,\, f) = (b,\, \mathrm{id})$, and $(1,\, f)(b,\, f^2) = (a^{-1},\, \mathrm{id})$. Thus E is non-abelian, and generated by $(1,\, f)$, $(a,\, f)$. A routine computation shows that $(1,\, f)^3 = (a,\, f)^3 = ((1,\, f)(a,\, f))^3 = ((1,\, f)^{-1}(a,\, f))^n = 1$.

The group E proves that $|G| = 3|H| = 3n^2$. In particular, $H \cong C_n \times C_n$. □

We would like to give a detailed description of the lattice of subgroups of $(3,\, 3 \mid 3,\, p)$ in terms of generators x and y. From a group-theoretical point of view, the groups are rather boring, nevertheless, the lattice can be nicely visualized. The cases $p = 2$ and $p = 3$ cause troubles, and *we exclude them from our discussion for the time being.*

Lemma 3. *Let G and H be defined as before. Then H is the Sylow p-subgroup of G, and contains $p + 1$ subgroups $H(i) = \langle h(i)\rangle$, for $0 \leqslant i < p$, or $p = \infty$, all isomorphic to C_p. We can take*

$$h(i) = x^2y(xy^2)^i, \ \text{for} \ \ 0 \leqslant i < p \ \ \text{and} \ \ h(\infty) = xy^2.$$

There are p^2 Sylow 3-subgroups $G(k,\,l) = \langle g(k,\,l)\rangle$, for $0 \leqslant k,\,l < p$, all isomorphic to C_3. We can take

$$g(k,\,l) = (x^2y)^{-k}(xy^2)^{-l}x(x^2y)^k(xy^2)^l.$$

Proof. The subgroup structure of H is obvious. Every element of $G \setminus H$ has order 3, so there are p^2 Sylow 3-subgroups of order 3 in G. The subgroup H acts transitively on the set of Sylow 3-subgroups. (By Sylow Theorems, G acts transitively on the copies of C_3. As $|G| = 3p^2$, the stabilizer of each C_3 under this action is isomorphic to C_3. Since p and 3 are relatively prime, no element of H can be found in any stabilizer.) This shows that our list of Sylow 3-subgroups is without repetitions, thus complete. □

For certain values of p (see below), there are no other subgroups in G. For the remaining values of p, there are additional subgroups of order $3p$.

If $K \leqslant G$ has order $3p$, it contains a unique normal subgroup of order p, say $L \leqslant H$. Since L is normalized by both K and H, it is normal in G. Then G/L is a non-abelian group of order $3p$, and has therefore p subgroups of order 3. Using the correspondence of lattices, we find p subgroups of order $3p$ containing L (the group K is one of them).

Lemma 4. *The group $H(i)$ is normal in G if and only if*

$$i^2 + i + 1 \equiv 0 \,(\mathrm{mod}\, p). \tag{3}$$

If $p \equiv 1 \pmod 3$, there are two solutions to (3). For other values of p, there is no solution.

Proof. We have

$$\begin{aligned} x^{-1}h(i)x &= x^{-1}x^2y(xy^2)^ix = xy^2y^2(xy^2)^ix \\ &= (xy^2)(y^2x)^{i+1} = (x^2y)^{-(i+1)}(xy^2). \end{aligned}$$

Thus $x^{-1}h(i)x$ belongs to $H(i)$ if and only if $(x^2y)^{-(i+1)i}(xy^2)^i = (x^2y)(xy^2)^i$, i.e. if and only if i satisfies (3). Similarly,

$$\begin{aligned} y^{-1}h(i)y &= y^{-1}x^2y(xy^2)^iy = (y^2x)(xy^2)y^2(xy^2)^iy \\ &= (y^2x)(xy^2)(y^2x)^i = (x^2y)^{-(i+1)}(xy^2). \end{aligned}$$

Then $y^{-1}h(i)y$ belongs to $H(i)$ if and only if i satisfies (3).

The quadratic congruence (3) has either two solutions or none. Pick $a \in GF(p)^*$, $a \neq 1$. Then $a^2 + a + 1 = 0$ if and only if $a^3 = 1$, since $a^3 - 1 = (a-1)(a^2 + a + 1)$. This simple argument shows that (3) has a solution if and only if 3 divides $p - 1 = |GF(p)^*|$. □

Theorem 5 (The Lattice of Subgroups of $(3,\,3\mid 3,\,p)$**).** *For a prime* $p>3$*, let* $G=(3,\,3\mid 3,\,p)$*,* $H=\langle x^2y,\,xy^2\rangle$*,* $h(i)=x^2y(xy^2)^i$ *for* $0\leqslant i<p$*,* $h(\infty)=xy^2$*,* $H(i)=\langle h(i)\rangle$*,* $g(k,\,l)=(x^2y)^{-k}(xy^2)^{-l}x(x^2y)^k(xy^2)^l$ *for* $0\leqslant k,\,l<p$*, and* $G(k,\,l)=\langle g(k,\,l)\rangle$*.*

Then $H(\infty)\cong C_p$*,* $H(i)\cong C_p$*,* $G(k,\,l)\cong C_3$ *are the minimal subgroups of* G*, and* $H(i)\vee H(j)=H\cong C_p\times C_p$ *for every* $i\neq j$*. When* 3 *does not divide* $p-1$*, there are no other subgroups in* G*. Otherwise, there are additional* $2p$ *non-abelian maximal subgroups of order* $3p$*;* p *for each* $1<i<p$ *satisfying* $i^3\equiv 1\pmod p$*. These subgroups can be listed as* $K(i,\,l)=H(i)\vee G(0,\,l)$*, for* $0\leqslant l<p$*. Then* $H(i)\vee G(k',\,l')=K(i,\,l)$ *if and only if* $l'-l\equiv ik'\pmod p$*; otherwise* $H(i)\vee G(k',\,l')=G$*. Finally, let* $(k,\,l)\neq(k',\,l')$*. Then* $G(k,\,l)\vee G(k',\,l')=H(i)\vee G(k,\,l)$ *if and only if there is* $1<i<p$ *satisfying* $i^3\equiv 1\pmod p$ *such that* $l'-l\equiv(k'-k)i\pmod p$*; otherwise* $G(k,\,l)\vee G(k',\,l')=G$*.*

The group $(3,\,3\mid 3,\,2)$ *is isomorphic to* A_4*, the alternating group on* 4 *points, and* $(3,\,3\mid 3,\,3)$ *is the unique non-abelian group of order* 27 *and exponent* 3*.*

Proof. Check that $h(i)^{-1}g(k,\,l)h(i)=g(k+1,\,l+i)$, and conclude that $H(i)\vee G(k,\,l)=H(i)\vee G(k',\,l')$ if and only if $l'-l\equiv i(k'-k)\pmod p$. This also implies that, for some $1<i<p$, $H(i)\vee G(k',\,l')$ equals $K(i,\,l)$ if and only if $l'-l\equiv ik'\pmod p$ and $i^3\equiv 1\pmod p$.

Finally, if $S=G(k,\,l)\vee G(k',\,l')\neq G$, it contains a unique $H(i)\trianglelefteq G$. Moreover, we have $S=H(i)\vee G(k,\,l)=H(i)\vee G(k',\,l')$ solely on the grounds of cardinality, and everything follows. □

We illustrate Theorem 5 with $p=7$. The congruence (3) has two solutions, $i=2$ and $i=4$. The subgroup lattice of $(3,\,3\mid 3,\,7)$ is depicted in the 3D Figure 1. The 49 subgroups $G(k,\,l)$ are represented by a parallelogram that is thought to be in a horizontal position. All lines connecting the subgroups $G(k,\,l)$ with $K(2,\,0)$ and $K(4,\,0)$ are drawn. The lines connecting the subgroups $G(k,\,l)$ with $K(2,\,j)$, $K(4,\,j)$, for $1\leqslant j<p$, are omitted for the sake of transparency. The best way to add these missing lines is by the means of affine geometry of $GF(p)\times GF(p)$. To determine which groups $G(k,\,l)$ are connected to the group $K(i,\,j)$, start at $G(0,\,j)$ and follow the line with slope i, drawn modulo the parallelogram.

The group A_4 fits the description of Theorem 5, too, as can be seen from its lattice of subgroups in Figure 2. So does the group $(3,\,3\mid 3,\,3)$.

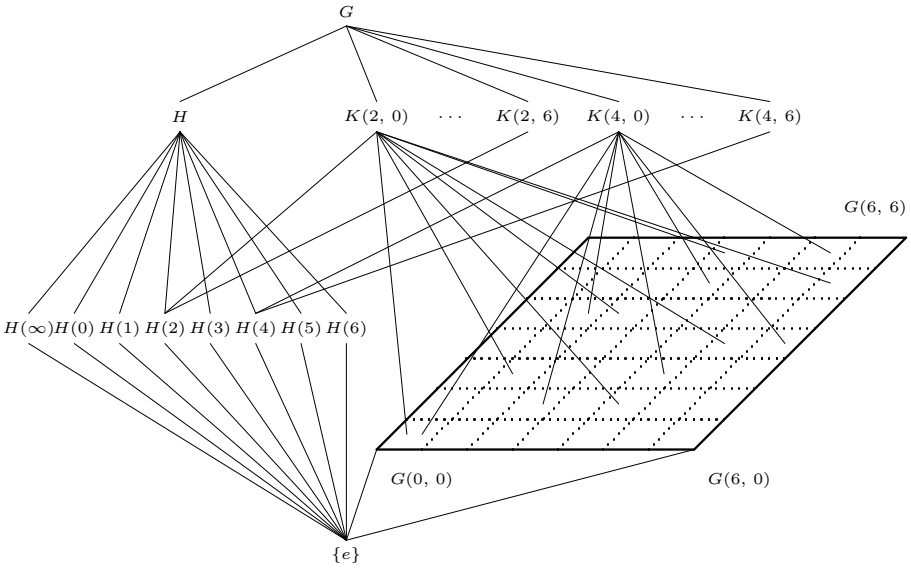


Figure 1: The lattice of subgroups of (3, 3 | 3, 7)

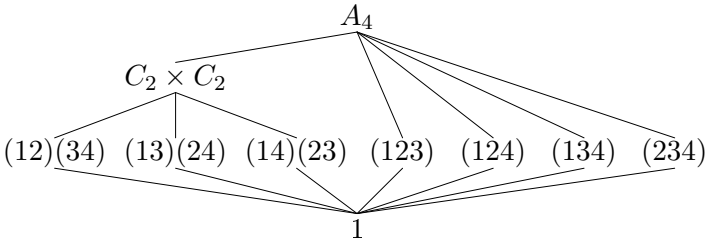


Figure 2: The subgroup structure of A_4

3. Three subgroups

We promised to show that each of the subgroups $\langle g_3,\, g_4\rangle$, $\langle g_3,\, g_5\rangle$, $\langle g_4,\, g_5\rangle$ of $M^*(q)$ is isomorphic to $(3,\, 3 \mid 3,\, p)$.

Proposition 3.1. *Let g_3, g_4, g_5 be defined as above, $q = p^r$. Then the three subgroups $\langle g_3,\, g_4\rangle$, $\langle g_3,\, g_5\rangle$, $\langle g_4,\, g_5\rangle$ of $M^*(p^r)$ are isomorphic to $(3,\, 3 \mid 3,\, p)$, if $q \neq 9$ is odd or $q = 2$.*

Proof. We prove that $G_1 = \langle g_3,\, g_4\rangle \cong (3,\, 3 \mid 3,\, p)$; the argument for the other two groups is similar. We have $g_3^3 = g_4^3 = (g_3g_4)^3 = (g_4g_3)^3 = (g_3^{-1}g_4)^p = (g_3^2g_4)^p = e$. Thus $G_1 \leqslant (3,\, 3 \mid 3,\, p)$. Also, $H_1 = \langle g_3^2g_4,\, g_3g_4^2\rangle \cong C_p \times C_p$. When $p \neq 3$, we conclude that $|G_1| = 3p^2$, since G_1 contains an element of order 3. When $p = 3$, we check that $g_3 \notin H_1$, and reach the same conclusion. □

We finish this paper with a now obvious observation, that in order to describe all subloops of $M^*(q)$, one only has to study the interplay of the isomorphic subgroups $\langle g_3,\, g_4\rangle$, $\langle g_3,\, g_5\rangle$, and $\langle g_4,\, g_5\rangle$.

References

[1] **H. S. M. Coxeter**: *The abstract groups $G^{m,n,p}$*, Trans. Amer. Math. Soc., **45** (1939), 73 – 150.

[2] **H. S. M. Coxeter and W. O. J. Moser**: *Generators and relations for discrete groups*, fourth edition, A Series of Modern Surveys in Mathematics, vol. **14**, Springer-Verlag (1980).

[3] **W. E. Edington**: *Abstract group definitions and applications*, Trans. Amer. Math. Soc., **25** (1923), 193 – 210.

[4] **L. Paige**: *A class of simple Moufang loops*, Proc. Amer. Math. Soc. **7** (1956), 471 – 482.

[5] **H. O. Pflugfelder**: *Quasigroups and Loops: Introduction*, Sigma series in pure mathematics, vol. **7**, Heldermann Verlag Berlin 1990.

[6] **P. Vojtěchovský**: *Generators for finite simple Moufang loops*, submitted, available at `http://www.vojtechovsky.com`

[7] **P. Vojtěchovský**: *Generators of nonassociative simple Moufang loops over finite prime fields*, J. Algebra **241** (2001), 186 – 192.

Department of Mathematics
Iowa State University
Ames, IA 50011
U.S.A.
petr@iastate.edu

Received May 7, 2001