Quasigroups and Related Systems **28** (2020), 203 – 228

Translatable quadratical quasigroups

Wieslaw A. Dudek and Robert A. R. Monzo

Abstract. The concept of a k-translatable groupoid is introduced. Those k-translatable quadratical quasigroups induced by the additive group of integers modulo m, where $k < 40$, are listed for $m \leqslant 1200$. The fine structure of quadratical quasigroups is explored in detail and the Cayley tables of quadratical quasigroups of orders 5, 9, 13 and 17 are produced. All but those of order 9 are k-translatable, for some k. Quadratical quasigroups induced by the additive group of integers modulo m are proved to be k-translatable, for some k. Open questions and thoughts about future research in this area are given.

1. Introduction

Geometrical motivations for the study of quadratical quasigroups have been given in [9, 10, 11, 12]. In particular Volenec [9, 10] defined a product $*$ on $\mathbb{C}$, the complex numbers, that defines a quadratical quasigroup. The product $x * y$ of two distinct elements is the third vertex of a positively oriented, isosceles right triangle in the complex plane, at which the right angle occurs.

The main aim of this paper is to give insight into the fine algebraic structure of quadratical quasigroups, in order to set the stage for, and to stimulate, further development of the general theory that is still in its relative infancy. This is the second of a series of four papers that advance this theory. We concern ourselves here mainly with the fine algebraic structure, rather than with the geometrical representations, of quadratical quasigroups. However, as noted by Volenec, each algebraic identity valid in the quadratical quasigroup $(\mathbb{C}, *)$ can be interpreted as a geometrical theorem and the theory of quadratical quasigroups gives a better insight into the mutual relations of such theorems ([9], page 108).

Volenec [9] proved that quadratical quasigroups have a number of properties, such as idempotency, mediality and cancellativity. These properties were applied by the authors in [3] to prove that quadratical quasigroups form a variety $\mathcal{Q}$. The spectrum of $\mathcal{Q}$ was proved to be contained in the set of all integers equal to 1 plus a multiple of 4. Quadratical quasigroups are uniquely determined by certain abelian groups and their automorphisms [1]. Necessary and sufficient conditions under which $\mathbb{Z}_m$, the additive group of integers modulo m, induces quadratical quasigroups are given in [3].

* Corresponding author: wieslaw.dudek@pwr.edu.pl
2010 Mathematics Subject Classification: 20N02, 20N05
Keywords: quadratical quasigroup, k-translatable groupoid, cycle.

This paper builds on the authors' work in [3], as well as the prior work of Polonijo [7], Volenec [9] and Dudek [1]. In Sections 3, 4, 5, 6 and 7 the notion of a *four-cycle*, which was introduced in [3], is used to explore in detail the fine structure of quadratical quasigroups. The concept of a four-cycle is applied in Sections 4 and 6 to produce Cayley tables for quadratical quasigroups of orders 5, 9, 13 and 17. These tables can be reproduced by model builders, but we would not achieve our aim of stimulating thought about the fine algebraic structure in that manner.

In Section 8, all of these quadratical quasigroups except those of order 9 are proved to be k-translatable, for some k. We prove that, up to isomorphism, there is only one quadratical quasigroup of order 9 and that it is self-dual. Quadratical quasigroups of order 25 and 29 are found. The one of order 25 is 18-translatable, its dual is 7-translatable, the quadratical quasigroup of order 29 is 12-translatable and its dual is 17-translatable.

Sections 8 and 9 of this paper explore other ways of constructing k-translatable quasigroups. We introduce the central concept of a k-translatable groupoid in Section 8 and use it to characterize quadratical quasigroups. In Section 9 necessary and sufficient conditions are found for a quasigroup induced by $\mathbb{Z}_m$ to be k-translatable. We prove that a quadratical quasigroup induced by $\mathbb{Z}_m$ is always k-translatable, for some k. The existence of k-translatable quadratical quasigroups induced by some $\mathbb{Z}_m$ is established for each integer k, where $1 < k < 11$. Values of m for which a quadratical quasigroup induced by $\mathbb{Z}_m$ is $(m-k)$-translatable are determined for each integer k, where $1 < k < 11$.

In Section 9 lists are given for k-translatable ($k < 40$) quadratical quasigroups of orders $m < 1200$, induced by $\mathbb{Z}_m$ and k-translatable quadratical quasigroups induced by $\mathbb{Z}_m$ for $m < 500$.

In a future publication, the two different approaches to the construction of quadratical quasigroups are united. It will be proved that a quadratical quasigroup is translatable if and only if it is induced by some $\mathbb{Z}_{4n+1}$. Finally, open questions and possible future directions for research are discussed in Section 9.

2. Preliminaries

Volenec [9] defined a *quadratical groupoid* as a right solvable groupoid satisfying the following condition:

$$xy \cdot x = zx \cdot yz. \tag{A}$$

He proved that such groupoids are quasigroups and satisfy the identities listed below.

Theorem 2.1. *A quadratical groupoid satisfies the following identities:*

$$x = x^2 \quad (idempotency), \tag{1}$$
$$x \cdot yx = xy \cdot x \quad (elasticity), \tag{2}$$
$$x \cdot yx = xy \cdot x = yx \cdot y \quad (strong\ elasticity), \tag{3}$$
$$yx \cdot xy = x \quad (bookend), \tag{4}$$
$$x \cdot yz = xy \cdot xz \quad (left\ distributivity), \tag{5}$$
$$xy \cdot z = xz \cdot yz \quad (right\ distributivity), \tag{6}$$
$$xy \cdot zw = xz \cdot yw \quad (mediality), \tag{7}$$
$$x(y \cdot yx) = (xy \cdot x)y, \tag{8}$$
$$(xy \cdot y)x = y(x \cdot yx), \tag{9}$$
$$xy = zw \longleftrightarrow yz = wx \quad (alterability). \tag{10}$$

These identities can be used to characterize quadratical quasigroups. Namely, the following theorem is proved in [3].

Theorem 2.2. *The class of all quadratical quasigroups form a variety uniquely defined by*

- (A), (3), (4), (7), *or*
- (1), (4), (7), *or*
- (2), (4), (7), *or*
- (4), (5), (10).

Quadratical quasigroups are uniquely characterized by commutative groups and their automorphisms. This characterization (proved in [1]) is presented below.

Theorem 2.3. *A groupoid $(G, \cdot)$ is a quadratical quasigroup if and only if there exists a commutative group $(G, +)$ in which for every $a \in G$ the equation $z + z = a$ has a unique solution $z \in G$ and φ, ψ are automorphisms of $(G, +)$ such that*

$$xy = \varphi(x) + \psi(y),$$

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

$$2\varphi\psi(x) = x$$

for all $x, y \in G$.

In this case we say that the quadratical quasigroup is *induced by* $(G, +)$.

We also will need the following two results proved in [3].

Theorem 2.4. *A finite quadratical groupoid has order $m = 4t + 1$.*

So, later it will be assumed that $m = 4t + 1$ for some natural t.

Theorem 2.5. *A quadratical groupoid induced by the additive group $\mathbb{Z}_m$ has the form*

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

where $a \in \mathbb{Z}_m$ *and*

$$2a^2 - 2a + 1 = 0. \tag{11}$$

3. Products in quadratical quasigroups

Let Q be a quadratical quasigroup and $a, b \in Q$ be two different elements. Suppose that $C = \{x_1, x_2, \ldots, x_n\} \subseteq Q$ consists of n distinct elements, such that $aba = x_1x_2 = x_2x_3 = x_3x_4 = \ldots = x_{n-1}x_n = x_nx_1$. Then C will be called an (*ordered*) *n-cycle based on aba*. Note that $x_1 \neq aba$, or else $x_1 = x_2 = \ldots = x_n = aba$. Note also that if $C = \{x_1, x_2, x_3, \ldots, x_n\} \subseteq Q$ is an n-cycle based on aba, then so is $C_i = \{x_i, x_{(i+1)mod\,n}, x_{(i+2)mod\,n}, \ldots, x_{(i+n-1)mod\,n}\}$.

In [3] is proved that in a quadratical quasigroup all n-cycles have the length $n = 4$. Moreover, if $a, b \in Q$ and $a \neq b$, then each element $x_1 \neq aba$ of Q is a member of a 4-cycle based on aba. Two 4-cycles based on aba, where $a \neq b$, are equal or disjoint. Note that in any 4-cycle $C = \{x_1, x_2, x_3, x_4\}$, $x_4 = x_1x_3$. Hence, $C = \{x, yx, y, xy\}$, where $x = x_1$ and $y = x_3$.

Definition 3.1. Let Q be a quadratical quasigroup with $\{a, b\} \subseteq Q$ and $a \neq b$. Then $\{a, b, ab, ba, aba\}$ contains five distinct elements. We will use the notation $[1,1] = a$, $[1,2] = ab$, $[1,3] = ba$ and $[1,4] = b$. We omit the commas and square brackets in the notation, when this causes no confusion, and write $11 = a$, $12 = ab$, $13 = ba$ and $14 = b$. For $n \geqslant 2$, by induction we define $n1 = (n-1)1 \cdot (n-1)2$, $n2 = (n-1)2 \cdot (n-1)4$, $n3 = (n-1)3 \cdot (n-1)1$, $n4 = (n-1)4 \cdot (n-1)3$ and $Hn = \{n1, n2, n3, n4\}$. On the occasions when we need to highlight that the element fk, $f \in \{1, 2, \ldots, n\}$ and $k \in \{1, 2, 3, 4\}$, is in the dual quadratical quasigroup Q^* we will denote it by fk^*. Similarly, $Hn^* = \{n1^*, n2^*, n3^*, n4^*\}$. Note that the values of both fk and fk^* depend on the choice of the elements a and b.

Example 3.2. $H2 = \{a \cdot ab, ab \cdot b, ba \cdot a, b \cdot ba\}$,
$H3 = \{(a \cdot ab)(ab \cdot b), (ab \cdot b)(b \cdot ba), (ba \cdot a)(a \cdot ab), (b \cdot ba)(ba \cdot a)\}$,
$H4 = \{(31 \cdot 32)(32 \cdot 34), (32 \cdot 34)(34 \cdot 33), (33 \cdot 31)(31 \cdot 32), (34 \cdot 33)(33 \cdot 31)\}$, where $31 = (a \cdot ab)(ab \cdot b)$, $32 = (ab \cdot b)(b \cdot ba)$, $33 = (ba \cdot a)(a \cdot ab)$ and $34 = (b \cdot ba)(ba \cdot a)$.

Example 3.3. $11^* = a$, $12^* = a * b$, $13^* = b * a$, $14^* = b$ and, for $n \geqslant 2$, by induction we define $n1^* = (n-1)1^* * (n-1)2^*$, $n2^* = (n-1)2^* * (n-1)4^*$, $n3^* = (n-1)3^* * (n-1)1^*$ and $n4^* = (n-1)4^* * (n-1)3^*$.

Example 3.4. $H2^* = \{a*(a*b), (a*b)*b, (b*a)*a, b*(b*a)\} = \{ba \cdot a, b \cdot ba, a \cdot ab, ab \cdot b\}$ and $52^* = 42^* \cdot 44^* = (32^* \cdot 34^*)(34^* \cdot 33^*) = (((ab*b)*(b*ba))*((b*ba)*(ba*a)))*(((b*ba)*(ba*a))*(ba*a)*(a*ab))$, where $a*ab = a*(a*b)$, $ab*b = (a*b)*b$, $ba*a = (b*a)*a$ and $b*ba = b*(b*a)$.

Note that the expression ab, when working in the dual groupoid $Q^* = (Q, *)$, equals $a * b$, which equals $b \cdot a$ in the original groupoid itself. This notation will cause no problems, as we will either calculate values only using the dot product or the star product, or when we are calculating using both products, as in Theorem 5.1, the distinction will be obvious.

The proofs of the following propositions are straightforward, using induction on n and the properties of quadratical quasigroups, and are omitted.

Proposition 3.5. *For any positive integer t, $t1 \cdot t4 = t2$, $t2 \cdot t3 = t4$, $t3 \cdot t2 = t1$ and $t4 \cdot t1 = t3$.*

Proposition 3.6. *For $t > 1$, $aba \cdot tk = (t-1)k$ for any $k \in \{1, 2, 3, 4\}$.*

Proposition 3.7. *For $t > 1$, $t1 \cdot aba = (t-1)2$, $t2 \cdot aba = (t-1)4$, $t3 \cdot aba = (t-1)1$ and $t4 \cdot aba = (t-1)3$.*

Proposition 3.8. *For any positive integer t, Ht contains 4 distinct elements.*

Proposition 3.9. *For any positive integer t, $Ht \cap \{aba\} = \emptyset$.*

Proposition 3.10. *For any positive integer t, $t1 \cdot t3 = t2 \cdot t1 = t3 \cdot t4 = t4 \cdot t2 = aba$.*

Proposition 3.11. *$Ht = \{t1, t3, t4, t2\}$ is a 4-cycle based on aba.*

Definition 3.12. We say that a *groupoid Q is of the form Qn*, for some positive integer n, if $Q = \{aba\} \bigcup_{t=1}^{n} Ht$ for some $\{a, b\} \subseteq Q$, where each Ht is as in Definition 3.1.

4. Quadratical quasigroups of form Q1 and Q2

We are now in a position to examine more closely the Cayley tables of quadratical quasigroups. This will aid in the construction of the tables for quadratical quasigroups of orders 5, 9, 13 and 17. Dudek [1] gave two examples of quadratical quasigroups of orders 5, 13 and 17 and six examples of quadratical quasigroups of order 9. A close examination of the fine structure will aid us in proving that all these quadratical quasigroups are of the form Qn, for some positive integer n. Each pair of quadratical quasigroups of orders 5, 13 or 17 will be proved to be dual groupoids. The 6 quadratical quasigroups of order 9 will be proved to be of form $Q2$ and self-dual. That is, up to isomorphism, there is only one quadratical quasigroup of order 9.

A method of constructing quadratical quasigroups of the form Qn is as follows. Proposition 3.6 implies that $aba \cdot Ht = H(t-1)$ for all $t \neq 1$. Since quadratical quasigroups are cancellative, we can assume that $aba \cdot H1 = Hn$. If we choose the value of $aba \cdot 11$ in $Hn = \{n1, n2, n3, n4\}$ then, using the properties of quadratical quasigroups, we can attempt to fill in the remaining unknown products in the

Cayley table. If this can be done without contradiction, then, using Theorem 2.2, we can check that the groupoid thus obtained is quadratical, by checking that it is bookend and medial. Completing the Cayley table is this way is not always possible, as shown in the following example.

Example 4.1. Suppose Q is a quadratical quasigroup of the form $Q2$. Then $aba \cdot 11 = aba \cdot a \in H2 = \{21, 22, 23, 24\} = \{a \cdot ab, ab \cdot b, ba \cdot a, b \cdot ba\}$. Now $aba \cdot a = a(ba \cdot a)$ and so $aba \cdot a \notin \{a \cdot ab, ba \cdot a\}$, since cancellativity, idempotency and alterability would imply that $a = b$ (if $aba \cdot a = ba \cdot a$) and $b = a \cdot ab$ (if $aba \cdot a = a \cdot ab$), the latter contradicting to the fact that two 4-cycles based on aba are equal or disjoint (cf. [3]). Hence, $aba \cdot a$ must be in the set $\{ab \cdot b, b \cdot ba\}$. However, if $aba \cdot a = b \cdot ba$, then by (10), $ab = ba \cdot aba = (b \cdot ab)a = aba \cdot a = b \cdot ba$, a contradiction since $H1 \cap H2 = \emptyset$.

Example 4.1 shows that $aba \cdot a = ab \cdot b$. Using the properties of quadratical quasigroups, the Cayley table of the groupoid of the form $Q2$ can only be completed in one way, as shown below here, in Table 1.

We then need to calculate all the possible products $xy \cdot yx$ and $xy \cdot zw$ in Table 1, to prove that they are equal to y and $xz \cdot yw$ respectively. Then, by Theorem 2.2, $Q2$ would be quadratical. This proves to be the case and we omit the detailed calculations. However, to give a flavour of the calculations we find all products $aba \cdot x$ and $x \cdot aba$ when $x \in H1$ and $aba \cdot a = ab \cdot b$.

Since $(a \cdot aba)(aba \cdot a) = (a \cdot aba)(ab \cdot b)$, it follows that we have $a \cdot aba = b \cdot ba$, $aba \cdot b = ba \cdot a$, $aba \cdot ab = (aba \cdot a)(aba \cdot b) = (ab \cdot b)(ba \cdot a) = b \cdot ba$ and, similarly $aba \cdot ba = a \cdot ab$. Then $aba \cdot ab = b \cdot ba$ implies $ba \cdot aba = ab \cdot b$. Also, $aba = (ab \cdot aba)(aba \cdot ab) = (ab \cdot aba)(b \cdot ba)$ implies $ab \cdot aba = ba \cdot a$. Finally, $b \cdot aba = (ab \cdot aba)(ba \cdot aba) = (ba \cdot a)(ab \cdot b) = a \cdot ab$.

$Q2$	$11 = a$	$12 = ab$	$13 = ba$	$14 = b$	aba	$21 = a \cdot ab$	$22 = ab \cdot b$	$23 = ba \cdot a$	$24 = b \cdot ba$
$11 = a$	a	$a \cdot ab$	aba	ab	$b \cdot ba$	ba	b	$ab \cdot b$	$ba \cdot a$
$12 = ab$	aba	ab	b	$ab \cdot b$	$ba \cdot a$	$b \cdot ba$	a	$a \cdot ab$	ba
$13 = ba$	$ba \cdot a$	a	ba	aba	$ab \cdot b$	ab	$b \cdot ba$	b	$a \cdot ab$
$14 = b$	ba	aba	$b \cdot ba$	b	$a \cdot ab$	$ab \cdot b$	$ba \cdot a$	a	ab
aba	$ab \cdot b$	$b \cdot ba$	$a \cdot ab$	$ba \cdot a$	aba	a	ab	ba	b
$21 = a \cdot ab$	$b \cdot ba$	b	$ba \cdot a$	a	ab	$a \cdot ab$	ba	aba	$ab \cdot b$
$22 = ab \cdot b$	$a \cdot ab$	$ba \cdot a$	ab	ba	b	aba	$ab \cdot b$	$b \cdot ba$	a
$23 = ba \cdot a$	ab	ba	$ab \cdot b$	$b \cdot ba$	a	b	$a \cdot ab$	$ba \cdot a$	aba
$24 = b \cdot ba$	b	$ab \cdot b$	a	$a \cdot ab$	ba	$ba \cdot a$	aba	ab	$b \cdot ba$

Table 1.

Proposition 4.2. *A quadratical quasigroup Q of order 9 is of the form $Q = Q2$.*

Proof. We have $Q = H1 \cup \{aba\} \cup C$, where C is a 4-cycle based on aba and $C \cap H1 = \emptyset$. We proceed to prove that $C = H2$.

Consider the following part of the Cayley table: $(H1 \cup \{aba\}) \cdot H1$.

Q	a	ab	ba	b
a	a		aba	ab
ab	aba	ab	b	
ba		a	ba	aba
b	ba	aba		b
aba				

From the table, clearly, if $ba \cdot a \in H1 \cup \{aba\}$, then $ba \cdot a \in \{ab, b\}$.

Assume that $ba \cdot a = ab$. Then we have $a = b \cdot ba$, $ab \cdot b = (ba \cdot a)b = (ba \cdot b) \cdot ab = aba \cdot ab = a(ba \cdot b) = (b \cdot ba)(ba \cdot b) = b(ba \cdot ab) = ba$ and $b = a \cdot ab$. Also, $aba \cdot a = a(ba \cdot a) = a \cdot ab = b$, $aba \cdot ab = ab \cdot (a \cdot ab) = ab \cdot b = ba$, $aba \cdot b = bab \cdot b = b(ab \cdot b) = b \cdot ba = a$ and $aba \cdot ba = (aba \cdot b)(aba \cdot a) = ab$. So, we have proved that $(H1 \cup \{aba\}) \cdot H1 = H1 \cup \{aba\}$.

Similarly, if $ba \cdot b = b$, then $(H1 \cup \{aba\}) \cdot H1 = H1 \cup \{aba\}$, which is not possible because, if $c \in C$, then $c \in C = \{ca, c \cdot ab, c \cdot ba, cb\}$, a contradiction. So, $ba \cdot a = c$, for some $c \in C$. Then, since $C = \{c, dc, d, cd\}$ for some $d \in C$, we have $aba = c \cdot dc = dc \cdot d = d \cdot cd = cd \cdot c$. So, $aba = (ba \cdot a) \cdot dc$, which implies $dc = b \cdot ba$. Also, $aba = cd \cdot (ba \cdot a)$, which implies $cd = a \cdot ab$. Then, $aba = dc \cdot d = (b \cdot ba)d$, which gives $d = ab \cdot b$. Hence, $C = \{a \cdot ab, ab \cdot b, ba \cdot a, b \cdot ba\} = H2$. □

So, we have proved that a quadratical quasigroup of order 9 must be the quasigroup Q2.

Open question. *Is a finite, idempotent, alterable, cancellative, elastic groupoid of form Qn quadratical?*

Note that we can prove that the answer is affirmative when $n = 1$ or $n = 2$.

Now, if we calculate the Cayley table for $(Q2)^*$, the dual of $Q2$, we see that the table for the dual product $*$ (defined as $a * b = b \cdot a$) is exactly the same as Table 1, where the product is the dot product $\cdot$. (For example, $((b * a) * a) * (b * a) = (a \cdot ab) * ab = ab \cdot (a \cdot ab) = b \cdot ba = (a * b) * b$ and, by Table 1, $(ba \cdot a) \cdot ba = ab \cdot b$). Hence, $Q2 \cong (Q2)^*$. Another way to put this is that the quadratical groupoid $Q2$ must be self-dual. An isomorphism θ between $Q2$ and $(Q2)^*$ is: $\theta a = a$, $\theta b = b$, $\theta(ab) = a * b$, $\theta(ba) = b * a$, $\theta(a \cdot ab) = a * (a * b)$, $\theta(ab \cdot b) = (a * b) * b$, $\theta(ba \cdot a) = (b * a) * a$ and $\theta(b \cdot ba) = b * (b * a)$.

Example 4.3. It is straightforward to calculate the Cayley tables of the quadratical quasigroups, each of order 9, given in [1]. They are each based on the group $\mathbb{Z}_3 \times \mathbb{Z}_3$ of ordered pairs of integers, with product being addition (mod 3). The products are defined as follows:

$(x, y) *_1 (z, u) = (y + z + 2u, x + y + 2z)$,
$(x, y) *_2 (z, u) = (2y + z + u, 2x + y + z)$,
$(x, y) *_3 (z, u) = (x + y + 2u, x + 2z + u)$,
$(x, y) *_4 (z, u) = (x + 2y + u, 2x + z + u)$,
$(x, y) *_5 (z, u) = (2x + y + 2z + 2u, 2x + 2y + z + 2u)$,
$(x, y) *_6 (z, u) = (2x + 2y + 2z + u, x + 2y + 2z + 2u)$.

In each table, if we calculate ab and ba for the ordered pairs $a = (1, 1)$ and $b = (1, 2)$ we see that $Q = \{aba\} \cup H1 \cup H2$ and that $aba \cdot a = ab \cdot b$. Therefore, these six quadratical quasigroups are isomorphic to each other and to $Q2$. We already knew that there is only one quadratical quasigroup of order 9, but these calculations clarify (and reinforce a conviction) that the quadratical quasigroups of order 9 presented in [1] are isomorphic.

Example 4.4. We now calculate the Cayley table for a groupoid $Q1$ and its dual, when $aba \cdot a \in \{ab, b\}$.

$Q1$	a	ab	ba	b	aba
a	a	ba	aba	ab	b
ab	aba	ab	b	a	ba
ba	b	a	ba	aba	ab
b	ba	aba	ab	b	a
aba	ab	b	a	ba	aba

$(Q1)^*$	a	$b * a$	$a * b$	b	aba
a	a	aba	b	$a * b$	$b * a$
$b * a$	$a * b$	$b * a$	a	aba	b
$a * b$	aba	b	$a * b$	$b * a$	a
b	$b * a$	a	aba	b	$a * b$
aba	b	$a * b$	$b * a$	a	aba

Table 2.

Checking these tables shows that each is medial and bookend and that, indeed, these two quadratical quasigroups are dual.

Open question. *Examining Tables* 1 *and* 2 *closely, we can show that any two distinct elements of* $Q1$ (*resp.* $(Q1)^*$, $Q2$) *generate* $Q1$ (*resp.* $(Q1)^*$, $Q2$). *This will later be seen to be the case also for* $Q3$, $Q4$ *and their duals. We conjecture that if* Q *is a quadratical quasigroup of form* Qn, *for some positive integer* n, *then it is generated by any two distinct elements. Such a property does not hold in quadratical quasigroups in general, as we shall now prove.*

Example 4.5. Since Q is a variety of groupoids, the direct product of quadratical quasigroups is quadratical. Hence, $Q1 \times Q1$ is quadratical. If we choose a base element, (a, b) say, then $Q1 \times Q1$ consists of six disjoint 4-cycles based on (a, b); namely,

$$\{(a,a),(a,aba),(a,ab),(a,ba)\}, \qquad \{(b,ab),(aba,ba),(ba,a),(ab,aba)\},$$
$$\{(ab,b),(b,b),(aba,b),(ba,b)\}, \qquad \{(ab,ab),(b,ba),(aba,a),(ba,aba)\},$$
$$\{(ba,ba),(ab,a),(b,aba),(aba,ab)\}, \quad \{(aba,aba),(ba,ab),(ab,ba),(b,a)\}.$$

If C is any one of these six 4-cycles, then no two distinct elements x and y of C generates $Q1 \times Q1$, because $\{x, y\} \subseteq C$ and C is a proper subquadratical quasigroup of $Q1 \times Q1$, isomorphic to $Q1$.

Example 4.6. $(Q1 \times Q1)^* = (Q1)^* \times (Q1)^*$ and $(Q1 \times (Q1)^*)^* = (Q1)^* \times Q1$. Note that (a, ba) and (ab, b) generate $Q1 \times (Q1)^*$ and (ba, a) and (b, ab) generate $(Q1)^* \times Q1$ while $Q1 \times Q1$ and $(Q1)^* \times (Q1)^*$ are not 2-generated.

5. The elements nk*

The following Theorem is easily proved for $k = 1$ and, by induction on k, is straightforward to prove for all $k \in \{0, 1, 2, \ldots\} = \mathbb{N}_0$. The proof is omitted but we proceed to give an idea of some of the calculations.

For $k = 0$

$$\begin{aligned}((4+4k)4)^* &= 44^* = (34 \cdot 33)^* = ((24 \cdot 23) \cdot (23 \cdot 21))^* \\ &= ((b \cdot ba)(ba \cdot a) \cdot (ba \cdot a)(a \cdot ab))^* = (ba \cdot a)(a \cdot ab) \cdot (a \cdot ab)(ab \cdot b) \\ &= (23 \cdot 21) \cdot (21 \cdot 22) = 33 \cdot 31 = 43 = ((4+4k)3).\end{aligned}$$

Note that we get the same result if we write

$$44^* = [(b * (b * a) * ((b * a) * a))] * [((b * a) * a) * (a * (a * b))].$$

Theorem 5.1. *For all $k \in \mathbb{N}_0$,*

$((1+4k)1)^*=(1+4k)1$, $((1+4k)2)^*=(1+4k)3$, $((1+4k)3)^*=(1+4k)2$, $((1+4k)4)^*=(1+4k)4$,
$((2+4k)1)^*=(2+4k)3$, $((2+4k)2)^*=(2+4k)4$, $((2+4k)3)^*=(2+4k)1$, $((2+4k)4)^*=(2+4k)2$,
$((3+4k)1)^*=(3+4k)4$, $((3+4k)2)^*=(3+4k)2$, $((3+4k)3)^*=(3+4k)3$, $((3+4k)4)^*=(3+4k)1$,
$((4+4k)1)^*=(4+4k)2$, $((4+4k)2)^*=(4+4k)1$, $((4+4k)3)^*=(4+4k)4$, $((4+4k)4)^*=(4+4k)3$.

Further, for simplicity, elements of the form $(xy)^*$ will be denoted as xy^*.

Now, considering the quadratical quasigroups of form Qn, from the remarks in the paragraph preceding Example 4.1, we see that there are at most 4 groupoids of the form Qn for any given integer n. Since the dual of a quadratical quasigroup of the form Qn must also have the form Qn, we can tell, from the following Theorem, which values of $aba \cdot a$ may yield groupoids that are duals of each other.

Theorem 5.2. *For all positive integers $n \geqslant 2$, the following identities are valid in a quadratical quasigroup of form Qn, depending on the value of $aba \cdot a$:*

$aba{\cdot}a$	$aba{\cdot}ab$	$aba{\cdot}ba$	$aba{\cdot}b$	$a{\cdot}aba$	$ab{\cdot}aba$	$ba{\cdot}aba$	$b{\cdot}aba$	$n1{\cdot}n2$	$n2{\cdot}n4$	$n3{\cdot}n1$	$n4{\cdot}n3$
$n1$	$n2$	$n3$	$n4$	$n2$	$n4$	$n1$	$n3$	a	ab	ba	b
$n2$	$n4$	$n1$	$n3$	$n4$	$n3$	$n2$	$n1$	ba	a	b	ab
$n3$	$n1$	$n4$	$n2$	$n1$	$n2$	$n3$	$n4$	ab	b	a	ba
$n4$	$n3$	$n2$	$n1$	$n3$	$n1$	$n4$	$n2$	b	ba	ab	a

$aba{\cdot}a$	$11{\cdot}34$	$23{\cdot}14$	$34{\cdot}14$	$14{\cdot}21$	
$n1$	$n3$	$n2$	$n1$	$n1$	$(n-1)2 = 11{\cdot}n1 = n2{\cdot}11$
$n2$	$n1$	$n4$	$n2$	$n2$	$(n-1)4 = 11{\cdot}n2 = n4{\cdot}11$
$n3$	$n4$	$n1$	$n3$	$n3$	$(n-1)1 = 11 \cdot n3 = n1{\cdot}11$
$n4$	$n2$	$n3$	$n4$	$n4$	$(n-1)3 = 11{\cdot}n4 = n3{\cdot}11$

Proof. We prove only the identities for when $aba{\cdot}a = n2$, as the proofs of the other three cases are similar. We have $aba{\cdot}n2$. Then, $aba = (a{\cdot}aba)(aba{\cdot}a) = (a{\cdot}aba){\cdot}n2$. By Proposition 3.11 and Theorem 2.1, $a \cdot aba = n4 = a \cdot bab = aba \cdot ab$. Then,

$n4 = aba \cdot ab = (aba \cdot a)(aba \cdot b) = n2 \cdot (aba \cdot b)$. By Proposition 3.5, $aba \cdot b = n3$. So $aba \cdot ba = (aba \cdot b)(aba \cdot a) = n3 \cdot n2 = n1$ (by Proposition 3.5). Then, $aba = (b \cdot aba)(aba \cdot b) = (b \cdot aba) \cdot n3$, which by Proposition 3.11 implies $b \cdot aba = n1$. Then, using Proposition 3.5, $ab \cdot aba = (a \cdot aba)(b \cdot aba) = n4 \cdot n1 = n3$ and $ba \cdot aba = (b \cdot aba)(a \cdot aba) = n1 \cdot n4 = n2$. We also have $n1 \cdot n2 = (aba \cdot ba)(ba \cdot aba) = ba$, $n2 \cdot n4 = (aba \cdot a)(a \cdot aba)) = a$, $n3 \cdot n1 = (aba \cdot b)(b \cdot aba) = b$ and $n4 \cdot n3 = (aba \cdot ab)(ab \cdot aba) = ab$. Now, $11 \cdot 34 = a \cdot (b \cdot ba)(ba \cdot a) = a(b \cdot ba) \cdot a(ba \cdot a) = (ab \cdot aba)(aba \cdot a) = n3 \cdot n2 = n1$, $34 \cdot 14 = (b \cdot ba)(ba \cdot a) \cdot b = (b \cdot ba)b \cdot (ba \cdot a)b = (b \cdot bab)(bab \cdot ab) = (b \cdot aba)(aba \cdot ab) = n1 \cdot n4 = n2$, $14 \cdot 21 = b(a \cdot ab) = ba \cdot bab = ba \cdot aba = n2$ and $23 \cdot 14 = (ba \cdot a)b = bab \cdot ab = aba \cdot ab = n4$.

Finally, $a \cdot n2 = a \cdot aba \cdot a = aba \cdot a \cdot aba = aba \cdot n4 = (n-1)4 = 11 \cdot n2$ and $n4 \cdot a = a \cdot aba \cdot a = aba \cdot a \cdot aba = (n-1)4 = n4 \cdot 11$.

This completes the proof of the validity of the identities indicated in row 3 of the two tables in Theorem 5.2, when $aba \cdot a = n2$. □

As mentioned above, Theorem 5.2 will be useful when we look for the duals of the quadratical quasigroups that we will call $Q3$ and $Q4$, as will the following concept.

Definition 5.3. If a quadratical quasigroup of form Qn exists for some integer n then the identity generated on the left (on the right) by an identity $kr \cdot ls = mt$, where $r, s, t \in \{1, 2, 3, 4\}$ and $k, l, m \leqslant n$, is defined as the identity

$$(aba \cdot kr)(aba \cdot ls) = aba \cdot mt \quad \text{(resp. } (kr \cdot aba)(ls \cdot aba) = mt \cdot aba)$$

and $kr \cdot ls = mt$ is called the *generating identity*.

Note that Propositions 3.6 and 3.7, along with Theorem 5.2, give the means of calculating identities generated on the left and right by a given identity. Multiplying on the left (or on the right) repeatedly n-times gives n distinct identities. These methods will later be used to prove that quadratical quasigroups of the form $Q6$ do not exist.

6. Quadratical quasigroups of forms Q3 and Q4

We give the Cayley tables of quadratical quasigroups of orders 13 and 17.

First we note that for a quadratical quasigroup of form $Q3$, if $aba \cdot a = n3 = 33 = (ba \cdot a)(a \cdot ab)$, then $aba \cdot a = a(ba \cdot a) = (a \cdot ab) \cdot aba = ab$, which implies, by cancellation, $ba \cdot a = b$, a contradiction because $H1 \cap H2 = \emptyset$. If $aba \cdot a = n4 = 34 = (b \cdot ba)(ba \cdot a)$, then $ab \cdot aba = a(b \cdot ba) = (ba \cdot a) \cdot aba = a$, which implies $b \cdot ba = a$, a contradiction. Hence, $aba \cdot a \in \{31, 32\} = \{(a \cdot ab)(ab \cdot b), (ab \cdot b)(b \cdot ba)\}$. Setting $aba \cdot a = a \cdot ab$ and using the properties of quadratical quasigroups (Theorem 2.1) we obtain the Cayley Table 3. It can be checked that it is medial and bookend and so, by Theorem 2.2, this groupoid is a quadratical quasigroup.

$Q3$	11	12	13	14	aba	21	22	23	24	31	32	33	34
11	11	21	aba	12	32	14	23	31	34	22	13	24	33
12	aba	12	14	22	34	32	13	33	21	23	24	31	11
13	23	11	13	aba	31	24	32	12	33	14	34	21	22
14	13	aba	24	14	33	31	34	22	11	32	21	12	23
aba	31	32	33	34	aba	11	12	13	14	21	22	23	24
21	32	23	34	13	12	21	31	aba	22	24	33	11	14
22	33	34	11	21	14	aba	22	24	32	12	23	13	31
23	24	14	31	32	11	33	21	23	aba	34	12	22	13
24	12	31	22	33	13	23	aba	34	24	11	14	32	21
31	34	13	21	24	22	12	33	14	23	31	11	aba	32
32	22	33	23	11	24	13	14	21	31	aba	32	34	12
33	14	22	32	23	21	34	24	11	12	13	31	33	aba
34	21	24	12	31	23	22	11	32	13	33	aba	14	34

Table 3.

There are then two ways to obtain the Cayley table for $(Q3)^*$. Firstly, we can use $aba * a = 32^* = [(a * b) * b] * [b * (b * a)]$ and, using the properties of quadratical quasigroups, we can then calculate the remaining products in Table 4.

Alternatively, we can calculate the products directly from Table 3, using our Theorem 5.1. For example, $23^* = (b * a) * a = a \cdot ab = 21$, and similarly $32^* = ((a * b) * b) * (b * (b * a)) = (ab \cdot b)(b \cdot ba) = 32$. Hence, $32^* * 23^* = 32 * 21 = 21 \cdot 32$. From Table 3, $21 \cdot 32 = 33$. But from Theorem 5.1, $33 = 33^*$. So, we obtain $32^* * 23^* = 33 = 33^*$. The remaining products in Table 4 can be calculated in similar fashion. Having already checked that Table 3 is quadratical, Table 4 also produces a quadratical quasigroup, the dual groupoid.

$(Q3)^*$	11^*	12^*	13^*	14^*	aba	21^*	22^*	23^*	24^*	31^*	32^*	33^*	34^*
11^*	11^*	21^*	aba	12^*	34^*	22^*	13^*	32^*	33^*	23^*	24^*	14^*	31^*
12^*	aba	12^*	14^*	22^*	33^*	34^*	24^*	31^*	11^*	13^*	21^*	32^*	23^*
13^*	23^*	11^*	13^*	aba	32^*	14^*	34^*	21^*	31^*	22^*	33^*	24^*	12^*
14^*	13^*	aba	24^*	14^*	31^*	32^*	33^*	12^*	23^*	34^*	11^*	21^*	22^*
aba	32^*	34^*	31^*	33^*	aba	11^*	12^*	13^*	14^*	21^*	22^*	23^*	24^*
21^*	34^*	13^*	33^*	24^*	12^*	21^*	31^*	aba	22^*	32^*	23^*	11^*	14^*
22^*	31^*	33^*	23^*	11^*	14^*	aba	22^*	24^*	32^*	12^*	34^*	13^*	21^*
23^*	14^*	22^*	32^*	34^*	11^*	33^*	21^*	23^*	aba	23^*	12^*	31^*	13^*
24^*	21^*	32^*	12^*	31^*	13^*	23^*	aba	34^*	24^*	11^*	14^*	22^*	33^*
31^*	33^*	24^*	11^*	21^*	22^*	12^*	23^*	14^*	34^*	31^*	13^*	aba	32^*
32^*	12^*	31^*	22^*	23^*	24^*	13^*	14^*	33^*	21^*	aba	32^*	34^*	11^*
33^*	22^*	23^*	34^*	13^*	21^*	24^*	32^*	11^*	12^*	14^*	31^*	33^*	aba
34^*	24^*	14^*	21^*	32^*	23^*	31^*	11^*	22^*	13^*	33^*	aba	12^*	34^*

Table 4.

Similarly, we can calculate the Cayley tables for $Q4$ and its dual $(Q4)^*$:

$Q4$	11	12	13	14	aba	21	22	23	24	31	32	33	34	41	42	43	44
11	11	21	aba	12	44	24	32	42	43	14	23	31	41	33	34	13	22
12	aba	12	14	22	43	44	23	41	34	32	13	42	21	11	31	24	33
13	23	11	13	aba	42	31	44	22	41	24	43	12	33	32	21	34	14
14	13	aba	24	14	41	42	43	33	21	44	34	22	11	23	12	31	32
aba	42	44	41	43	aba	11	12	13	14	21	22	23	24	31	32	33	34
21	44	32	43	23	12	21	31	aba	22	34	42	11	14	24	33	41	13
22	41	43	21	34	14	aba	22	24	32	12	33	13	44	42	23	11	31
23	31	24	42	44	11	33	21	23	aba	41	12	32	13	34	14	22	43
24	22	42	33	41	13	23	aba	34	24	11	14	43	31	12	44	32	21
31	43	23	34	13	22	12	42	14	33	31	41	aba	32	44	11	21	24
32	33	41	11	21	24	13	14	31	44	aba	32	34	42	22	43	23	12
33	24	14	44	32	21	41	34	11	12	43	31	33	aba	13	22	42	23
34	12	31	22	42	23	32	11	43	13	33	aba	44	34	21	24	14	41
41	21	34	12	31	32	14	33	44	23	22	11	24	43	41	13	aba	42
42	14	22	32	33	34	43	13	21	31	23	24	41	12	aba	42	44	11
43	32	33	23	11	31	34	24	12	42	13	44	21	22	14	41	43	aba
44	34	13	31	24	33	22	41	32	11	42	21	14	23	43	aba	12	44

Table 5.

$(Q4)^*$	11^*	12^*	13^*	14^*	aba	21^*	22^*	23^*	24^*	31^*	32^*	33^*	34^*	41^*	42^*	43^*	44^*
11^*	11^*	21^*	aba	12^*	41^*	34^*	24^*	43^*	42^*	13^*	33^*	22^*	44^*	14^*	23^*	31^*	32^*
12^*	aba	12^*	14^*	22^*	42^*	41^*	33^*	44^*	23^*	24^*	11^*	43^*	31^*	32^*	13^*	34^*	21^*
13^*	23^*	11^*	13^*	aba	43^*	22^*	41^*	32^*	44^*	34^*	42^*	14^*	21^*	24^*	31^*	12^*	33^*
14^*	13^*	aba	24^*	14^*	44^*	43^*	42^*	21^*	31^*	41^*	23^*	32^*	12^*	33^*	34^*	22^*	11^*
aba	43^*	41^*	44^*	42^*	aba	11^*	12^*	13^*	14^*	21^*	22^*	23^*	24^*	31^*	32^*	33^*	34^*
21^*	41^*	24^*	42^*	33^*	12^*	21^*	31^*	aba	22^*	44^*	34^*	11^*	14^*	23^*	43^*	32^*	13^*
22^*	44^*	42^*	31^*	23^*	14^*	aba	22^*	24^*	32^*	12^*	43^*	13^*	33^*	34^*	21^*	11^*	41^*
23^*	22^*	34^*	43^*	41^*	11^*	33^*	21^*	23^*	aba	32^*	12^*	42^*	13^*	44^*	14^*	24^*	31^*
24^*	32^*	43^*	21^*	44^*	13^*	23^*	aba	34^*	24^*	11^*	14^*	31^*	41^*	12^*	33^*	42^*	22^*
31^*	42^*	33^*	23^*	11^*	22^*	12^*	34^*	14^*	43^*	31^*	41^*	aba	32^*	13^*	44^*	21^*	24^*
32^*	21^*	44^*	12^*	31^*	24^*	13^*	14^*	41^*	33^*	aba	32^*	34^*	42^*	22^*	11^*	23^*	43^*
33^*	34^*	13^*	41^*	24^*	21^*	32^*	44^*	11^*	12^*	43^*	31^*	33^*	aba	42^*	22^*	14^*	23^*
34^*	14^*	22^*	32^*	43^*	23^*	42^*	11^*	31^*	13^*	33^*	aba	44^*	34^*	21^*	24^*	41^*	12^*
41^*	31^*	23^*	34^*	13^*	32^*	14^*	43^*	33^*	21^*	22^*	44^*	24^*	11^*	41^*	12^*	aba	42^*
42^*	33^*	32^*	11^*	21^*	34^*	31^*	13^*	22^*	41^*	23^*	24^*	12^*	43^*	aba	42^*	44^*	14^*
43^*	24^*	14^*	33^*	32^*	31^*	44^*	23^*	12^*	34^*	42^*	13^*	21^*	22^*	11^*	41^*	43^*	aba
44^*	12^*	31^*	22^*	34^*	33^*	24^*	32^*	42^*	11^*	14^*	21^*	41^*	23^*	43^*	aba	13^*	44^*

Table 6.

Groups of orders 13 and 17 are isomorphic to the additive groups $\mathbb{Z}_{13}$ and $\mathbb{Z}_{17}$, respectively. So, by Theorem 2.5, quasigroups $Q3$ and $Q4$ are isomorphic to quadratical quasigroups induced by $\mathbb{Z}_{13}$ and $\mathbb{Z}_{17}$, respectively. Direct computations show that $Q3$ is isomorphic to the quadratical quasigroup $(\mathbb{Z}_{13}, \cdot)$ with the operation $x \cdot y = 11x + 3y (\mathrm{mod}\, 13)$; the dual quasigroup $(Q3)^*$ is isomorphic to the quasigroup $(\mathbb{Z}_{13}, \circ)$ with the operation $x \circ y = 3x + 11y (\mathrm{mod}\, 13)$. Similarly,

$Q4$ is isomorphic to $(\mathbb{Z}_{17}, \cdot)$ with the operation $x \cdot y = 11x + 7y (\mathrm{mod}\, 17)$. Its dual quasigroup $(Q4)^*$ is isomorphic to the quasigroup $(\mathbb{Z}_{17}, \circ)$ with the operation $x \circ y = 7x + 11y (\mathrm{mod}\, 17)$.

7. No quadratical quasigroup of form Q6 exists

The quasigroup $x \cdot y = [9x + 21y]_{29}$ is clearly idempotent, medial and bookend. Therefore, by Theorem 2.2, it is quadratical. Set $a = 1$ and $b = 2$. Then we can calculate that $aba = 16$, $H1 = \{1, 22, 10, 2\}$, $H2 = \{7, 8, 24, 25\}$, $H3 = \{28, 17, 15, 4\}$, $H4 = \{29, 5, 27, 3\}$, $H5 = \{18, 21, 11, 14\}$, $H6 = \{23, 19, 13, 9\}$ and $H7 = \{26, 12, 20, 6\}$. Hence, this quasigroup and its dual are of the form $Q7$. So, we have so far shown that there are quadratical quasigroups of the form $Q1$, $Q2$, $Q3$, $Q4$ and $Q7$.

It follows from Theorem 4.11 [3] that there are no quadratical quasigroups of order 21 or 33, so there are no quadratical quasigroups of the form $Q5$ or $Q8$.

Theorem 7.1. *There is no quadratical quasigroup of form $Q6$.*

Proof. Case 1: $aba \cdot a = 61$. Using Propositions 3.6, 3.7, Theorem 5.2 and Theorem 2.1, we see that $aba \cdot a = 61$, by (10), implies

$$a \cdot 61 = 61 \cdot aba = 52 = 62 \cdot 11 \overset{(10)}{=} aba \cdot 62 = 52 \cdot 52. \tag{12}$$

Then, $62 = 61 \cdot 64$, by Proposition 3.5. This, by Proposition 3.6, gives $52 = 51 \cdot 54$. Also, $62 = 52 \cdot 54$, by Definition 3.1, whence $52 = 42 \cdot 44$, by Proposition 3.6 and (10), and so

$$52 = 51 \cdot 54 = 42 \cdot 44. \tag{13}$$

Theorem 5.2 implies $61 = 14 \cdot 21 = 34 \cdot 14$, $62 = 23 \cdot 14$ and $63 = 11 \cdot 34$. So, these identities generate the following:

$$52 = 63 \cdot 12 = 13 \cdot 64 = 64 \cdot 21 = 23 \cdot 63. \tag{14}$$

As a consequence of (12), (13), (15), Proposition 3.5 and Proposition 3.10 we can see that the solutions to the equation $52 = 12 \cdot x$ must be in the set $\{14, 22, 23, 24, 31, 32, 33, 34, 41, 42, 43, 51, 53\}$. Now, by Definition 3.1, we obtain $22 = 12 \cdot 14 \neq 52$ and so $x \neq 14$.

To eliminate the other possibilities for x we now use the generating identities (15) through (25), indicated in the Table 7 below.

	(15)	(16)	(17)	(18)	(19)	(20)	(21)	(22)	(23)	(24)	(25)
	$(n$–$1)2$ $=11{\cdot}n1$	$(n$–$1)2$ $=n2{\cdot}11$	$aba{\cdot}11$ $=61$	$11{\cdot}aba$ $=62$	*Prop.* 3.5	*Def.* 3.1	$n1=$ 14·21	$n2=$ 23·14	$n3=$ 11·34	$n1=$ 34·14	*idem.*
52	11·61	62·11	$aba{\cdot}62$	$61{\cdot}aba$	51·54	42·44	63·12	13·64	64·21	23·13	52·52
44	62·52	54·62	$aba{\cdot}54$	$52{\cdot}aba$	42·43	34·33	51·64	61·22	53·12	11·61	44·44
33	54·44	43·54	$aba{\cdot}43$	$44{\cdot}aba$	34·31	23·21	42·53	52·41	41·64	62·52	33·33
21	43·33	31·43	$aba{\cdot}31$	$33{\cdot}aba$	23·22	11·12	34·41	44·32	32·53	54·34	21·21
12	31·21	22·31	$aba{\cdot}22$	$21{\cdot}aba$	11·14	62·64	23·32	33·24	24·41	43·33	12·12
64	22·12	14·22	$aba{\cdot}14$	$12{\cdot}aba$	62·63	54·53	11·24	21·13	13·32	31·21	64·64
53	14·64	63·14	$aba{\cdot}63$	$64{\cdot}aba$	54·51	43·41	62·13	12·61	61·24	22·12	53·53
41	63·53	51·63	$aba{\cdot}51$	$53{\cdot}aba$	43·42	31·32	54·61	64·52	52·13	14·54	41·41
32	51·41	42·51	$aba{\cdot}42$	$41{\cdot}aba$	31·34	22·24	43·52	53·44	44·61	63·53	32·32
24	42·32	34·42	$aba{\cdot}34$	$32{\cdot}aba$	22·23	14·13	31·44	41·33	33·52	51·41	24·24
13	34·24	23·34	$aba{\cdot}23$	$24{\cdot}aba$	14·11	63·61	22·33	32·21	21·44	42·32	13·13
61	23·13	11·23	$aba{\cdot}11$	$13{\cdot}aba$	63·62	51·52	14·21	24·12	12·33	34·14	61·61
51	13·63	61·13	$aba{\cdot}61$	$63{\cdot}aba$	53·52	41·42	64·11	14·62	62·23	24·64	51·51
31	53·43	41·53	$aba{\cdot}41$	$43{\cdot}aba$	33·32	21·22	44·51	54·42	42·63	64·44	31·31
11	33·23	21·33	$aba{\cdot}21$	$23{\cdot}aba$	13·12	61·62	24·31	34·22	22·43	44·24	11·11
62	21·11	12·21	$aba{\cdot}12$	$11{\cdot}aba$	61·64	52·54	13·22	23·14	14·31	33·23	62·62
54	12·62	64·12	$aba{\cdot}64$	$62{\cdot}aba$	52·53	44·43	61·14	11·63	63·22	21·11	54·54
43	64·54	53·64	$aba{\cdot}53$	$54{\cdot}aba$	44·41	33·31	52·63	62·51	51·14	12·62	43·43
34	52·42	44·52	$aba{\cdot}44$	$42{\cdot}aba$	32·33	24·23	41·54	51·43	43·62	61·51	34·34
23	44·34	33·44	$aba{\cdot}33$	$34{\cdot}aba$	24·21	13·11	32·43	42·31	31·54	52·42	23·23
14	32·22	24·32	$aba{\cdot}24$	$22{\cdot}aba$	12·13	64·63	21·34	31·23	23·42	41·31	14·14
63	24·14	13·24	$aba{\cdot}13$	$14{\cdot}aba$	64·61	53·51	12·23	22·11	11·34	32·22	63·63
42	61·51	52·61	$aba{\cdot}52$	$51{\cdot}aba$	41·44	32·34	53·62	63·54	54·11	13·63	42·42
22	41·31	32·41	$aba{\cdot}32$	$31{\cdot}aba$	21·24	12·14	33·42	43·34	34·51	53·53	22·22

Table 7.

Assuming that $Q6$ is quadratical, using the properties of a quadratical quasigroup we will prove that all the remaining possible values of x lead to a contradiction.

When we use a particular value of an element we will refer to the column in which this value appears in Table 7. For example, we will use the fact that $52 = 63 \cdot 12$, from (21), henceforth without mention

By (21), if $52 = 12 \cdot 53 = 63 \cdot 12$, then $12 = 53 \cdot 63$, and, multiplying on the right by aba gives $64 = 41 \cdot 51$, which, along with $51 \cdot 41 = 24$, (from (24)) gives $51 = 64 \cdot 24$. This contradicts $51 = 64 \cdot 11$, from (21).

If $52 = 12{\cdot}51 = 63{\cdot}12$ then $12 = 51{\cdot}63 = 62{\cdot}64$, from (20). Hence, by (19) and (20), $61 = 63 \cdot 62 = 64 \cdot 51 = 51 \cdot 52$. Therefore, using (24), $51 = 52 \cdot 64 = 24 \cdot 64$, a contradiction.

If $52 = 12 \cdot 43 = 63 \cdot 12$ then, by (23), $12 = 43 \cdot 63 = 24 \cdot 41$. By Proposition 3.11 we have $63 \cdot 24 = 41 \cdot 43 = aba = 23 \cdot 24$, contradiction.

If $52 = 12 \cdot 42 = 63 \cdot 12$ then, by (23), is $12 = 42 \cdot 63 = 24 \cdot 41$. By Proposition 3.11 and (24), $51 = 41 \cdot 42 = 63 \cdot 24 = 24 \cdot 64$. So, by (20), $24 = 64 \cdot 63 = 14$,

contradiction.

If $52 = 12 \cdot 41 = 63 \cdot 12$ then, by (23), $12 = 41 \cdot 63 = 24 \cdot 41$ and so, using (15), $41 = 63 \cdot 24 = 63 \cdot 53$, contradiction.

If $52 = 12 \cdot 34 = 63 \cdot 12$ then, by (21), $12 = 34 \cdot 63 = 23 \cdot 32$ and, by Proposition 3.11 and (22), $42 = 32 \cdot 34 = 63 \cdot 23 = 63 \cdot 54$, contradiction.

If $52 = 12 \cdot 33 = 63 \cdot 12$ then, by (21), $12 = 33 \cdot 63 = 23 \cdot 32$ and so, by Propositions 3.11 and 3.5, $34 = 32 \cdot 33 = 63 \cdot 23 = 24 \cdot 23$, contradiction.

If $52 = 12 \cdot 32 = 63 \cdot 12$ then, by (21), $12 = 32 \cdot 63 = 23 \cdot 32$ and so, by (24), $32 = 63 \cdot 33 = 63 \cdot 53$, contradiction.

If $52 = 12 \cdot 31 = 63 \cdot 12$ then, by (15), $12 = 31 \cdot 63 = 31 \cdot 21$, contradiction.

If $52 = 12 \cdot 24 = 63 \cdot 12$ then, by (15), $12 = 24 \cdot 63 = 24 \cdot 41$, contradiction.

If $52 = 12 \cdot 23 = 63 \cdot 12$ then, by (21), $12 = 23 \cdot 63 = 23 \cdot 32$, contradiction.

If $52 = 12 \cdot 22 = 63 \cdot 12$ then, by (26), $12 = 22 \cdot 63 = 22 \cdot 31$, contradiction.

If $52 = 12 \cdot 14 = 63 \cdot 12$ then, by Proposition 3.11, $52 = 12 \cdot 14 = 22$, contradiction.

In this way we have proved that when $aba \cdot a = 61$, there is no right solvability, a contradiction.

The proof that there is no right solvability in Case 2 ($aba \cdot a = 62$), Case 3 ($aba \cdot a = 63$) and Case 4 ($aba \cdot a = 64$) are similar, where the values in Table 7 are different, according to Theorem 5.2. We omit these detailed calculations. □

There are 32 quadratical quasigroups of order 25 (cf. [3]). Some of them are isomorphic to quasigroups $Q1 \times Q1$, $Q1 \times (Q1)^*$, $(Q1)^* \times Q1$, $(Q1)^* \times (Q1)^*$.

Theorem 7.2. *Quadratical quasigroups induced by $\mathbb{Z}_{25}$ are not isomorphic to $Q1 \times Q1$, $Q1 \times (Q1)^*$, $(Q1)^* \times Q1$, $(Q1)^* \times (Q1)^*$.*

Proof. There are only two quadratical quasigroups induced by $\mathbb{Z}_{25}$ (cf. [3]). Their operations are given by $x \cdot y = 22x + 4y (\mathrm{mod}\, 25)$ and $x \circ y = 4x + 22y (\mathrm{mod}\, 25)$. Quasigroups $Q1$ and $(Q1)^*$ are isomorphic, respectively, to quasigroups $(\mathbb{Z}_5, \cdot)$ and $(\mathbb{Z}_5, \circ)$, where $x \cdot y = 4x + 2y (\mathrm{mod}\, 5)$ and $x \circ y = 2x + 4y (\mathrm{mod}\, 5)$.

Suppose that $(\mathbb{Z}_{25}, \cdot)$ is isomorphic to $Q1 \times Q1$ or to $Q1 \times (Q1)^*$. Since in $(\mathbb{Z}_5, \cdot)$ we have $x \cdot xy = yx$, in $Q1 \times Q1$ and $Q1 \times (Q1)^*$ for all $\overline{x} = (x, a) \neq \overline{y} = (y, a)$, $\bar{x} \cdot \bar{x}\bar{y} = \bar{y}\bar{x}$. But in $(\mathbb{Z}_{25}, \cdot)$ we have $22\bar{y} + 4\bar{x} = \bar{y}\bar{x} = \bar{x} \cdot \bar{x}\bar{y} = 10\bar{x} + 16\bar{y}$, which implies $\bar{x} = \bar{y}$. So, $(\mathbb{Z}_{25}, \cdot)$ cannot be isomorphic to $Q1 \times Q1$ or $Q1 \times (Q1)^*$.

In $(Q1)^* \times Q1$ and $(Q1)^* \times (Q1)^*$ for all $\overline{x} = (x, a) \neq \overline{y} = (y, a)$, we have $\bar{y}\bar{x} \cdot \bar{x} = \bar{x}\bar{y}$. But in $(\mathbb{Z}_{25}, \cdot)$ we have $22\bar{x} + 4\bar{y} = \bar{x}\bar{y} = \bar{y}\bar{x} \cdot \bar{x} = 9\bar{y} + 17\bar{x}$, which implies $\bar{x} = \bar{y}$. So, $(\mathbb{Z}_{25}, \cdot)$ also cannot be isomorphic to $(Q1)^* \times Q1$ or $(Q1)^* \times (Q1)^*$.

In the same manner we can prove that $(\mathbb{Z}_{25}, \circ)$ is not isomorphic to $Q1 \times Q1$, $Q1 \times (Q1)^*$, $(Q1)^* \times Q1$, $(Q1)^* \times (Q1)^*$. □

8. Translatable groupoids

Patterns of *translatability* can be hidden in the Cayley tables of quadratical quasigroups. One can assume the properties of quadratical quasigroups and then calcu-

late whether translatable groupoids of various orders exist with these properties. We proceed to prove that the quadratical quasigroups $Q1$, $(Q1)^*$, $Q3$, $(Q3)^*$, $Q4$ and $(Q4)^*$ are translatable and that $Q2$ is not translatable.

Definition 8.1. A finite groupoid $Q = \{1, 2, \ldots, n\}$ is called *k-translatable*, where $1 \leqslant k < n$, if its Cayley table is obtained by the following rule: If the first row of the Cayley table is $a_1, a_2, \ldots, a_n$, then the q-th row is obtained from the $(q-1)$-st row by taking the last k entries in the $(q-1)-$st row and inserting them as the first k entries of the q-th row and by taking the first $n-k$ entries of the $(q-1)$-st row and inserting them as the last $n-k$ entries of the q-th row, where $q \in \{2, 3, \ldots, n\}$. Then the (ordered) sequence $a_1, a_2, \ldots, a_n$ is called a *k-translatable sequence* of Q with respect to the ordering $1, 2, \ldots, n$. A groupoid is called a *translatable groupoid* if it has a k-translatable sequence for some $k \in \{1, 2, \ldots, n\}$.

It is important to note that a k-translatable sequence of a groupoid Q depends on the ordering of the elements in the Cayley table of Q. A groupoid may be k-translatable for one ordering but not for another (see Example 8.13 below). Unless otherwise stated we will assume that the ordering of the Cayley table is $1, 2, \ldots, n$ and the first row of the table is $a_1, a_2, \ldots, a_n$.

Proposition 8.2. *The additive group $\mathbb{Z}_n$ is $(n-1)$-translatable.*

The example below shows that there are $(n-1)$-translatable quasigroups of order n which are not a cyclic group.

Example 8.3. Consider the following three groupoids of order $n = 5$.

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

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

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

These groupoids are 4-translatable quasigroups but they are not groups. The first is idempotent, the second is without idempotents, the third is a cyclic quasigroup generated by 1 or by 5.

Proposition 8.4. *Any $(n-1)$-translatable groupoid of order n is commutative.*

Proof. In a k-translatable groupoid $i \cdot j = a_{(i-1)(n-k)+j}$, where the subscript is calculated modulo n. If $k = n-1$, then $i \cdot j = a_{i+j-1} = j \cdot i$. □

Theorem 8.5. *There are no $(m-1)$-translatable quadratical quasigroups of order m.*

Proof. By Proposition 8.4 such a quasigroup is commutative. Since it also is bookend and idempotent, $x = (y \cdot x) \cdot (x \cdot y) = (x \cdot y) \cdot (x \cdot y) = x \cdot y$, so it cannot be a quasigroup. □

The following proposition is obvious.

Proposition 8.6. *Every* 1*-translatable groupoid is unipotent, i.e., in such groupoid there exists an element* a *such that* $x^2 = a$ *for every* x*.*

Corollary 8.7. *There is no idempotent* 1*-translatable groupoid of order* $n > 1$*.*

Proposition 8.8. *A* k*-translatable groupoid of order* n *containing a cancellable element is a quasigroup if and only if* $(k, n) = 1$*.*

Proof. Let Q be a k-translatable groupoid of order n and let a be its cancellable element. Then in the Cayley table $[x_{ij}]_{n\times n}$ corresponding to this groupoid the a-row contains all elements of Q. Without loss of generality we can assume that this is the first row. If this row has the form $a_1, a_2, \ldots, a_n$, then other entries have the form $x_{ij} = a_{(i-1)(n-k)+j}$, where the subscript $(i-1)(n-k)+j$ is calculated modulo n. Obviously, for fixed $i = 1, 2, \ldots, n$, all entries $x_{i1}, x_{i2}, \ldots, x_{in}$ are different.

If $(n, k) = 1$, then also $(n, n-k) = 1$. So, in this case, also all $x_{1j}, x_{2j}, \ldots, x_{nj}$ are different. Hence, this table determines a quasigroup.

If $(n, k) = t > 1$, then $(n, n-k) = t$ and the equation $(i-1)(n-k) = 0$ has at least two solutions in the set $\{1, 2, \ldots, n\}$. Thus, in the Cayley table of such groupoid at least two rows are identical. Hence such groupoid cannot be a quasigroup. □

Theorem 8.9. *For every odd* n *and every* $k > 1$ *such that* $(k, n) = 1$ *there is at most one idempotent* k*-translatable quasigroup. For even* n *there are no such quasigroups.*

Proof. Let $a_1, a_2, a_3, \ldots, a_n$ be the first row of a k-translatable quasigroup Q.

This quasigroup is idempotent only in the case when in its Cayley table we have $1 = x_{11}$, $2 = x_{22} = a_{(n-k)+2}$, $3 = x_{33} = a_{2(n-k)+3}$, $4 = x_{44} = a_{3(n-k)+4}$, and so on. This means that the main diagonal of the table $[x_{ij}]_{n\times n}$ should contains elements $a_1, a_{(n-k)+2}, a_{2(n-k)+3}, \ldots, a_{(n-1)(n-k)+n}$, where all subscripts are calculated modulo n. Obviously, $a_{t(n-k)+t} = a_{t'(n-k)+t'}$ only in the case when $t - tk \equiv t' - t'k (\mathrm{mod}\, n)$, i.e., $(t - t')(k - 1) \equiv 0 (\mathrm{mod}\, n)$. If n is odd and $(n, k) = 1$, then for some k also is possible $(n, k-1) = 1$. In this case the equation $z(k-1) \equiv 0 (\mathrm{mod}\, n)$ has only one solution $z = 0$, so $t = t'$. Hence the diagonal of the table $[x_{ij}]_{n\times n}$ contains n different elements.

If n is even and $(n, k) = 1$, then k is odd. Thus, $k-1$ is even and $(n, k-1) \neq 1$. Hence, the equation $z(k-1) \equiv 0 (\mathrm{mod}\, n)$ has at least two solutions. Consequently, the diagonal of the table $[x_{ij}]_{n\times n}$ contains at least two equal elements. This contradicts to the fact that this quasigroup is idempotent. Therefore, for even n there are no idempotent k-translatable quasigroups. □

Corollary 8.10. *For every odd* n *and every* $k > 1$ *such that* $(n, k) = (n, k-1) = 1$ *there is exactly one idempotent* k*-translatable quasigroup of order* n*.*

Corollary 8.11. *The first row of an idempotent k-translatable quasigroup $Q = \{1, 2, \ldots, n\}$ has the form $1, a_2, a_3, \ldots, a_n$, where $a_{(i-1)(n-k)+i(\mathrm{mod}\, n)} = i$ for every $i \in Q$.*

Example 8.12. Consider an idempotent quasigroup $Q = \{1, 2, \ldots, 7\}$. From the proof of Theorem 8.9 it follows that if this quasigroup is 3-translatable, then the first row of its Cayley table has the form $1, 4, 7, 3, 6, 2, 5$. If it is 4-translatable, then the first row has the form $1, 3, 5, 7, 2, 4, 6$.

Example 8.13. The following example shows that for $Q1 = \{a, ab, ba, b, aba\}$ the sequence a, ba, aba, ab, b is 3-translatable, but $Q1$ presented in the form $Q1' = \{a, b, ab, ba, aba\}$ has no translatable sequences.

$Q1$	a	ab	ba	b	aba
a	a	ba	aba	ab	b
ab	aba	ab	b	a	ba
ba	b	a	ba	aba	ab
b	ba	aba	ab	b	a
aba	ab	b	a	ba	aba

$Q1'$	a	b	ab	ba	aba
a	a	ab	ba	aba	b
b	ba	b	aba	ab	a
ab	aba	a	ab	b	ba
ba	b	aba	a	ba	ab
aba	ab	ba	b	a	aba

The sequence $a, aba, b, a*b, b*a$ is 2-translatable for $(Q1)^* = \{a, b*a, a*b, b, aba\}$. $(Q1')^* = \{a, b, b*a, a*b, aba\}$ has no translatable sequence.

$(Q1)^*$	a	$b*a$	$a*b$	b	aba
a	a	aba	b	$a*b$	$b*a$
$b*a$	$a*b$	$b*a$	a	aba	b
$a*b$	aba	b	$a*b$	$b*a$	a
b	$b*a$	a	aba	b	$a*b$
aba	b	$a*b$	$b*a$	a	aba

$(Q1')^*$	a	b	$b*a$	$a*b$	aba
a	a	$a*b$	aba	b	$b*a$
b	$b*a$	b	a	aba	$a*b$
$b*a$	$a*b$	aba	$b*a$	a	b
$a*b$	aba	$b*a$	b	$a*b$	a
aba	b	a	$a*b$	$b*a$	aba

By Corollary 8.10, the quasigroup $Q1$ is isomorphic to a 3-translatable quasigroup $(\mathbb{Z}_5, \circ)$ with the operation $x \circ y = 4x + 2y (\mathrm{mod}\, 5)$. The dual quasigroup $(Q1)^*$ is isomorphic to a 2-translatable quasigroup $(\mathbb{Z}_5, \diamond)$ with the operation $x \diamond y = 2x + 4y (\mathrm{mod}\, 5)$.

Theorem 8.14. *A groupoid isomorphic to a k-translatable groupoid also has a k-translatable sequence.*

Proof. Let α be an isomorphism from a k-translatable groupoid $(Q, \cdot)$ to a groupoid $(S, \circ)$. If Q is with ordering $1, 2, \ldots, n$, then on S we consider ordering induced by α, namely $\alpha(1), \alpha(2), \ldots, \alpha(n)$. Suppose that the first row of the Cayley table of Q has the form $a_1, a_2, \ldots, a_n$. Then in the i-th row and j-th column of this table is $x_{ij} = a_{(i-1)(n-k)+j(\mathrm{mod}\, n)}$. Consequently, in the $\alpha(i)$-row and $\alpha(j)$-th column of the Cayley table $[z_{ij}]$ of S we have $z_{\alpha(i),\alpha(j)} = \alpha(i) \circ \alpha(j) = \alpha(i \cdot j) = \alpha(x_{ij})$. Since Q is k-translatable, for every $1 \leqslant t \leqslant k$, we have $a_{i,n-k+t} = a_{i+1,t}$. Thus, $z_{\alpha(i),\alpha(n-k+t)} = \alpha(i) \circ \alpha(n-k+t) = \alpha(x_{i,n-k+t}) = \alpha(x_{i+1,t}) = \alpha((i+1) \cdot t) =$

$\alpha(i+1)\circ\alpha(t) = z_{\alpha(i+1),\alpha(t)}$. This shows that S also is k-translatable (for ordering $\alpha(1), \alpha(2), \ldots, \alpha(n)$). □

Theorem 8.15. *An idempotent cancellable groupoid of order* 9 *is not translatable.*

Proof. Let $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9$ be the first row of the Cayley table of an idempotent cancellable groupoid Q. Then obviously $a_i \neq a_j$ for $i \neq j$. If Q is k-translatable, then $x_{44} = 4 = a_{3(9-k)+4}$. Since $3(9-k)+4 \equiv 4 (\mathrm{mod}\, 9)$ only for $k = 3$ and $k = 6$, this groupoid can be 3-translatable or 6-translatable. But in this case the fourth row coincides with the first, so Q cannot be cancellable. □

Corollary 8.16. *The quadratical quasigroups of order* 9 *are not translatable.*

Theorem 8.17. *An idempotent, bookend quasigroup Q, where $Q = \{1, 2, \ldots, n\}$, is k-translatable if and only if for every $i \in Q$ we have $i = a_{(s-1)(n-k)+t(\mathrm{mod}\, n)}$, where $s, t \in Q$ are such that*

$$\begin{cases} k-2 \equiv s(k-1)(\mathrm{mod}\, n), \\ ik-1 \equiv t(k-1)(\mathrm{mod}\, n). \end{cases} \tag{15}$$

Proof. Let $1, a_2, a_3, \ldots, a_n$ be the first row of the Cayley table $[x_{ij}]$ of an idempotent, bookend quasigroup $Q = \{1, 2, 3, \ldots, n\}$. If it is k-translatable, then, by Corollary 8.11, we have $a_{(i-1)(n-k)+i(\mathrm{mod}\, n)} = i$ for each $i \in Q$.

Moreover, in this quasigroup for every $i \in Q$ should be

$$\begin{aligned} i = (1 \cdot i) \cdot (i \cdot 1) = a_i \cdot x_{i1} = a_i \cdot a_{(i-1)(n-k)+1(\mathrm{mod}\, n)} \\ = s \cdot t = x_{st} = a_{(s-1)(n-k)+t(\mathrm{mod}\, n)}, \end{aligned}$$

where

$$\begin{cases} a_i = a_{(s-1)(n-k)+s(\mathrm{mod}\, n)} = s, \\ a_{(i-1)(n-k)+1(\mathrm{mod}\, n)} = a_{(t-1)(n-k)+t(\mathrm{mod}\, n)} = t \end{cases}$$

for some $s, t \in \{1, 2, \ldots, n\}$ satisfying (15).

The converse statement is obvious. □

Corollary 8.18. *A quadratical quasigroup of order* 25 *can be k-translatable only for $k = 7$ or $k = 18$.*

Proof. Let $Q = \{1, 2, \ldots, 25\}$ be a quadratical quasigroup. By Theorem 8.17, in this quasigroup for $i = 2$ should be

$$a_{27-k(\mathrm{mod}\, 25)} = x_{st} = a_{(s-1)(25-k)+t(\mathrm{mod}\, 25)},$$

where $s, t \in \{1, 2, \ldots, 25\}$ satisfy the equations

$$\begin{cases} k-2 \equiv s(k-1)(\mathrm{mod}\, 25), \\ 2k-1 \equiv t(k-1)(\mathrm{mod}\, 25). \end{cases}$$

To reduce the number of solutions of these equations observe that

$$x_{i1} \neq 1 \longleftrightarrow a_{(i-1)(25-k)+1(\mathrm{mod}\,25)} \neq 1 = a_1 \longleftrightarrow (i-1)k \not\equiv 0(\mathrm{mod}\,25).$$

The last, for $i = 6$, is possible only for $k \neq 5, 10, 15, 20$.

Also

$$x_{ii} \neq 1 \longleftrightarrow a_{(i-1)(25-k)+i(\mathrm{mod}\,25)} \neq 1 = a_1 \longleftrightarrow (i-1)(k-1) \not\equiv 0(\mathrm{mod}\,25),$$

which for $i = 6$ is possible only for $k \neq 6, 11, 16, 21$.

Hence Q cannot be k-translatable for $k \in \{5, 6, 10, 11, 15, 16, 20, 21\}$. By Theorem 8.5 and Corollary 8.7 it also cannot be k-translatable for $k \in \{1, 24, 25\}$.

In other cases, for $i = 2$, we obtain

k	2	3	4	7	8	9	12	13	14	17	18	19	22	23
s	25	13	9	5	8	4	10	3	24	15	23	19	20	18
t	3	15	19	23	20	24	18	25	4	12	5	9	8	10
x_{st}	a_5	a_4	a_{12}	a_{20}	a_{14}	a_{22}	a_{10}	a_{24}	a_7	a_{24}	a_9	a_{17}	a_{15}	a_{19}
a_{27-k}	a_{25}	a_{24}	a_{23}	a_{20}	a_{19}	a_{18}	a_{15}	a_{14}	a_{13}	a_{10}	a_9	a_8	a_5	a_4

Since $x_{st} = a_{27-k}$ only for $k = 7$ and $k = 18$, a quasigroup of order 25 can be k-translatable only for $k = 7$ and $k = 18$.

Direct computations shows that $\mathbb{Z}_{25}$ with the operation $x \cdot y = 22x + 4y(\mathrm{mod}\,25)$ is an example of a 7-translatable quadratical quasigroup of order 25. Its dual quasigroup is a 18-translatable. □

By changing the order of rows and columns in Tables 3, 4, 5 and 6 we obtain the following two theorems.

Theorem 8.19. *The sequence* $11, 12, 33, 21, 31, 34, 24, 32, 13, 14, 13, aba, 22$ *is* 5*-translatable for* $Q3 = \{11, 14, 34, 12, 23, 24, 33, aba, 32, 21, 22, 13, 31\}$.

The sequence $11^*, 12^*, 23^*, aba^*, 22^*, 13^*, 14^*, 34^*, 24^*, 32^*, 33^*, 21^*, 31^*$ *is* 8*-translatable for* $(Q3)^* = \{11^*, 14^*, 31^*, 13^*, 21^*, 22^*, 33^*, aba^*, 32^*, 23^*, 24^*, 12^*, 34^*\}$.

Theorem 8.20. *The sequence*

$$11, 12, 42, 43, 13, 14, 33, 21, 31, 44, 23, aba, 22, 41, 34, 24, 32$$

is 13*-translatable for*

$$Q4 = \{11, 14, 23, 24, 43, 31, 41, 12, 33, aba, 32, 13, 44, 34, 42, 21, 22\}.$$

The sequence

$$11^*, 12^*, 34^*, 24^*, 32^*, 44^*, 23^*, aba^*, 22^*, 41^*, 33^*, 21^*, 31^*, 13^*, 14^*, 43^*, 42^*$$

is 4*-translatable for*

$$(Q4)^* = \{11^*, 14^*, 21^*, 22^*, 44^*, 34^*, 42^*, 13^*, 33^*, aba^*, 32^*, 12^*, 43^*, 31^*, 41^*, 23^*, 24^*\}.$$

Quasigroups $Q3$ and $(Q3)^*$ are isomorphic, respectively, to quasigroups $(\mathbb{Z}_{13}, \cdot)$ and $(\mathbb{Z}_{13}, \circ)$, where $x \cdot y = 11x + 3y(\mathrm{mod}\,13)$ and $x \circ y = 3x + 11y(\mathrm{mod}\,13)$.

Quasigroups $Q4$ and $(Q4)^*$ are isomorphic, respectively, to quasigroups $(\mathbb{Z}_{17}, \cdot)$ and $(\mathbb{Z}_{17}, \circ)$, where $x \cdot y = 11x + 7y(\mathrm{mod}\,17)$ and $x \circ y = 7x + 11y(\mathrm{mod}\,17)$.

9. Translatable quasigroups induced by groups $\mathbb{Z}_m$

In this section we describe quadratical quasigroups induced by groups $\mathbb{Z}_m$. We start with some general results.

Lemma 9.1. *A quasigroup of the form $x * y = ax + by + c$ induced by a group $\mathbb{Z}_m$ is k-translatable if and only if $a + kb \equiv 0 (\mathrm{mod}\, m)$.*

Proof. The i-th row of the Cayley table of this quasigroup has the form

$$a(i-1)+c, a(i-1)+b+c, a(i-1)+2b+c, \ldots, a(i-1)+(m-1)b+c,$$

the $(i+1)$-row has the form

$$ai+c, ai+b+c, ai+2b+c, \ldots, ai+(m-1)b+c.$$

So, this quasigroup is k-translatable if and only if

$$ai+c = a(i-1)+(m-k)b+c (\mathrm{mod}\, m),$$

i.e., if and only if $a + kb \equiv 0 (\mathrm{mod}\, m)$. □

Corollary 9.2. *A quasigroup $(\mathbb{Z}_m, \diamond)$, where $x \diamond y = ax + y + c$, is $(m-a)$-translatable.*

Theorem 9.3. *Each quadratical quasigroup induced by group $\mathbb{Z}_m$ is k-translatable for some $1 < k < m-1$, namely for k such that $(a-1)k \equiv a (\mathrm{mod}\, m)$. This is valid for exactly one value of k.*

Proof. By Theorem 2.5 and Lemma 9.1 a quadratical quasigroup induced by $\mathbb{Z}_m$ is k-translatable if and only if there exist k such that $a \equiv (1-a)k (\mathrm{mod}\ m)$, i.e., $(a-1)k \equiv a (\mathrm{mod}\ m)$. Since $(a-1, m) = 1$, the last equation has exactly one solution in $\mathbb{Z}_m$ (cf. [8]). □

Theorem 9.4. *A quadratical quasigroup $(\mathbb{Z}_m, \cdot)$ with $x \cdot y = ax + (1-a)y$ is k-translatable if and only if its dual quasigroup $(\mathbb{Z}_m, \circ)$, where $x \circ y = (1-a)x + ay$, is $(m-k)$-translatable.*

Proof. Let $(\mathbb{Z}_m, \cdot)$ be k-translatable, then $(a-1)k \equiv a (\mathrm{mod}\, m)$, i.e., $k \equiv \frac{a}{a-1} (\mathrm{mod}\ m)$. If $(\mathbb{Z}_m, \circ)$ is t-translatable, then $ak \equiv (a-1) (\mathrm{mod}\, m)$, i.e., $t \equiv \frac{a-1}{a} (\mathrm{mod}\ m)$. ($\frac{a}{a-1}$ and $\frac{a1}{a}$ are well defined in $\mathbb{Z}_m$ because $(a, m) = (a-1, m) = 1$.) Thus $k + t = \frac{2a^2-2a+1}{a(a-1)} = 0 (\mathrm{mod}\ m)$, by Theorem 2.5. Hence $k + t = m$. □

Note that this theorem is not valid for quasigroups which are not quadratical. Indeed, a quasigroup $(\mathbb{Z}_7, \cdot)$ with $x \cdot y = 4x + y (\mathrm{mod}\, 7)$ is 3-translatable, but its dual quasigroup $(\mathbb{Z}_7, *)$, where $x * y = x + 4y (\mathrm{mod}\, 7)$, is 5-translatable.

Corollary 9.5. *There are no self-dual quadratical quasigroups induced by groups $\mathbb{Z}_m$.*

Using Theorem 9.3 we can calculate all k-translatable quadratical quasigroups induced by groups $\mathbb{Z}_m$. For this, it is better to rewrite the condition given in Theorem 9.3 in the form $(k-1)a \equiv k(\mathrm{mod}\, m)$.

2-TRANSLATABLE QUADRATICAL QUASIGROUPS

In this case $a \equiv 2(\mathrm{mod}\, m)$, where a satisfies (5). So, $5 \equiv 0(\mathrm{mod}\, m)$. Thus $m = 5$. Therefore there is only one 2-translatable quadratical quasigroup induced by $\mathbb{Z}_m$. It is induced by $\mathbb{Z}_5$ and has the form $x \cdot y = 2x + 4y(\mathrm{mod}\, 5)$.

3-TRANSLATABLE QUADRATICAL QUASIGROUPS

Then $2a \equiv 3(\mathrm{mod}\ m)$. Since (5) can be written in the form $2a(a-1)+1 = 0$, we also have $3a \equiv 2(\mathrm{mod}\ m)$. This, together with $4a \equiv 6(\mathrm{mod}\ m)$, implies $a = 4$. Hence $8 \equiv 3(\mathrm{mod}\ m)$. Thus $m = 5$. Therefore there is only one 3-translatable quadratical quasigroup induced by $\mathbb{Z}_m$. It is induced by $\mathbb{Z}_5$ and has the form $x \cdot y = 4x + 2y(\mathrm{mod}\, 5)$.

4-TRANSLATABLE QUADRATICAL QUASIGROUPS

Now $3a \equiv 4(\mathrm{mod}\, m)$ and $6a \equiv 8(\mathrm{mod}\, m)$. From (5) we obtain $6a(a-1)+3 = 0$, which together with the last equation gives $8a \equiv 5(\mathrm{mod}\, m)$. This, with $9a \equiv 12(\mathrm{mod}\, m)$, implies $a = 7$. Hence $21 \equiv 4(\mathrm{mod}\, m)$. Thus $m = 17$. Therefore there is only one 4-translatable quadratical quasigroup induced by $\mathbb{Z}_m$. It is induced by $\mathbb{Z}_{17}$ and has the form $x \cdot y = 7x + 11y(\mathrm{mod}\, 17)$.

5-TRANSLATABLE QUADRATICAL QUASIGROUPS

Now $4a \equiv 5(\mathrm{mod}\, m)$ and $5a \equiv 3(\mathrm{mod}\, m)$, by (5). Thus, $16a \equiv 20(\mathrm{mod}\, m)$ and $15a \equiv 9(\mathrm{mod}\, m)$, which implies $a = 11$. Hence $44 \equiv 5(\mathrm{mod}\, m)$. Thus $m = 13$. Therefore a 5-translatable quadratical quasigroup is induced by $\mathbb{Z}_{13}$ and has the form $x \cdot y = 11x + 4y(\mathrm{mod}\, 13)$.

6-TRANSLATABLE QUADRATICAL QUASIGROUPS

Now $5a \equiv 6(\mathrm{mod}\, m)$ and $12a \equiv 7(\mathrm{mod}\, m)$, by (5). Thus, $25a \equiv 30(\mathrm{mod}\, m)$ and $24a \equiv 14(\mathrm{mod}\, m)$, which implies $a = 16$. Hence $80 \equiv 6(\mathrm{mod}\, m)$. Thus $m = 37$. Therefore a 6-translatable quadratical quasigroup is induced by $\mathbb{Z}_{37}$ and has the form $x \cdot y = 16x + 22y(\mathrm{mod}\, 37)$.

7-TRANSLATABLE QUADRATICAL QUASIGROUPS

Now $6a \equiv 7(\mathrm{mod}\, m)$ and $7a \equiv 4(\mathrm{mod}\, m)$, by (5). Thus, $a \equiv (-3)(\mathrm{mod}\, m)$ and $(-18) \equiv 7(\mathrm{mod}\, m)$. Consequently, $25 \equiv 0(\mathrm{mod}\, m)$. Hence $m = 25$. (The case $m = 5$ is impossible because must be $m > k = 7$.) Therefore $a = 22$. So, a 7-translatable quadratical quasigroup is induced by $\mathbb{Z}_{25}$ and has the form $x \cdot y = 22x + 4y(\mathrm{mod}\, 25)$.

8-TRANSLATABLE QUADRATICAL QUASIGROUPS

Now $7a \equiv 8(\mathrm{mod}\, m)$ and $16a \equiv 9(\mathrm{mod}\, m)$, by (5). Thus, $49a \equiv 56(\mathrm{mod}\, m)$ and $48a \equiv 27(\mathrm{mod}\, m)$ shows that $a \equiv 29(\mathrm{mod}\, m)$. Hence $7 \cdot 29 \equiv 8(\mathrm{mod}\, m)$ and $16 \cdot 29 \equiv 9(\mathrm{mod}\, m)$ imply $195 \equiv 0(\mathrm{mod}\, m)$ and $455 \equiv 0(\mathrm{mod}\, m)$. Therefore, $65 \equiv 0(\mathrm{mod}\, m)$. Since $m > k = 8$, the last means that $m = 65$ or $m = 13$. So, a

8-translatable quadratical quasigroup is induced by $\mathbb{Z}_{13}$ or by $\mathbb{Z}_{65}$. In the first case it has the form $x \cdot y = 3x + 11y (\mathrm{mod}\, 13)$, in the second $x \cdot y = 29x + 37y (\mathrm{mod}\, 65)$.

9-translatable quadratical quasigroups

In this case $8a \equiv 9 (\mathrm{mod}\, m)$ and $9a \equiv 5 (\mathrm{mod}\, m)$, by (5). So, $a \equiv (-4) (\mathrm{mod}\, m)$, and consequently $41 \equiv 0 (\mathrm{mod}\, m)$. Thus, $m = 41$. Hence a 9-translatable quadratical quasigroup is induced by $\mathbb{Z}_{41}$ and has the form $x \cdot y = 37x + 5y (\mathrm{mod}\, 41)$.

10-translatable quadratical quasigroups

In a similar way we can see that there is only one 10-translatable quasigroup induced by $\mathbb{Z}_m$. It is induced by $\mathbb{Z}_{101}$ and has the form $x \cdot y = 46x + 56y (\mathrm{mod}\, 101)$.

As a consequence of the above calculations and Theorem 9.4 we obtain the following list of $(m - k)$-translatable quadratical quasigroups induced by $\mathbb{Z}_m$.

$(m-2)$-translatable quadratical quasigroups

There is only one such quasigroup. It is induced by $\mathbb{Z}_5$ and has the form $x \cdot y = 4x + 2y (\mathrm{mod}\, 5)$.

$(m-3)$-translatable quadratical quasigroups

There is only one such quasigroup. It has the form $x \cdot y = 2x + 4y (\mathrm{mod}\, 5)$.

$(m-4)$-translatable quadratical quasigroups

There is only one such quasigroup. It has the form $x \cdot y = 11x + 7y (\mathrm{mod}\, 17)$.

$(m-5)$-translatable quadratical quasigroups

There is only one such quasigroup. It has the form $x \cdot y = 3x + 11y (\mathrm{mod}\, 13)$.

$(m-6)$-translatable quadratical quasigroups

There is only one such quasigroup. It has the form $x \cdot y = 22x + 16y (\mathrm{mod}\, 37)$.

$(m-7)$-translatable quadratical quasigroups

There is only one such quasigroup. It has the form $x \cdot y = 4x + 22y (\mathrm{mod}\, 25)$.

$(m-8)$-translatable quadratical quasigroups

There are only two such quasigroups. The first has the form $\cdot x \cdot y = 11x + 3y (\mathrm{mod}\, 13)$, the second $x \cdot y = 37x + 29y (\mathrm{mod}\, 65)$.

$(m-9)$-translatable quadratical quasigroups

There is only one such quasigroup. It has the form $x \cdot y = 5x + 37y (\mathrm{mod}\, 41)$.

$(m-10)$-translatable quadratical quasigroups

Such a quasigroup is induced by $\mathbb{Z}_{101}$ and has the form $x \cdot y = 56x + 46y (\mathrm{mod}\, 101)$.

Below, for $k < 40$, we list all k-translatable quadratical quasigroups of order

$m \leqslant 1200$ defined on $\mathbb{Z}_m$.

k	m	a	b
2	5	2	4
3	5	4	2
4	17	7	11
5	13	11	7
6	37	16	22
7	25	22	4
8	13	3	11
	65	29	37
9	41	37	5
10	101	46	56
11	61	56	6
12	29	9	21
	145	67	79
13	17	11	7
	85	79	7
14	197	92	106
15	113	106	8
16	257	121	137

k	m	a	b
17	29	21	9
	145	137	9
18	25	4	22
	65	24	42
	325	154	172
19	181	172	10
20	401	191	211
21	221	211	11
22	97	38	60
	485	232	254
23	53	42	12
	265	254	12
24	577	277	301
25	313	301	13
26	677	326	352
27	73	60	14
	365	352	14
28	157	65	93
	785	379	407

k	m	a	b
29	421	407	15
30	53	12	42
	901	436	466
31	37	22	16
	481	466	16
32	41	5	37
	205	87	119
	1025	497	529
33	109	93	17
	545	529	17
34	89	28	62
	1157	562	596
35	613	596	18
36	1297	631	667
37	137	119	19
	685	667	198
38	85	24	62
	289	126	164
39	761	742	20

10. Classification of quadratical quasigroups

We have classified translatable quadratical quasigroups in several ways. Firstly, all k-translatable quadratical quasigroups induced by $\mathbb{Z}_m$ were calculated for $k \in \{2.3.\ldots,10\}$. Secondly, for a quadratical quasigroup of order m we calculated all $(m-t)$-translatable quadratical quasigroups for $t \in \{2,3,\ldots,10\}$. Then we calculated all k-translatable quadratical quasigroups ($k < 40$) on $\mathbb{Z}_m$ of order $m < 1200$. We now list all k-translatable quadratical quasigroups induced by $\mathbb{Z}_m$, for $m < 500$. A list of all translatable quadratical quasigroups of the form Qn, up to a certain order, remains uncalculated.

Below are listed all k-translatable quadratical quasigroups of the form $x \cdot y = ax + by (\mathrm{mod}\, m)$, where $a < b$, defined on the group $\mathbb{Z}_m$ for $m < 500$. Dual quasigroups $x \circ y = bx + ay (\mathrm{mod}\, m)$ are omitted.

For example, the group $\mathbb{Z}_{65}$ induces four quadratical quasigroups: $x \cdot y = 24x + 42y (\mathrm{mod}\, 65)$, $x \cdot y = 29x + 37y (\mathrm{mod}\, 65)$ and two duals to these two. The first is 18-translatable, the second 8-translatable. In the table below these dual quasigroups $x \cdot y = 42x + 24y (\mathrm{mod}\, 65)$ and $x \cdot y = 37x + 29y (\mathrm{mod}\, 65)$ are not listed.

m	a	b	k
5	2	4	2
13	3	11	8
17	7	11	4
25	4	22	18
29	9	21	12
37	16	22	6
41	5	37	32
53	12	42	30
61	6	56	50
65	24	42	18
	29	37	8
73	14	60	46
85	7	79	72
	24	62	38
89	28	62	34
97	38	60	22
101	46	56	10
109	17	93	76
113	8	106	98
125	29	97	68
137	19	119	100
145	9	137	128
	67	79	12
149	53	97	44
157	65	93	28
169	50	120	70

m	a	b	k
173	47	127	80
181	10	172	162
185	22	164	142
	59	127	68
193	41	153	112
197	92	106	14
205	37	169	132
	87	119	32
221	11	211	200
	24	198	174
229	54	176	122
233	45	189	144
241	89	153	64
257	121	137	16
265	12	254	242
	42	224	182
269	94	176	82
277	109	169	60
281	27	255	228
289	126	164	38
293	78	216	138
305	67	239	172
	117	189	72
313	13	301	288
317	102	216	114
325	29	297	268
	154	172	18

m	a	b	k
337	95	243	148
349	107	243	136
353	156	198	42
365	14	352	338
	87	279	192
373	135	239	104
377	50	328	278
	154	224	70
389	58	332	274
397	32	366	334
401	191	211	20
409	72	338	266
421	15	407	392
425	79	347	268
	147	279	132
433	90	344	254
445	62	384	322
	117	329	212
449	34	416	382
457	55	403	348
461	207	255	48
481	16	466	450
	133	349	216
485	157	329	172
	232	254	22
493	79	415	336
	96	398	302

10. Open questions and problems

Problem 1. *For which values of n are there quadratical quasigroups of form Qn?*

Note that $n \notin \{5, 6, 8, 14, 17, 19, 33, 26, 32, \ldots\}$. Moreover, from Theorem 4.11 in [3] it follows that there are no such quasigroups if there is a prime $p|4n+1$ such that $p \equiv 3 (\mathrm{mod}\, 4)$.

Problem 2. *Is every quadratical quasigroup Q of form Qn translatable ($n \neq 2$)?*

The answer is positive if Q is isomorphic to a quasigroup induced by $\mathbb{Z}_{4m+1}$.

Problem 3. *Are there self-dual, quadratical groupoids of order greater than 9?*

Such quasigroups cannot be induced by $\mathbb{Z}_m$.

Problem 4. *Is every quadratical groupoid of order greater than 9 and of form Qn ($n \geqslant 3$) generated by any two of its distinct elements?*

Problem 5. *If a quadratical quasigroup Q of order m is k-translatable, then is Q^* $(m-k)$-translatable?*

For quadratical quasigroups induced by $\mathbb{Z}_m$ the answer is positive.

References

[1] **W.A. Dudek**, *Quadratical quasigroups*, Quasigroups and Related Systems, **4** (1997), 9 – 13.

[2] **W.A. Dudek**, *Parastrophes of quasigroups*, Quasigroups and Related Systems, **23** (2015), 221 – 230.

[3] **W.A. Dudek and R.A.R. Monzo**, *On the fine structure of quadratical quasigroups*, Quasigroups and Related Systems, **24** (2016), 205 – 218.

[4] **W.A. Dudek and R.A.R. Monzo**, *Translatability and translatable semigroups*, Open Math., **16** (2018), 1266 – 1282.

[5] **W.A. Dudek and R.A.R. Monzo**, *The structure of idempotent translatable quasigroups*, Bull. Malays. Math. Sci. Soc., **43** (2020), 1603 – 1621.

[6] **B. Ganter and H. Werner**, *Equational classes of Steiner systems*, Algebra Universalis, **5** (1975), 125 – 140.

[7] **M. Polonijo**, *A note on Ward quasigroups*, An. Ştiinţ. Univ. Al. I. Cuza Iaşi. Sectţ. I a Mat. (N.S.), **32**(2) (1986), 5 – 10.

[8] **I. M. Vinogradov**, *Foundations of the theory of numbers*, (Russian), Nauka, Moscow, (1965).

[9] **V. Volenec**, *Quadratical groupoids*, Note di Matematica, **13**(1) (1993), 107 – 115.

[10] **V. Volenec**, *Squares in quadratical quasigroups*, Quasigroups and Related Systems **7** (2000), 37 – 44.

[11] **V. Volenec and R. Kolar-Šuper**, *Skewsquares in quadratical quasigroups*, Comment. Math. Univ. Carolin., **49** (2008), 397 – 410.

[12] **V. Volenec and R. Kolar-Šuper**, *Parallelograms in quadratical quasigroups*, Quasigroups and Related Systems, **18** (2010), 229 – 240.

Received September 20, 2020

W.A. Dudek
Faculty of Pure and Applied Mathematics, Wroclaw University of Science and Technology,
50-370 Wroclaw, Poland
E-mail: wieslaw.dudek@pwr.edu.pl

R.A.R. Monzo
Flat 10, Albert Mansions, Crouch Hill, London N8 9RE, United Kingdom
E-mail: bobmonzo@talktalk.net

Quasigroups and Related Systems **28** (2020), 229 – 236

A note on the construction of right conjugacy closed loops

Gerhard Hiss and Lucia Ortjohann

Abstract. We describe a group theoretical construction of non-associative right conjugacy closed loops with abelian inner mapping groups.

1. Introduction

A *loop* is a quasigroup with an identity element. If the multiplication of the loop is associative, it is a group. In the following, every loop, and in particular every group, will be assumed to be finite.

Let $(\mathcal{L}, *)$ be a loop with identity element $1_\mathcal{L}$. For every $x \in \mathcal{L}$, we denote by R_x the *right multiplication* by x in $\mathcal{L}$, i.e. $R_x : \mathcal{L} \to \mathcal{L}, y \mapsto y * x$, and we set $R_\mathcal{L} := \{R_x \mid x \in \mathcal{L}\}$. Then $\mathrm{RM}(\mathcal{L}) := \langle R_\mathcal{L} \rangle \leqslant \mathrm{Sym}(\mathcal{L})$ and its subgroup $\mathrm{Stab}_{\mathrm{RM}(\mathcal{L})}(1_\mathcal{L})$ are called the *right multiplication group*, and the *inner mapping group* of $\mathcal{L}$, respectively. The *envelope* of $\mathcal{L}$ consists of the triple $(\mathrm{RM}(\mathcal{L}), \mathrm{Stab}_{\mathrm{RM}(\mathcal{L})}(1_\mathcal{L}), R_\mathcal{L})$. To simplify notation, let us put $G := \mathrm{RM}(\mathcal{L})$, $H := \mathrm{Stab}_{\mathrm{RM}(\mathcal{L})}(1_\mathcal{L})$ and $T := R_\mathcal{L}$. Clearly, G acts faithfully and transitively on $\mathcal{L}$, which may hence be identified with the set of right cosets of H in G. Notice that $\mathcal{L}$ is a group if and only if $|G| = |\mathcal{L}|$, or, equivalently, $H = \{1\}$. By definition, T generates G, and one can check that T is a transversal for the set of right cosets of H^g in G for every $g \in G$. Envelopes of loops are generalized to *loop folders*.

The connection between loops and loop folders, summarized below, goes back to Baer [3], and is described in detail by Aschbacher in [2, Section 1]. In the following, G denotes a finite group and H a subgroup of G; we write $H\backslash G$ for the set of right cosets of H in G. The triple (G, H, T) is called a *loop folder* if $T \subseteq G$ is a transversal for $H^g\backslash G$ for every $g \in G$, and if $1 \in T$. We call (G, H, T) *faithful* if G acts faithfully on $H\backslash G$, i.e. if $\mathrm{core}_G(H) = \{1\}$.

By construction, the envelope (G, H, T) of a loop $\mathcal{L}$ is a faithful loop folder with $G = \langle T \rangle$, and there is a natural bijection between T and $\mathcal{L}$. Conversely, given a loop folder (G, H, T), one can construct a loop $(T, *)$ on the set T in such a way that (G, H, T) is isomorphic to the envelope of $(T, *)$, provided (G, H, T) is faithful and $G = \langle T \rangle$. This motivates the following definition. A transversal T for $H\backslash G$ is called a *generating transversal* if $G = \langle T \rangle$.

2010 Mathematics Subject Classification: Primary: 20N05, Secondary: 20D99, 20K01
Keywords: Finite loops, conjugacy closed, invariant transversals

A loop $\mathcal{L}$ is called *right conjugacy closed* or an RCC-*loop* if the set $R_{\mathcal{L}}$ is closed under conjugation, i.e. if $R_x^{-1}R_yR_x \in R_{\mathcal{L}}$ for all $x, y \in \mathcal{L}$. Analogously, a loop folder (G, H, T) is called *right conjugacy closed*, or an RCC-*loop folder* if T is G-invariant under conjugation, i.e. $g^{-1}tg \in T$ for all $g \in G, t \in T$. Clearly, a loop is right conjugacy closed if and only if its envelope is an RCC-loop folder.

In this paper we construct envelopes of RCC-loops with abelian inner mapping groups. The following trivial observations form the starting point of our construction.

Proposition 1. *Let G be a finite group, $Q \trianglelefteq G$ and $H \leqslant G$ with $H \cap Q = \{1\}$. Let $\hat{T} = \{t_1, \ldots, t_n\}$ be a transversal for HQ in G. Then $T := \hat{T}Q$ is a transversal for H in G and $\{t_1Q, \ldots, t_nQ\}$ is a transversal for HQ/Q in G/Q. Furthermore, we have the following two statements.*

(*a*) *The transversal $\{t_1Q, \ldots, t_nQ\}$ is G/Q-invariant if and only if T is G-invariant.*

(*b*) *The transversal $\{t_1Q, \ldots, t_nQ\}$ generates G/Q if and only if T generates G.*

Thus if $\mathrm{core}_G(H) = \{1\}$ and the transversal $\{t_1Q, \ldots, t_nQ\}$ is G/Q-invariant and generates G/Q, then (G, H, T) is an envelope of an RCC-*loop, which is non-associative if $\{1\} \lneq H \lneq G$.* □

Notice that $\mathrm{core}_G(H) \leqslant C_H(Q)$ under our assumption $H \cap Q = \{1\}$, so that $C_H(Q) = \{1\}$ implies $\mathrm{core}_G(H) = \{1\}$. If G/Q is abelian, then H is abelian and T is G-invariant by part (a) of Proposition 1. This holds in particular for Q equal to the commutator subgroup $[G, G]$ of G. We conjecture that the converse of this statement holds.

Conjecture 1. *Let G be a finite group, $H \leqslant G$ an abelian subgroup such that there exists a G-invariant transversal T for $H\backslash G$ with $1 \in T$, i.e. (G, H, T) is an* RCC-*loop folder. Then $[G, G] \cap H = \{1\}$.* □

In Section 3 we prove this conjecture in special cases. The conjecture also makes sense if G is an infinite group, but this more general question is out of the scope of this paper.

2. Generating transversals for abelian groups

In this section we investigate the existence of generating transversals in abelian groups. Let p be a prime. We first show that if G is an abelian p-group, and the index of H in G is larger than the minimal size of a generating set of G, there exists a generating transversal for $H\backslash G$ containing 1. We generalize this result for an arbitrary abelian group G, however with a stronger condition on the index of H in G.

The minimal size of a generating set of G is called the *rank* of G, i.e.

$$\mathrm{rk}(G) := \min\{|S| \mid S \subseteq G, G = \langle S\rangle\}.$$

A cyclic group of order n is denoted by C_n. If T is a generating transversal for $H\backslash G$ containing 1, then necessarily, $|G : H| > \mathrm{rk}(G)$. For the sake of clarity in the proofs to follow, we write the elements of a direct product $A \times B$ of groups as pairs (a, b) with $a \in A$, $b \in B$.

Proposition 2. *Let G be an abelian p-group. Suppose that $H \leqslant G$ is a subgroup of G such that $|G : H| > \mathrm{rk}(G)$. Then there exists a generating transversal T for $H\backslash G$ with $1 \in T$.*

Proof. We proceed by induction on the order of G, where the base case is trivial. For the induction step, we assume that $G \neq \{1\}$, that the statement holds for every abelian p-group of order less than $|G|$, and distinguish two cases.
Case 1: For every decomposition

$$G = C_{m_1} \times C_{m_2} \times \cdots \times C_{m_r}, \tag{1}$$

with $\{1\} \neq C_{m_i} \leqslant G$ for $1 \leqslant i \leqslant r$, we have $C_{m_i} \not\leqslant H$ for all $1 \leqslant i \leqslant r$.

Consider an arbitrary decomposition of G as in (1), and let a_i be a generator of C_{m_i} for every $1 \leqslant i \leqslant r$. Then $G = \langle a_1, \ldots, a_r\rangle$ and our assumption implies that $a_i \notin H$ for all $1 \leqslant i \leqslant r$. Suppose that for any $1 \leqslant i \neq j \leqslant r$, the generators a_i and a_j of G lie in distinct cosets of H in G. Then there is a transversal for $H\backslash G$ containing $\{1, a_1, \ldots, a_r\}$ and we are done. Otherwise, $Ha_i = Ha_j$ for some $1 \leqslant i \neq j \leqslant r$. Without loss of generality, we may assume that $|a_j| \geq |a_i|$. Then

$$G = \langle a_1\rangle \times \cdots \times \langle a_{j-1}\rangle \times \langle a_j a_i^{-1}\rangle \times \langle a_{j+1}\rangle \times \cdots \times \langle a_r\rangle,$$

and we have $\langle a_j a_i^{-1}\rangle \leqslant H$. We have thus reduced the assertion to the following situation.
Case 2: There exist $\{1\} \neq C_{m_i} \leqslant G$ for $1 \leqslant i \leqslant r$ such that

$$G = C_{m_1} \times C_{m_2} \times \cdots \times C_{m_r},$$

and $C_{m_j} \leqslant H$ for some $1 \leqslant j \leqslant r$.

Note that the generators of these cyclic groups form a minimal generating set of G of size r. Thus, it follows from Burnside's basis theorem [5, III, Satz 3.15] that $r = \mathrm{rk}(G)$.

Set $U := C_{m_j}$,

$$\widetilde{G} := C_{m_1} \times \cdots \times C_{m_{j-1}} \times C_{m_{j+1}} \times \cdots \times C_{m_r},$$

and $\widetilde{H} := \widetilde{G} \cap H$. Clearly, $\widetilde{H}$ is a complement to U in H and thus, without loss of generality, we may assume that

$$G = \widetilde{G} \times U \quad \text{and} \quad H = \widetilde{H} \times U.$$

By construction,

$$\mathrm{rk}(\widetilde{G}) = r - 1 < r = \mathrm{rk}(G).$$

Since $\left|\widetilde{G}\right| < |G|$ and

$$\left|\widetilde{G} : \widetilde{H}\right| = |G : H| > \mathrm{rk}(G) > \mathrm{rk}(\widetilde{G}), \tag{2}$$

we can apply the induction hypothesis to $\widetilde{G}$ and hence there exists a generating transversal $\widetilde{T}$ for $\widetilde{H}\backslash\widetilde{G}$ with $1 \in \widetilde{T}$. Moreover, from Equation (2) we obtain

$$\left|\widetilde{T} - \{1\}\right| = \left|\widetilde{G} : \widetilde{H}\right| - 1 > \mathrm{rk}(\widetilde{G}). \tag{3}$$

Suppose that $\widetilde{T} - \{1\}$ is a minimal generating set for $\widetilde{G}$. Then Burnside's basis theorem [5, III, Satz 3.15] implies that $\left|\widetilde{T} - \{1\}\right| = \mathrm{rk}(\widetilde{G})$, contradicting Equation (3). Thus there exists $1 \neq t \in \widetilde{T}$ such that $t = t_1 \cdots t_k$ for certain $t_1, \ldots, t_k \in \langle \widetilde{T} \backslash \{1, t\} \rangle$.

Now $\widetilde{T} \times \{1\}$ is a transversal for $H\backslash G$ and we set

$$T := (\widetilde{T} \times \{1\} \setminus \{(t, 1)\}) \cup \{(t, u)\},$$

where u is a generator of U. Clearly, $(1, 1) \in T$, and T is a transversal for $H\backslash G$ since $(t, 1)$ and (t, u) lie in the same coset of H in G. It remains to show that T generates G. Recall that $t = t_1 \cdots t_k$ with $t_1, \ldots, t_k \in \langle \widetilde{T} \setminus \{1, t\} \rangle$. As $(t_1, 1), \ldots, (t_k, 1) \in \langle T \rangle$, we also have $(t^{-1}, 1) \in \langle T \rangle$. Hence $(1, u) = (t^{-1}, 1)(t, u) \in \langle T \rangle$ and then $(t, 1) = (t, u)(1, u^{-1}) \in \langle T \rangle$. We conclude that $\langle T \rangle \geqslant \langle \widetilde{T} \rangle \times \langle u \rangle = \widetilde{G} \times U = G$ and we are done. □

Let G be an abelian group and let $p_1, \ldots, p_n$ be the distinct prime divisors of G. Assume that $G = G_1 \times \cdots \times G_n$ with $G_i := O_{p_i}(G)$ for all $1 \leqslant i \leqslant n$. Then an easy induction on n shows that

$$\mathrm{rk}(G) = \max\{\mathrm{rk}(G_i) \mid 1 \leqslant i \leqslant n\}. \tag{4}$$

We now transfer the result of Proposition 2 to an arbitrary abelian group.

Theorem 1. *Let G be an abelian group, let $p_1, \ldots, p_n$ be the distinct prime divisors of G and let $H \leqslant G$. Then*

$$G = G_1 \times \cdots \times G_n \quad \text{and} \quad H = H_1 \times \cdots \times H_n,$$

with $G_i := O_{p_i}(G)$ and $H_i := O_{p_i}(H)$. If

$$\max\{|G_i : H_i| \mid 1 \leqslant i \leqslant n\} > \mathrm{rk}(G),$$

then there exists a generating transversal for $H\backslash G$ containing 1.

Proof. Without loss of generality, we assume that

$$|G_1 : H_1| = \max\{|G_i : H_i| \mid 1 \leqslant i \leqslant n\}$$

and we set $\widetilde{G} := G_2 \times \cdots \times G_n$ and $\widetilde{H} := H_2 \times \cdots \times H_n$. Then $G = G_1 \times \widetilde{G}$ and $H = H_1 \times \widetilde{H}$. Equation (4) yields

$$\begin{aligned} m := |G_1 : H_1| &= \max\{|G_i : H_i| \mid 1 \leqslant i \leqslant n\} > \mathrm{rk}(G) \\ &= \max\{\ \mathrm{rk}(G_i)\ \mid 1 \leqslant i \leqslant n\} \geqslant \mathrm{rk}(G_1). \end{aligned}$$

Since G_1 is an abelian p_1-group with $|G_1 : H_1| > \mathrm{rk}(G_1)$, it follows from Proposition 2 that there exists a transversal $T_1 = \{t_1, \ldots, t_m\}$ for $H_1\backslash G_1$ with $t_1 = 1$ and $G_1 = \langle T_1 \rangle$. We are done if $n = 1$. Assume from now on that $n > 1$.

Put $K := H_1 \times \widetilde{G}$. Then $H \leqslant K \leqslant G$ and $|G : K| = |G_1 : H_1| = m$. We next construct a generating transversal for $K\backslash G$ containing 1. Our hypothesis and Equation (4) imply that

$$\begin{aligned} k := \mathrm{rk}(\widetilde{G}) &= \max\{\mathrm{rk}(G_i) \mid 2 \leqslant i \leqslant n\} \leqslant \mathrm{rk}(G) \\ &< \max\{|G_i : H_i| \mid 1 \leqslant i \leqslant n\} = |G_1 : H_1| = m. \end{aligned}$$

Let S be a generating set of $\widetilde{G}$ with $|S| = k$. Then S is a minimal generating set and thus $1 \notin S$. Write $S \cup \{1\} := \{s_1, \ldots, s_{k+1}\}$ with $s_1 = 1$. Now $|S \cup \{1\}| = k+1 \leqslant m$, and we set

$$R := \bigcup_{i=1}^{k+1} (t_i, s_i) \cup \bigcup_{j=k+2}^{m} (t_j, s_1).$$

As $t_1 = 1$ and $s_1 = 1$, we have $(1, 1) \in R$ and $|R| = m = |G : K|$. We proceed to show that R is a generating transversal for $K\backslash G$. Suppose that $(t_i, s_j), (t_k, s_l) \in R$ such that $(t_i, s_j)(t_k, t_l)^{-1} \in H_1 \times \widetilde{G}$. Then $t_i t_k^{-1} \in H_1$ and as T_1 is a transversal for $H_1\backslash G_1$, it follows that $i = k$. This implies that $j = l$. We conclude that R is a transversal for $K\backslash G$. The fact $\gcd(|G_1|, |\widetilde{G}|) = 1$ yields that for every $(t, s) \in R$ there exist $a, b \in \mathbb{Z}$ such that $(t, s)^a = (1, s)$ and $(t, s)^b = (t, 1)$. Hence

$$\langle R \rangle \geqslant \langle T_1 \rangle \times \langle S \rangle = G_1 \times \widetilde{G} = G$$

and thus, R is a generating transversal for $K\backslash G$ with $1 \in R$.

Let V be a transversal for $H\backslash K$ with $1 \in V$. Then $T := VR$ is a transversal for $H\backslash G$. Since $1 \in V$, we have $R \subseteq T$ and it follows that $\langle T \rangle \geqslant \langle R \rangle = G$. This implies that T is a generating transversal for $H\backslash G$ with $1 \in T$. □

With this result and Proposition 1 we can construct envelopes of RCC-loops.

Corollary 1. *Let G be a group and let H be a subgroup of G. Let Q be a normal subgroup of G such that G/Q is abelian, $H \cap Q = \{1\}$, $C_H(Q) = \{1\}$ and*

$$\max\{|O_p(G/Q) : O_p(HQ/Q)| \mid p \text{ prime divisor of } G/Q\} > \mathrm{rk}(G/Q).$$

Then there exists a G-invariant generating transversal T for $H\backslash G$ with $1 \in T$, and G acts faithfully on $H\backslash G$; thus (G, H, T) is an envelope of a non-associative RCC*-loop.* □

Recall that T in Corollary 1 arises from multiplying a generating transversal for $HQ\backslash G$ with Q; see Proposition 1. If G is a Frobenius group with kernel Q (in which case $Q = [G, G]$, the commutator subgroup of G), every G-invariant transversal for $H\backslash G$ has this form (see [7, Theorem 3.6]). In general there may be G-invariant transversals, which are not obtained in this way. Since $[G, G]$ is the smallest normal subgroup of G with abelian quotient, we can replace Q by $[G, G]$.

Let us investigate the range of Corollary 1 by comparing with the examples presented in [1, Appendix B]. Let $n \in \{6, 8, 9, 10, 12, 14, 15, 21\}$ and let G be one of the transitive groups of degree n listed in this appendix. In each case, let H denote the stabilizer of 1 in G. Assume that H is abelian, and put $Q := [G, G]$. Using GAP, once checks that $H \cap Q = \{1\}$ in each case. Trivially, $\mathrm{core}_G(H) = \{1\}$, although, in general, $C_H(Q)$ is non-trivial. (The latter just means that the sufficent condition for $\mathrm{core}_G(H)$ to be trivial mentioned after Proposition 1 is not necessary.) Now, unless the GAP-identity number of G is one of $(8, 17)$, $(12, 15)$, $(12, 28)$ or $(12, 42)$, the displayed condition in Corollary 1 is satisfied, so that one of the RCC-loops arising from G and H is of the form constructed in Proposition 1.

Finally, notice that the construction of RCC-loops arising from Proposition 1 is, of course, not restricted to the case G/Q abelian. For example, consider the transitive group L of degree 6 with GAP-identity number $(6, 5)$, and let H denote the stabilizer of 1 in L. Then H is cyclic of order 3, and $L/Z(L) \cong \mathrm{SL}_2(2)$; thus L acts on the Klein four group Q in such a way that $C_H(Q) = \{1\}$. Letting G denote the semidirect product $G = L \ltimes Q$ and identifying H with a subgroup of G, Proposition 1, applied to the invariant transversals for $H\backslash L$, yields invariant transversals for $H\backslash G$, and thus RCC-loops of order 24.

3. A conjecture for RCC-loop folders

In this final section we discuss Conjecture 1. Using GAP [4], this conjecture has been verified for all non-abelian groups of order smaller than 40 by the second author in her master thesis [7], and for the multiplication groups of RCC-loops of order up to 30, by Artic in her dissertation [1].

It follows from a result of Zappa, that Conjecture 1 holds in case H is a Hall subgroup of G. Indeed, Zappa shows that if H is a nilpotent Hall subgroup of G such that there exists a transversal for $H\backslash G$ which is invariant under conjugation by H, then H has a normal complement; see [8, Proposizione XIV 12.1]. Now if H

is abelian, the commutator subgroup of G is contained in this normal complement. In [6], Kochendörffer generalizes Zappa's result. We present the essence of Zappa's and Kochendörffer's argument in the following theorem.

Theorem 2. *Let G be a finite group and let H be an abelian Hall subgroup of G. Suppose that there exists transversal T for $H\backslash G$ which is invariant under conjugation by H. Then $[G,G]\cap H=\{1\}$.*

Proof. This is very much inspired by the proof of [6, Theorem]. The transfer map

$$\tau : G \to H, x \mapsto \prod_{t\in T} \lambda_x^T(t),$$

where $\lambda_x^T(t)$ is the unique element in H such that $tx=\lambda_x^T(t)t'$ for some $t'\in T$, is a group homomorphism; see [5, IV, Hauptsatz 1.4].

Let $h\in H$ and let $h':=\lambda_h^T(t)$ for some $t\in T$. Then $th=h't'$ for some $t'\in T$. It follows that $hh'^{-1}=t^{-1}h't'h'^{-1}\in H$ and since T is H-invariant, we have $h't'h'^{-1}\in T$. Thus, $t=h't'h'^{-1}$. This yields that $h=h'=\lambda_h^T(t)$ and hence

$$\tau(h)=\prod_{t\in T}\lambda_h^T(t)=\prod_{t\in T}h=h^{|G:H|}.$$

As H is an abelian Hall subgroup of G, the map $f:H\to H, h\mapsto h^{|G:H|}$ is an isomorphism. Thus $\ker\tau\cap H=\{1\}$. Furthermore, $G/\ker\tau$ is abelian, because the image of τ is abelian as subgroup of H. Hence, $[G,G]\leqslant\ker\tau$. We conclude that $[G,G]\cap H\leqslant\ker\tau\cap H=\{1\}$. □

In the next example we show that for the conclusion of Conjecture 1 to be true, it is not enough to require the existence of an H-invariant transversal for $H\backslash G$.

Example 1. Let $G:=Q_8$ and let $H:=Z(G)$. Then H is abelian and every transversal of $H\backslash G$ is H-invariant. However, $H=Z(G)=[G,G]$. Notice that there does not exist any G-invariant transversal for $H\backslash G$.

However, if p is a prime, G is a group of order p^3 and there exists a G-invariant transversal for $H\backslash G$, then Conjecture 1 holds.

Lemma 1. *Let G be a p-group with $[G,G]=Z(G)$ and $|Z(G)|=p$. Suppose that $H\leqslant G$ is abelian and that there exists a G-invariant transversal T of $H\backslash G$ containing* 1. *Then $[G,G]\cap H=\{1\}$.*

Proof. Since T is G-invariant, T is a union of conjugacy classes of G. As $1\in T$, we conclude that T contains at least p conjugacy classes with exactly one element, i.e. T contains at least p elements of $Z(G)$. Hence $[G,G]=Z(G)\subseteq T$ and thus $[G,G]\cap H\subseteq T\cap H=\{1\}$. □

This lemma shows that Conjecture 1 holds for groups of order p^3.

Acknowledgements

We are grateful to Gabriele Nebe for a crucial hint in the proof of Theorem 1. We thank Klaus Lux for carefully reading a first version of this article and for his comments which considerably improved the exposition. Finally, we thank the referee for interesting suggestions.

References

[1] **K. Artic**, *On right conjugacy closed loops and right conjugacy closed loop folders*, Dissertation, RWTH Aachen University, 2017.

[2] **M. Aschbacher**, *On Bol loops of exponent 2*, J. Algebra, **288** (2005), 99 – 136.

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

[4] **The GAP Group**, *GAP – Groups, Algorithms, and Programming, Version 4.10.2*; 2019, `https://www.gap-system.org`.

[5] **B. Huppert**, *Endliche Gruppen I*, Springer-Verlag, 1967.

[6] **R. Kochendörffer**, *On supplements in finite groups*, J. Austral. Math. Soc., **3** (1963), 63 – 67.

[7] **L. Ortjohann**, *Invariant transversals in finite groups*, Master Thesis, RWTH Aachen University, 2019, `https://arxiv.org/abs/2005.01380`.

[8] **G. Zappa**, *Fondamenti di teoria dei gruppi, Vol. II*, 18 Edizioni Cremonese, Rome, 1970.

Received May 05, 2020

Lehrstuhl für Algebra und Zahlentheorie
RWTH Aachen University
Pontdriesch 14/16
52062 Aachen
Germany
E-mails: gerhard.hiss@math.rwth-aachen.de, lucia.ortjohann@rwth-aachen.de

Quasigroups and Related Systems **28** (2020), 237 – 242

Maximal cyclic subgroups of a finite abelian p-group of rank two

Pradeep Kumar

Abstract. Let G be a finite group. A cyclic subgroup of G that is not a proper subgroup of any other proper cyclic subgroup of G is called a maximal cyclic subgroup and the set of all maximal cyclic subgroups of G is denoted by $\mathcal{M}_G$. In this paper, we find the cardinality of the set $\mathcal{M}_G$, where G is a finite abelian p-group of rank two. As an application, we obtain the independence number of the power graph of the group G.

1. Introduction

Counting the number of subgroups of finite groups is one of the old problems in finite group theory and it is still frequently studied. In [2], Bhowmik gave a method to determine the total number of subgroups of a finite abelian p-group. A simple formula, in the case of a finite abelian p-group of rank two was obtained by Călugăreanu [3], Petrillo [10] and Tóth [14] by using Goursat's lemma. In [13], Tóth obtained the number of cyclic subgroups of a finite abelian group.

Let G be a finite group. A cyclic subgroup of G that is not a proper subgroup of any other proper cyclic subgroup of G is called a *maximal cyclic subgroup* and the set of all maximal cyclic subgroups of G is denoted by $\mathcal{M}_G$. Let Γ be a graph. A set of pairwise non-adjacent vertices of Γ is called an *independent set*. The maximum size of an independent set in a graph Γ is called the *independence number* of Γ and denoted by $\beta(\Gamma)$.

Let G be a group. The *undirected power graph* $\mathcal{P}(G)$ has the vertex set G and two distinct vertices x and y are adjacent if $x = y^m$ or $y = x^m$ for some positive integer m. The concepts of a power graph and an undirected power graph were first considered by Kelarev and Quinn [8] and Chakrabarty et al. [6], respectively. Since this paper deals only with undirected graphs, for convenience throughout we use the term "power graph" to refer to an undirected power graph. Recently, a lot of interesting results on the power graphs have been obtained, see for example [4, 5]. A detailed list of open problems and results can be found in [1]. Chakrabarty et al. [6], found that the power graph $\mathcal{P}(G)$ is complete if and only if G is a cyclic group of order p^n, where p is a prime number and n is a non-negative integer. Sehgal and Singh [12] obtained the degree of a vertex in the power graph of a finite abelian

2010 Mathematics Subject Classification: 20D15; 05C25
Keywords: Power graph; Independence number; p-Groups; Maximal cyclic subgroups

group. Chelevam and Sattanathan [7] determined the finite abelian groups whose power graphs are planar. They have also characterized the finite abelian groups G with $\beta(\mathcal{P}(G)) = 2$. In [9], X. Ma et al. obtained that the independence number of the power graph of a finite p-group G is equal to the cardinality of the set $\mathcal{M}_G$. For generalized extraspecial p-groups G with $p > 2$, $\beta(\mathcal{P}(G))$ had been determined in [**?**] by calculating the cardinality of the set $\mathcal{M}_G$.

In this paper, we find the cardinality of the set $\mathcal{M}_G$, where G is an abelian p-group of rank two. Equivalently, we find the independence number of $\mathcal{P}(G)$.

Throughout the paper p denotes a prime number. Let $|X|$ denote the cardinality of the set X and $o(x)$ denote the order of the element x in the group G. Let $\langle g\rangle$ denote the cyclic subgroup of the group G generated by $g \in G$ and the identity element of the group G is denoted by e. For a positive integer n, $\phi(n)$ denotes the Euler's totient function. Let $\mathcal{C}(G)$ denote the set of all distinct cyclic subgroups of the group G. Note that $(\mathcal{C}(G), \subseteq)$ is a poset.

2. Preliminaries

We will start with the basic facts that will be needed later.

Lemma 2.1. *Let $G \cong \mathbb{Z}_{p^{\beta_1}} \times \mathbb{Z}_{p^{\beta_2}} \cong \langle x\rangle \times \langle y\rangle$ where $o(x) = p^{\beta_1}$ and $o(y) = p^{\beta_2}$ and $\beta_1 \geqslant \beta_2 \geqslant 1$. Let $g = x^{p^{k_1}\alpha_1} y^{p^{k_2}\alpha_2} \neq e \in G$. If $0 < k_i$ and $p \nmid \alpha_i\ \forall\ i \in \{1, 2\}$, then there are p cyclic subgroups of order $o(g)p$ containing $\langle g\rangle$. Further, if for some $i = i_o$, $k_{i_o} = 0$ and $\alpha_{i_o} \neq 0$, then $\langle g\rangle$ doesn't contained in any cyclic subgroup of order $o(g)p$.*

Proof. Let $g \in G$ such that $g = x^{p^{k_1}\alpha_1} y^{p^{k_2}\alpha_2}$, where $p \nmid \alpha_i$ for $i \in \{1, 2\}$. First, we count the number of elements $h \in G$ such that $h^p = g$. Consider $h = x^{r_1} y^{r_2}$. Now, $h^p = g$ implies $x^{pr_1} y^{pr_2} = x^{p^{k_1}\alpha_1} y^{p^{k_2}\alpha_2}$. So $p^{k_i}\alpha_i = pr_i \mod p^{\beta_i}\ \forall\ i \in \{1, 2\}$. For fixed i, latter equation has integer solution r_i if and only if $p \mid p^{k_i}\alpha_i$. Thus, if for some $i = i_o$, $k_{i_o} = 0$ and $\alpha_{i_o} \neq 0$, then there doesn't exist any $h \in G$ such that $h^p = g$.

Now, assume $k_i > 0,\ \forall\ i$. So, if $p^{k_i}\alpha_i \equiv pr_i \mod p^{\beta_i}$, then $p^{k_i-1}\alpha_i \equiv r_i \mod p^{\beta_i-1}$. Thus, the latter equation has p distinct solutions for each fixed i and that are $r_i = p^{k_i-1}\alpha_i + kp^{\alpha_1-1}$, where $0 \leqslant k \leqslant p-1$. Thus, for given $g = x^{p^{k_1}\alpha_1} y^{p^{k_2}\alpha_2}$, where $p \nmid \alpha_i$ and $k_i > 0$, there are p^2 elements $h \in G$ such that $h^p = g$ and $o(h) = o(g)p$.

Now, let $\langle h\rangle$ be a cyclic subgroup of order $o(g)p$ such that $\langle g\rangle \subset \langle h\rangle$ and $h^p = g$. Suppose $w \in \langle h\rangle$ such that $w^p = g$, then $w = h^r$ and $h^{rp} = h^p = g$. This implies that $rp \equiv p \mod o(h)$. Thus, $r = 1 + k\frac{o(h)}{p}$, where $1 \leqslant k \leqslant p$. Thus, each cyclic subgroup $\langle h\rangle$ of order $o(g)p$ contains p distinct elements $w \in \langle h\rangle$ such that $w^p = g$. Hence that, there are $\frac{p^2}{p} = p$ cyclic subgroups of order $o(g)p$ containing g for $k_i > 0\ \forall\ i$. This completes the proof. □

Corollary 2.2. *Suppose* $G \cong \mathbb{Z}_{p^{\beta_1}} \times \mathbb{Z}_{p^{\beta_2}}$, $\beta_1 > \beta_2$. *Then a cyclic subgroup* $H = \langle x^{p^{\beta_1 - t}} y^b \rangle$ *(where* $\beta_2 \leqslant t < \beta_1, 1 \leqslant b \leqslant p^{\beta_2}$ *) of order* p^t *is contained in a cyclic subgroup of order* p^{t+1} *if and only if* $p \mid b$.

Proof. This follows from Lemma 2.1. □

Recall that the set of all maximal cyclic subgroups of the finite group G is denoted by $\mathcal{M}_G$ and the independence number of the graph Γ is denoted by $\beta(\Gamma)$.

Theorem 2.3. [9, Corollary 2.14] *Let* G *be a* p*-group. Then* $\beta(\mathcal{P}(G)) = |\mathcal{M}_G|$.

3. Maximal cyclic subgroups

In this section, we find the number of maximal cyclic subgroups of $\mathbb{Z}_{p^r} \times \mathbb{Z}_{p^s}, r \geqslant s \geqslant 1$. For the rest of the paper, we fixed that $G \cong \mathbb{Z}_{p^r} \times \mathbb{Z}_{p^s} \cong \langle x \rangle \times \langle y \rangle$, where $o(x) = p^r$ and $o(y) = p^s$ and $r \geqslant s \geqslant 1$.

The number of cyclic subgroups of order p in G is $p+1$ and these cyclic groups are given as $\{\langle y^{p^{s-1}} \rangle\} \cup \{\langle x^{p^{r-1}} y^{ip^{s-1}} \rangle \mid 1 \leqslant i \leqslant p\}$. From [11], we know that a cyclic subgroup of order p^t $(t > 1)$ contains exactly one cyclic subgroup of order p. Let X_i be the set of all cyclic subgroups of G containing cyclic subgroup $\langle x^{p^{r-1}} y^{ip^{s-1}} \rangle$ for $1 \leqslant i \leqslant p$ and X_0 be the set of all cyclic subgroups of G containing $\langle y^{p^{s-1}} \rangle$.

Lemma 3.1. *The number of cyclic subgroups of order* p^t *in* X_i, $0 \leqslant i \leqslant p$ *is* p^{t-1} *where* $1 \leqslant t \leqslant s$.

Proof. By Lemma 2.1, each cyclic subgroup of order p^t is contained in p cyclic subgroups of order p^{t+1}, $1 \leqslant t < s$. Thus, it is immediate that each X_i contains p^{t-1} cyclic subgroups of order p^t, $1 \leqslant t \leqslant s$. □

Let $\mathcal{M}(X_i, \subseteq)$ denote the set of all maximal elements of the poset $(X_i, \subseteq)$.

Lemma 3.2. $|\mathcal{M}_G| = \sum_{i=0}^{p} |\mathcal{M}(X_i, \subseteq)|$.

Proof. Recall that $\mathcal{C}(G)$ is the set of all distinct cyclic subgroups of the group G. Let $\mathcal{C}^*(G)$ be the set $\mathcal{C}(G) \backslash \langle e \rangle$. Define a relation R on $\mathcal{C}^*(G)$ such that $\langle x \rangle, \langle y \rangle \in \mathcal{C}^*(G)$ are said to be related if $\langle x \rangle$ and $\langle y \rangle$ contain a unique cyclic subgroup of order p. It is immediate the R is an equivalence relation. Since, G has $p+1$ cyclic subgroups of order p, $\mathcal{C}^*(G)$ has $p+1$ equivalence classes. Clearly, X_i, $0 \leqslant i \leqslant p$ are these equivalence classes. It is easy to observe that if $\langle x \rangle \in X_i$ and $\langle y \rangle \in X_j$ for $i \neq j$, $0 \leqslant i, j \leqslant p$, then $\langle x \rangle \nsubseteq \langle y \rangle$ and $\langle y \rangle \nsubseteq \langle x \rangle$. Thus, a maximal element of the poset $(X_i, \subseteq)$ is a maximal cyclic subgroup of G. This completes the proof. □

Theorem 3.3. *Let* $G \cong \mathbb{Z}_{p^r} \times \mathbb{Z}_{p^s}$, $r > s$. *Then*

$$\beta(\mathcal{P}(G)) = |\mathcal{M}_G| = \begin{cases} 2p^s + \phi(p^s)(r-s-1), & r \geqslant s \\ p^s + p^{s-1}, & r = s. \end{cases}$$

Proof. Suppose $r > s$. Now assume that $s < t \leqslant r$. Take $g = x^a y^b \in G$. If the order of g is p^t, then $g = x^{p^{r-t}k} y^b$, where $\gcd(k, p) = 1$, $1 \leqslant k \leqslant p^t$ and $1 \leqslant b \leqslant p^s$. Thus, the number of elements of order p^t is $\phi(p^t)p^s$. Since, each cyclic subgroup of order p^t contains $\phi(p^t)$ elements of order p^t, so the number of cyclic subgroups of order p^t is $\frac{\phi(p^t)p^s}{\phi(p^t)} = p^s$ and they are $\langle x^{p^{r-t}} y^b \rangle$, $1 \leqslant b \leqslant s$. Further, $(x^{p^{r-t}} y^b)^{p^{t-1}} = x^{p^{r-1}}$. Thus, all cyclic subgroups of order p^t, $t > s$ belong to X_p. By Corollary 2.2, cyclic subgroup $H = \langle x^{p^{r-t}} y^b \rangle$ of order p^t is contained in cyclic subgroup of order p^{t+1} if and only if $p \mid b$ and if $p \mid b$, then H is contained in p cyclic subgroups of order p^{t+1} $(t < r)$. Hence, out of p^s only p^{s-1} cyclic subgroups of order p^t are contained in cyclic subgroups of order p^{t+1}.

Again, the number of cyclic subgroups of order p^s in the set X_p is p^{s-1} (Lemma 3.1) and the number of cyclic subgroups of order p^{s+1} is p^s and each cyclic subgroup of order p^s is contained in at most p cyclic subgroups of order p^{s+1} (Lemma 2.1). Thus, each cyclic subgroup of order p^s is contained in p cyclic subgroups of order p^{s+1} in the set X_p. By Lemmas 2.1 and 3.1, it is clear that X_p has p^{t-1} cyclic subgroups of order p^t and each cyclic subgroup of order p^t is contained in p cyclic subgroups of order p^{t+1} in X_p for $1 \leqslant t < s$.

The number of cyclic subgroups of order p^t in X_i for $0 \leqslant i \leqslant p-1$ is p^{t-1}, for $1 \leqslant t \leqslant s$ (Lemma 3.1) and none of cyclic subgroups of order p^t for $t > s$ belong to $X_i (0 \leqslant i \leqslant p-1)$. Further, each cyclic subgroup of order p^t is contained in p cyclic subgroups of order p^{t+1} for $1 \leqslant t < s$ in X_i.

Collecting all arguments, the Hasse diagram of the poset $(X_p, \subseteq)$ is given in Figure 1 and the Hasse diagram of the poset $(X_i, \subseteq)$ $(0 \leqslant i \leqslant p-1)$ is given in Figure 2.

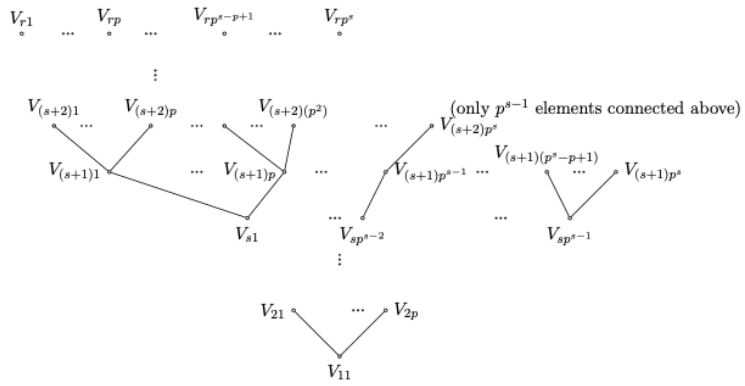

Figure 1: The Hasse diagram of the poset $(X_p, \subseteq)$

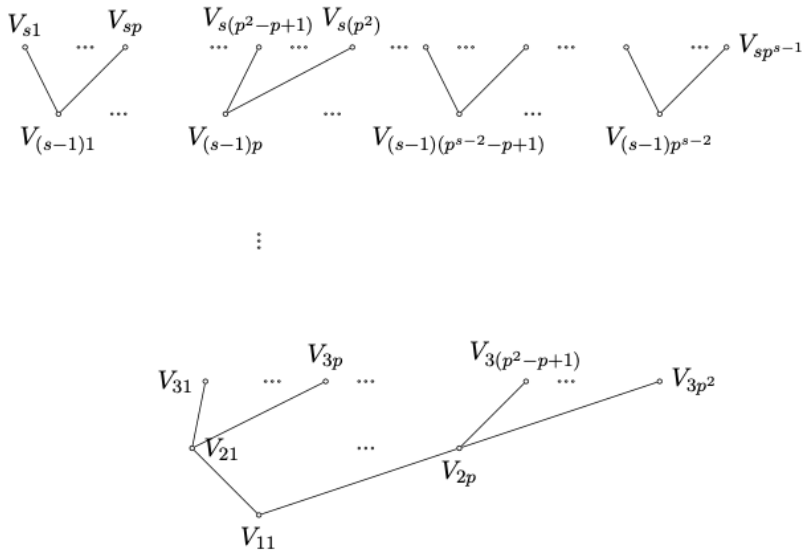

Figure 2: The Hasse diagram of the poset $(X_i, \subseteq)$, for $0 \leqslant i \leqslant p-1$

In Figures 1 and 2, V_{tj} denotes the element of X_i, $0 \leqslant i \leqslant p$ of cardinality p^t. $(X_p, \subseteq)$ has $p^s + \phi(p^s)(r-s-1)$ maximal elements (see Figure 1) and $(X_i, \subseteq)$ for $0 \leqslant i \leqslant p-1$ has p^{s-1} maximal elements. Thus, by Lemma 3.2, $|\mathcal{M}_G| = 2p^s + \phi(p^s)(r-s-1)$ for $r > s$. Now, for $r = s$. Only the cyclic subgroups of order p^s are maximal elements in X_i, $0 \leqslant i \leqslant p$ and each X_i has p^{s-1} cyclic subgroups of order p^s. Thus, by Lemma 3.2, $|\mathcal{M}_G| = p^s + p^{s+1}$, for $r = s$. Hence by Theorem 2.3, we complete the proof. □

Acknowledgments. The author wish to thank the referee for giving useful suggestions for improvement of the article.

References

[1] **J. Abawajy, A. Kelarev and M. Chowdhary**, *Power graphs: A survey*, Electron. J. Graph Theory Appl., **1** (2013), 125 – 147.

[2] **G. Bhowmik**, *Evaluation of divisor functions of matrices*, Acta Arith., **74** (1996), 155 – 159.

[3] **G. Călugăreanu**, *The total number of subgroups of a finite abelian group*, Sci. Math. Jpn., **60** (2004), 157 – 167.

[4] **P.J. Cameron**, *The power graph of a finite group II*, J. Group Theory, **13** (2010), 779 – 783.

[5] **P.J. Cameron and S. Ghosh**, *The power graph of a finite group*, Discrete Math., **311** (2011), 1220 – 1222.

[6] **I. Chakrabarty, S. Ghosh and M.K. Sen**, *Undirected power graphs of semigroups*, Semigroup Forum, 78 (2009), 410 – 426.

[7] **T.T. Chelevam and M. Sattanathan**, *Power graph of finite abelian groups*, Algebra Discrete Math., **16** (2013), 33 – 41.

[8] **A.V. Kelarev and S.J. Quinn**, *A combinatorial property and power graphs of groups*, Contributions to General Algebra, **12** (Vienna, 1999), Heyn, Klagenfurt, 2000, 229 – 235.

[9] **X. Ma, R. Fu and X. Lu**, *On the independence number of the power graph of a finite group*, Indag. Math., **29** (2) (2018), 794 – 806.

[10] **J. Petrillo**, *Counting subgroups in a direct product of a finite cyclic groups*, The College Math. J., **42** (2011), 215 – 222.

[11] **A. Sehgal, S. Sehgal and P.K. Sharma**, *The number of subgroups of a finite abelian p-group of rank two*, J. Algebra and Number Theory Academia, **5**(1) (2015), 23 – 31.

[12] **A. Sehgal and S.N. Singh**, *The degree of a vertex in the power graph of a finite abelian group*, https://arxiv.org/abs/1901.08187.

[13] **L. Tóth**, *On the number of cyclic subgroups of a finite abelian group*, Bull. Math. Soc. Sci. Math. Roumanie, **55** (2012), 423 – 428.

[14] **L. Tóth**, *Subgroups of finite abelian groups having rank two via Goursat's Lemma*, Tatra Mt. Math. Publ., **59** (2014), 93 – 103.

Received January 03, 2020

Department of Mathematics
Central University of South Bihar, Gaya-824236, India
E-mail: 14p.shaoran@gmail.com

Quasigroups and Related Systems **28** (2020), 243 – 250

On the component graphs of finitely generated free semimodules

Sushobhan Maity and Anjan Kumar Bhuniya

Abstract. A semiring S is said to have invariant basis number property if any two bases of a finitely generated free semimodule over S have the same cardinality. Here we characterize reduced zero and reduced non-zero component graphs of every finitely generated free semimodule $\mathcal{V}$ over such semirings. It is shown that if $|S| \geqslant \aleph_0$, these two graphs of a semimodule $\mathcal{V}$ over S are isomorphic.

1. Introduction

In the recent years, there has been a flow of various ideas in the study of algebraic structures using graphs defined on themselves. Various algebraic structures like semigroups [5], groups [2], rings [1] and vector spaces [6, 8] have been characterized in this way. In [6], Das introduced non-zero component graph on a finite dimensional vector space.

Recently, semimodules over a semiring have created attention to the researchers for their different interesting uncommon features. Many of the results of vector spaces do not match with the results of semimodules. For example, in a vector space every basis is a free basis and converesely, which does not hold in a semimodule in general [10].

Here we consider both zero and non-zero component graphs of a finitely generated free semimodule. Also we introduce reduced non-zero component graph and reduced zero component graph on a finitely generated free semimodule and prove that they are isomorphic. This isomorphism ensures that studying either of them is sufficient to know about both. Here we study reduced non-zero component graph.

2. Definitions and preliminary results

Let $G = (M, E)$ be a graph. All graphs considered here are simple. A subset I of M is said to be independent if no two elements of I are pairwise adjacent. The maximum number of elements of an independent set is called the independence number of G. A subset D of M is called dominating if each element of

2010 Mathematics Subject Classification: 05C25, 05C69, 16Y60.
Keywords: semiring, semimodule, free set, graph isomorphism.

$M \setminus D$ is adjacent to at least one element of D. If no proper subset of D is a dominating set for G, then D is called a minimal dominating set for G. The least cardinality of a dominating set is called the domination number of G. Two graphs (M, E) and $G' = (M', E')$ are said to be isomorphic if there exists a bijective mapping $\phi : M \to M'$ such that $a \sim b$ in M if and only if $\phi(a) \sim \phi(b)$ in M'. A path of length k in a graph G is an alternating sequence of vertices and edges $a_0, e_0, a_1, e_1, a_2, \ldots, a_{k-1}, e_{k-1}, a_k$, where a_i's are distinct (except possibly a_0, a_k) and e_i is the edge joining a_i and a_{i+1}. If there exists a path between any pair of distinct vertices, then it is called connected. The distance between two vertices $a, b \in M$, $d(a, b)$ is defined as the length of the shortest path between a and b. The diameter of a graph G is defined as $diam(G) = max_{a,b \in M} d(a, b)$, if it exists. Otherwise, $diam(G)$ is defined as ∞.

We refer to [3] for further notions on graph theory and [7] for basic notions and results on semirings and semimodules.

A semiring S is an algebraic system $(S, +, \cdot, 0, 1)$ such that $(S, +, 0)$ is a commutative monoid and $(S, \cdot, 1)$ is a monoid, connected by the ring-like distributive laws. Also we assume that $(S, \cdot)$ is commutative, $0 \neq 1$ and the zero element 0 is absorbing, that is $s0 = 0s = 0$ for all $s \in S$. We say that $s \in S$ is invertible if $st = 1$ for some $t \in S$ and denote the set of all invertible elements of S by $U(S)$. If a semiring S is such that $U(S) = S \setminus \{0\}$, then S is said to be a semifield.

Definition 2.1. Let S be a semiring. A *left S-semimodule* is a commutative monoid $(\mathcal{V}, +)$ with additive identity θ for which we have a function $S \times \mathcal{V} \longrightarrow \mathcal{V}$, denoted by $(\lambda, \alpha) \longmapsto \lambda\alpha$ and called as *scalar multiplication*, which satisfies the following conditions for all $a, b \in S$ and $u, v \in \mathcal{V}$:

(i) $a(u + v) = au + av$;
(ii) $(a + b)v = av + bv$;
(iii) $(ab)v = a(bv)$;
(iv) $1v = v$;
(v) $a\theta = \theta = 0v$.

Right S-semimodules are defined analogously. In this paper a semimodule $\mathcal{V}$ over S means left S-semimodule. The elements of $\mathcal{V}$ are called vectors and the elements of S are called scalars.

Let S be a semiring. Then a semimodule $\mathcal{V}$ over S is also known as a semilinear space over S. If a semiring S is a ring, then any semilinear space $\mathcal{V}$ over S is an S-module. In particular, if S is a field then any semilinear space over S is a linear space (or, vector space) over S.

Let B be a non-empty subset of $\mathcal{V}$. Then we denote

$$span(B) = \{\textstyle\sum_{i=1}^{n} c_i x_i : n \in \mathbb{N}, c_i \in S, x_i \in B\}.$$

If $span(B) = \mathcal{V}$, then B is called a generating subset of $\mathcal{V}$. A semimodule $\mathcal{V}$ having a finite generating set B is called finitely generated. A nonempty subset D of vectors in $\mathcal{V}$ is called linearly dependent if there exists $x \in D$ such that

$x \in span(D - \{x\})$; otherwise it is called linearly independent; and free if each element of $\mathcal{V}$ is expressed as a linear combination of the elements of D in at most one way. It is easy to see that every free subset of $\mathcal{V}$ is linearly independent. A linearly independent generating subset of $\mathcal{V}$ is called a basis of $\mathcal{V}$ and a free generating subset of $\mathcal{V}$ is called a free basis of $\mathcal{V}$ [10]. If $\mathcal{V}$ has a free basis then it is called a free semimodule. It is easy to see that every finitely generated semimodule has a basis, and every free basis is a basis [10].

Definition 2.2. A semiring S is said to have *invariant basis number* [IBN] property if any two bases of a finitely generated free semimodule over S have the same cardinality.

A semiring S has the IBN property if and only if for every $s, t \in S$, $s + t = 1$ implies that either $s \in U(S)$ or $t \in U(S)$ [Theorem 4.3; [10]]. Hence every semifield has the IBN property. In particular, the semiring $\mathbb{R}^+ \cup \{0\}$ of all non-negative real numbers, the max-plus semiring $\mathbb{R}_{max}$ and many other tropical semirings are of this type. Apart from the semifields, the semiring $\mathbb{N} \cup \{0\}$ of all non-negative integers also has this property. Thus we see that many useful as well as algebraically important semirings have the IBN property.

Henceforth, unless stated otherwise, S is a semiring having invariant basis number property and $\mathcal{V}$ is a finitely generated free semimodule over S. Let $\mathcal{V}$ be a finitely generated free semimodule over S, then from Corollary 3.1 [10], it follows that every vector of $\mathcal{V}$ can be expressed uniquely in terms of each basis. The cardinality of a basis of $\mathcal{V}$ is denoted by $dim(\mathcal{V})$.

Isomorphism of semimodules is defined similarly to modules. It follows from Corollary 5.2 [9], that semimodules $\mathcal{V}$ and $\mathcal{W}$ are isomorphic if and only if $dim(\mathcal{V}) = dim(\mathcal{W})$.

If $X = \{x_1, x_2, \ldots, x_n\}$ is a basis of a semimodule $\mathcal{V}$, then every vector $v \in \mathcal{V}$ can be expressed uniquely as $v = c_1x_1 + \cdots + c_nx_n$; $c_i \in S$. We call c_i the i-th component of $\mathcal{V}$ and is denoted by v_i.

Definition 2.3. The non-zero component graph of $\mathcal{V}$ relative to the basis X, is defined as $\Gamma_X(\mathcal{V}) = (\mathbb{V}, \mathbb{E})$, where $\mathbb{V} = \mathcal{V} \setminus \{\theta\}$ and $(\alpha, \beta) \in \mathbb{E}$ if there exists i such that α_i, β_i are non-zero.

Note that the vectors of the form $v = c_1x_1 + c_2x_2 + \cdots + c_nx_n$, whose all components are non-zero, adjacent to every other vertex of $\Gamma_X(\mathcal{V})$. These vertices do not have much role on the parameters of $\Gamma_X(\mathcal{V})$. So we propose to consider the graph $\Gamma^*_X(\mathcal{V})$ obtained from $\Gamma_X(\mathcal{V})$ after deletion of such vertices. We call $\Gamma^*_X(\mathcal{V})$ the reduced non-zero component graph of $\mathcal{V}$ with respect to the basis $X = \{x_1, x_2, \ldots, x_n\}$.

Theorem 2.4. *Let $\mathcal{V}$ be a semimodule over a semiring S. Let $\Gamma^*_X(\mathcal{V})$ and $\Gamma^*_Y(\mathcal{V})$ be the reduced non-zero component graphs of $\mathcal{V}$ with respect to the bases $X = \{x_1, x_2, \ldots, x_n\}$ and $Y = \{y_1, y_2, \ldots, y_n\}$ of $\mathcal{V}$. Then $\Gamma^*_X(\mathcal{V})$ and $\Gamma^*_Y(\mathcal{V})$ are graph isomorphic.*

Proof. Define a mapping $\sigma : \mathcal{V} \longrightarrow \mathcal{V}$ such that

$$\sigma(c_1x_1 + c_2x_2 + \cdots + c_nx_n) = c_1y_1 + c_2y_2 + \cdots + c_ny_n.$$

Then clearly σ is an isomorphism on $\mathcal{V}$ such that $\sigma(x_i) = y_i$ for all $i \in \{1, 2, \ldots, n\}$. We show that the restriction of σ on non-null vectors of $\mathcal{V}$ such that at least one component is zero induces a graph isomorphism $\sigma^* : \Gamma^*_X(\mathcal{V}) \longrightarrow \Gamma^*_Y(\mathcal{V})$. Clearly σ^* is a bijection. Let $\alpha = c_1x_1+c_2x_2+\cdots+c_nx_n$ and $\beta = d_1x_1+d_2x_2+\cdots+d_nx_n$ with $\alpha \sim \beta$ in $\Gamma^*_X(\mathcal{V})$. Then there exists i such that $c_i, d_i \neq 0$. Hence $\sigma^*(\alpha) \sim \sigma^*(\beta)$ in $\Gamma^*_Y(\mathcal{V})$. Similarly it can be shown that if α and β are not adjacent in $\Gamma^*_X(\mathcal{V})$, then $\sigma^*(\alpha)$ and $\sigma^*(\beta)$ are not adjacent in $\Gamma^*_Y(\mathcal{V})$. □

Now we define the zero component graph $\Gamma_{0X}(\mathcal{V})$ and reduced zero component graph $\Gamma^*_{0X}(\mathcal{V})$ of a semimodule $\mathcal{V}$ as follows:

Definition 2.5. Let $\mathcal{V}$ be a semimodule with a basis X. The zero component graph of $\mathcal{V}$ is defined as the graph $\Gamma_{0X}(\mathcal{V}) = (V, \mathcal{E})$, where $V = \mathcal{V} \setminus \{\sum c_ix_i : c_1 \cdot c_2 \cdots c_n \neq 0\}$, that is V consists of the elements whose at least one component is zero and $(\alpha, \beta) \in \mathcal{E}$ if there exists i such that both α_i and β_i are zero. Note that $\theta \sim v$ for every v in $\Gamma_{0X}(\mathcal{V})$. In fact θ is the only vertex having this property. The subgraph $\Gamma^*_{0X}(\mathcal{V})$ obtained by deletion of θ, is called the *reduced zero-component graph* of $\mathcal{V}$.

For any two bases X and Y of $\mathcal{V}$, proceeding similarly as in the proof of Theorem 2.4, we can prove that $\Gamma^*_{0X}(\mathcal{V})$ and $\Gamma^*_{0Y}(\mathcal{V})$ are graph isomorphic.

Since the graphs are independent of the choice of a particular basis (up to isomorphism), so we denote the reduced non-zero component graph of $\mathcal{V}$ by $\Gamma^*(\mathcal{V})$ and the reduced zero component graph of $\mathcal{V}$ by $\Gamma^*_0(\mathcal{V})$.

Notice that the vertex set of both $\Gamma^*(\mathcal{V})$ and $\Gamma^*_0(\mathcal{V})$ is same and for the next sections of this article we denote it by $\mathbb{V}$ and $X = \{x_1, x_2, \ldots, x_n\}$ denotes a basis.

3. Properties of the graph $\Gamma^*(\mathcal{V})$

In this section, we investigate some basic properties like connectedness, completeness, domination number, independence number of the graph $\Gamma^*(\mathcal{V})$. Also we show that two semimodules $\mathcal{V}$ and $\mathcal{W}$ are isomorphic if and only if the graphs $\Gamma^*(\mathcal{V})$ and $\Gamma^*(\mathcal{W})$ are isomorphic.

Since any two elements of a basis are pairwise non-adjacent, $\Gamma^*(\mathcal{V})$ is not complete.

Theorem 3.1. *If $n \geqslant 3$, $\Gamma^*(\mathcal{V})$ is connected and $diam(\Gamma^*(\mathcal{V})) = 2$.*

Proof. If $\alpha, \beta \in \mathbb{V}$ are adjacent, then $d(\alpha, \beta) = 1$; otherwise, there exist distinct i, j such that $\alpha_i, \beta_j \neq 0$. Since $n \geqslant 3$, there exists $\gamma \in \mathbb{V}$ such that $\gamma_i, \gamma_j \neq 0$. So $\alpha \sim \gamma$ and $\beta \sim \gamma$ and hence $d(\alpha, \beta) = 2$. Thus $\Gamma^*(\mathcal{V})$ is connected and $diam(\Gamma^*(\mathcal{V})) = 2$. □

Theorem 3.2. *The domination number of* $\Gamma^*(\mathcal{V})$ *is* 2.

Proof. It is easily seen that $\{x_1 + x_2 + \cdots + x_{n-1}, x_2 + x_3 + \cdots x_n\}$ is a minimal dominating subset of $\Gamma^*(\mathcal{V})$. If possible, let $\{\alpha\}$ be a dominating subset of $\Gamma^*(\mathcal{V})$. Then there exists i such that $\alpha_i = 0$. Consider $\beta \in \mathbb{V}$ such that $\beta_i \neq 0$ but $\beta_j = 0$ for all $j \neq i$. Then $\alpha \nsim \beta$. Hence the result. □

Theorem 3.3. *If* $D = \{y_1, y_2, \ldots, y_l\}$ *is a minimal dominating set of* $\Gamma^*_X(\mathcal{V})$*, then* $l \leqslant n$.

Proof. Let $D_i = D \setminus \{y_i\}$ for $i \in \{1, 2, \ldots, n\}$. Since D is a minimal dominating set, for all $i \in \{1, 2, \ldots, l\}$, D_i is not a dominating subset of $\Gamma^*_X(\mathcal{V})$. So, for each $i \in \{1, 2, \ldots, l\}$, there exists $z_i \in \Gamma^*(\mathcal{V})$ such that $z_i \sim y_i$ but $z_i \nsim y_j$ for $j \neq i$. Since $z_i \neq \theta$, there exists t_i such that $(z_i)_{t_i} \neq 0$. So $x_{t_i} \nsim y_j$ for $j \neq i$ but $x_{t_i} \sim y_i$ as D is a minimal dominating set.

Now we show that $x_{t_i} \neq x_{t_j}$ for $i \neq j$. If possible, let $x_{t_i} = x_{t_j}$ for some $i \neq j$. Since $x_{t_i} \sim y_i$ and $x_{t_i} = x_{t_j}$, so $x_{t_j} \sim y_i$ which contradicts that $x_{t_i} \nsim y_j$ for all $i \neq j$. Hence $x_{t_i} \neq x_{t_j}$ for $i \neq j$. Since $x_{t_1}, x_{t_2}, \ldots, x_{t_l}$ are all distinct, it follows that $l \leqslant n$. □

Theorem 3.4. *The independence number of* $\Gamma^*_X(\mathcal{V})$ *is* n.

Proof. It is easy to observe that $\{x_1, x_2, \ldots, x_n\}$ is an independent set of $\Gamma^*_X(\mathcal{V})$. So the independence number of $\Gamma^*_X(\mathcal{V})$ is greater than or equal to n. If possible, let $\{y_1, y_2, \ldots, y_l\}$ be an independent set of $\Gamma^*_X(\mathcal{V})$ such that $l > n$. Since for all $i \in \{1, 2, \ldots, l\}$, $y_i \neq \theta$, there exists t_i such that $(y_i)_{t_i} \neq 0$. We show that $t_i \neq t_j$ when $i \neq j$. If $t_i = t_j = t$ for some $i \neq j$, then t_i th component of both y_i and y_j is non-zero and hence $y_i \sim y_j$, which is a contradiction to the independence of y_i and y_j. Since there are exactly n distinct x_i, the independence number of $\Gamma^*_X(\mathcal{V})$ is n. □

Lemma 3.5. *Let* I *be an independent set in* $\Gamma^*_X(\mathcal{V})$*, then* I *is linearly independent in* $\mathcal{V}$.

Proof. Let $I = \{y_1, y_2, \ldots, y_l\}$ be an independent set of $\Gamma^*_X(\mathcal{V})$. Then by Theorem 3.4, $l \leqslant n$. If possible, let I be linearly dependent in $\mathcal{V}$. Then there exists $i \in \{1, 2, \ldots, l\}$ such that y_i is expressed as a linear combination of $y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_l$, i.e., $y_i = c_1y_1 + c_2y_2 + \cdots + c_{i-1}y_{i-1} + c_{i+1}y_{i+1} + \cdots + c_ly_l = \sum_{j=1, j\neq i}^{l} c_jy_j$

Let $y_j = \sum_{t=1}^{n} d_{tj}x_t$ for $j = 1, 2, \ldots, i-1, i+1, \ldots, l$. Thus,

$$y_i = (c_1d_{11} + \cdots + c_{i-1}d_{1,i-1} + c_{i+1}d_{1,i+1} + \cdots + c_ld_{1l})x_1 + (c_1d_{21} + \cdots + c_{i-1}d_{2,i-1} + c_{i+1}d_{2,i+1} + \cdots + c_ld_{2l})x_2 + \cdots + (c_1d_{n1} + \cdots + c_{i-1}d_{n,i-1} + c_{i+1}d_{n,i+1} + \cdots + c_ld_{nl})x_n$$

Since $y_i \neq \theta$, there exists t_0 such that $(y_i)_{t_0} \neq 0$. So, there exists y_k such that $k \neq i$ and $(y_k)_{t_0} \neq 0$, otherwise t_0-th component of y_i will be 0. Which shows that $\{y_1, y_2, \ldots, y_l\}$ is not independent in $\Gamma^*_X(\mathcal{V})$. This contradiction shows that $\{y_1, y_2, \ldots, y_l\}$ is linearly independent in $\mathcal{V}$. □

Remark 3.6. Converse of the Lemma 3.5 is not true, in general, if we consider the subset $\{x_1, x_1 + x_2\}$ of a three dimensional semimodule with respect to the basis $\{x_1, x_2, x_3\}$.

Now, we show that two semimodules are isomorphic if and only if their corresponding reduced non-zero component graphs are isomorphic.

Lemma 3.7. *Two semimodules $\mathcal{V}$ and $\mathcal{W}$ are isomorphic if and only if the reduced non-zero component graphs $\Gamma^*(\mathcal{V})$ and $\Gamma^*(\mathcal{W})$ are isomorphic.*

Proof. Let $\mathcal{V}$ and $\mathcal{W}$ be isomorphic and $\sigma : \mathcal{V} \longrightarrow \mathcal{W}$ be an isomorphism. Then $Y = \{\sigma(x_1), \sigma(x_2), \ldots,$
$\sigma(x_n)\}$ is a basis of W. Consider the restriction $\sigma^* : \Gamma^*_X(\mathcal{V}) \longrightarrow \Gamma^*_Y(\mathcal{W})$ given by

$$\sigma^*(c_1x_1 + c_2x_2 + \cdots + c_nx_n) = c_1\sigma(x_1) + c_2\sigma(x_2) + \cdots + c_n\sigma(x_n)$$

where $c_1 \cdot c_2 \cdots c_n = 0$ but $(c_1, c_2, \ldots, c_n) \neq (0, 0, \ldots, 0)$. Clearly σ^* is a bijection. Let $\alpha = c_1x_1 + \cdots + c_nx_n$ and $\beta = d_1x_1 + \cdots + d_nx_n$. Then $\alpha \sim \beta$ in $\Gamma^*_X(\mathcal{V})$ if and only if there exists i such that $c_i, d_i \neq 0$ if and only if $\sigma^*(\alpha) \sim \sigma^*(\beta)$ in $\Gamma^*_Y(W)$. Therefore $\Gamma^*(\mathcal{V})$ and $\Gamma^*(W)$ are isomorphic.

Conversely, let $\phi : \Gamma^*(\mathcal{V}) \to \Gamma^*(\mathcal{W})$ be a graph isomorphism. let $dim(\mathcal{V}) = m$ and $dim(W) = n$. Since isomorphism preserves the independence number, the independence number of $\Gamma^*(\mathcal{V})$ equals to the independence number of $\Gamma^*(\mathcal{W})$ and hence $m = n$. So $\mathcal{V}$ and $\mathcal{W}$ are isomorphic. □

Thus we see that a semimodule isomorphism $\sigma : \mathcal{V} \to \mathcal{W}$ is also a graph isomorphism (ignoring the null vector and vectors of the form $c_1x_1 + \cdots + c_nx_n$ such that $c_1 \cdot c_2 \ldots c_n \neq 0$), however the converse may not be true which is shown in the following example.

Example 3.8. Consider the semimodule $\mathbb{N}_0^2$ over $\mathbb{N}_0$, the set of all nonnegative integers, with respect to usual addition and multiplication. Then the vertex set $\mathbb{V}$ of $\Gamma^*(\mathbb{N}_0^2)$, is $\{(a, b) \in \mathbb{N}_0^2 : a = 0 \text{ or } b = 0 \text{ and } (a, b) \neq (0, 0)\}$. Define a map $\phi : \mathbb{V} \to \mathbb{V}$ defined by $\phi(1, 0) = (3, 0)$, $\phi(3, 0) = (1, 0)$, $\phi(n, 0) = (n, 0)$ for $n \neq 1, 3$ and $\phi(0, m) = (0, m)$, where $m \in \mathbb{N}_0$. Then ϕ is a graph isomorphism on $\Gamma^*(\mathbb{N}_0^2)$ but it can not be extended to a linear transformation on $\mathbb{N}_0^2$. Otherwise $(1, 0) = \phi(3, 0) = 3\phi(1, 0) = (9, 0)$, which is a contradiction.

Now, we study the form of automorphisms of $\Gamma^*(\mathcal{V})$.

Theorem 3.9. *Let ϕ be a graph automorphism on $\Gamma^*_X(\mathcal{V})$. Then ϕ permutes the elements of $X = \{x_1, x_2, \ldots, x_n\}$ of $\mathcal{V}$ with some non-zero scalar multiplication, i.e. there exists a permutation $\sigma \in S_n$ such that $\phi(x_i) = c_ix_{\sigma(i)}$, where c_i's are non-zero.*

Proof. Since ϕ is a graph automorphism on $\Gamma^*_X(\mathcal{V})$ and $\{x_1, x_2, \ldots, x_n\}$ is an independent set of vertices in $\Gamma^*_X(\mathcal{V})$, therefore $\{\phi(x_i) : i = 1, 2, \ldots, n\}$ is also an independent set of vertices in $\Gamma^*_X(\mathcal{V})$. Let

$$\begin{aligned}\phi(x_1) &= c_{11}x_1 + c_{12}x_2 + \cdots + c_{1n}x_n\\ \phi(x_2) &= c_{21}x_1 + c_{22}x_2 + \cdots + c_{2n}x_n\\ &\cdots\cdots\cdots\cdots\cdots\cdots\\ \phi(x_n) &= c_{n1}x_1 + c_{n2}x_2 + \cdots + c_{nn}x_n\end{aligned}$$

Since $\phi(x_1) \neq 0$, there exists $j_1 \in \{1, 2, \ldots, n\}$ such that $c_{1j_1} \neq 0$. Therefore $c_{ij_1} = 0$ for all $i \neq 1$ because $\phi(x_i)$ is not adjacent to $\phi(x_1)$ for all $i \neq 1$. Similarly, for $\phi(x_2)$, there exists $j_2 \in \{1, 2, \ldots, n\}$ such that $c_{2j_2} \neq 0$ and $c_{ij_2} = 0$ for all $i \neq 2$. Moreover, $j_1 \neq j_2$ as $\phi(x_1)$ and $\phi(x_2)$ are not adjacent. Proceeding in this way, we see that for $\phi(x_n)$, there exists $j_n \in \{1, 2, \ldots, n\}$ such that $c_{nj_n} \neq 0$ and $c_{ij_n} = 0$ for all $i \neq n$ and $j_1, j_2, \ldots, j_n \in \{1, 2, \ldots, n\}$ are all distinct numbers.

Thus we see that $c_{kj_l} = 0$ for all $k \neq l$ and $c_{kj_k} \neq 0$, where $k, l \in \{1, 2, \ldots, n\}$. Let $\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix}$. Then σ is a permutation on $\{1, 2, \ldots, n\}$ and $\phi(x_i) = c_{ij_i}x_{j_i} = c_{ij_i}x_{\sigma(i)}$, where $c_{ij_i} \neq 0$ and hence the result follows. □

Theorem 3.10. *Let ϕ be a graph automorphism on $\Gamma^*_X(\mathcal{V})$ such that ϕ maps x_i into $c_{ij_i}x_{\sigma(i)}$ for some $\sigma \in S_n$, where $c_{ij_i} \neq 0$. Then, for $\{i_1, i_2, \ldots, i_k\} \subset \{1, 2, \ldots, n\}$, if c_i's are non-zero, then $\phi(c_1x_{i_1} + \cdots + c_kx_{i_k}) = d_1x_{\sigma(i_1)} + \cdots + d_kx_{\sigma(i_k)}$, where d_i's are non-zero.*

Proof. Since $cx_i \sim x_i$ in $\Gamma^*_X(\mathcal{V})$ and ϕ is an automorphism on $\Gamma^*_X(\mathcal{V})$, $\phi(cx_i) \sim \phi(x_i)$ i.e., $\phi(cx_i) \sim c_{ij}x_{\sigma(i)}$. So, $\sigma(i)$-th component of $\phi(cx_i)$ is non-zero. If possible, let $\sigma(j)$-th component of $\phi(cx_i)$ is non-zero for $j \neq i$. Then $\phi(cx_i) \sim x_{\sigma(j)}$ i.e. $\phi(cx_i) \sim \phi(x_j)$. Which in turn implies that $cx_i \sim x_j$ for $i \neq j$, which is a contradiction since $\{x_1, x_2, \ldots, x_n\}$ is an independent set. Therefore, $\phi(cx_i) = dx_{\sigma(i)}$ for some $d \neq 0$.

Now, for all $\{i_1, i_2, \ldots, i_k\} \subset \{1, 2, \ldots, n\}$,

$$\begin{aligned}&c_1x_{i_1} + c_2x_{i_2} + \cdots + c_kx_{i_k} \sim x_{i_1}\\ \Rightarrow &\phi(c_1x_{i_1} + c_2x_{i_2} + \cdots + c_kx_{i_k}) \sim \phi(x_{i_1}) = cx_{\sigma(i_1)} \text{ for some } c \neq 0.\end{aligned}$$

Which implies that $\phi(c_1x_{i_1} + c_2x_{i_2} + \cdots + c_kx_{i_k}) \sim x_{\sigma(i_1)}$. Similarly, $\phi(c_1x_{i_1} + c_2x_{i_2} + \cdots + c_kx_{i_k}) \sim x_{\sigma(i_2)}$ and so on. Therefore, $\phi(c_1x_{i_1} + c_2x_{i_2} + \cdots + c_kx_{i_k}) = d_1x_{\sigma(i_1)} + d_2x_{\sigma(i_2)} + \cdots + d_kx_{\sigma(i_k)}$, where d_i's are non-zero □

Corollary 3.11. *If $n \geqslant 3$, then $\Gamma^*_X(\mathcal{V})$ is not vertex transitive.*

Proof. If $n \geqslant 3$, then by Theorem 3.10, there does not exist any automorphism which maps x_1 to $x_1 + x_2$. □

4. Graph isomorphism of $\Gamma^*(\mathcal{V})$ and $\Gamma^*_0(\mathcal{V})$

In this section we show that for a semimodule $\mathcal{V}$ over S, if $|S| \geqslant \aleph_0$, then the reduced non-zero component graph and reduced zero component graph of $\mathcal{V}$ are

isomorphic. Now we show that if $|S| < \aleph_0$, then the two graphs $\Gamma^*(\mathcal{V})$ and $\Gamma_0^*(\mathcal{V})$ may not be isomorphic.

Example 4.12. Let $S = \{0, 1, a\}$ be the chain $0 < a < 1$. Consider the semimodule S^3 over S and a basis $E = \{(1,0,0),(0,1,0),(0,0,1)\}$. Then the vertex set of both reduced zero and reduced non-zero component graphs of S^3 is $\{(1,0,0),(1,0,a),(1,0,1),(1,1,0),(1,a,0),(a,0,0),(a,0,a),(a,0,1),(a,a,0),(a,1,0),(0,a,a),(0,a,0),(0,a,1),(0,0,a),(0,0,1),(0,1,0),(0,1,1),(0,1,a)\}$. The degree of $(1,0,0)$ in $\Gamma_E^*(S^3)$ is 9. But, there does not exist any element of degree 9 in $\Gamma_{0E}^*(S^3)$. Therefore $\Gamma_E^*(S^3)$ is not isomorphic to $\Gamma_{0E}^*(S^3)$.

Theorem 4.13. *Let $\mathcal{V}$ be a semimodule over S and X be a basis of $\mathcal{V}$. If $|S| \geqslant \aleph_0$, then $\Gamma_X^*(\mathcal{V})$ and $\Gamma_{0X}^*(\mathcal{V})$ are isomorphic.*

Proof. Let $X = \{x_1, x_2, \ldots, x_n\}$. Then the two graphs $\Gamma_X^*(\mathcal{V})$ and $\Gamma_{0X}^*(\mathcal{V})$ have the same set of vertices $\mathbb{V} = \{\sum_{i=1}^n a_i x_i : \exists i, j \text{ such that } a_i = 0 \text{ and } a_j \neq 0\}$. For $A = \{i_1, i_2, \ldots, i_k\} \subset \{1, 2, \ldots, n\}$, denote $Z_A = \{\sum a_i x_i \in \mathcal{V} : a_{i_1} = \ldots = a_{i_k} = 0$ and $a_i \neq 0$ otherwise $\}$. Then $\mathbb{V}$ is a disjoint union of the sets Z_A, where A is a non-empty proper subset of $\{1, 2, \ldots, n\}$, i.e. $\mathbb{V} = \bigcup Z_A$. Now, since $|S| \geqslant \aleph_0$, $|Z_A| = |Z_{A^c}| = |\mathbb{V}|$, which implies that there exists a bijection $\phi_A : Z_A \to Z_{A^c}$.

Thus we get a bijection $\phi = \cup\phi_A : \mathbb{V} \longrightarrow \mathbb{V}$ such that $a \sim b$ in $\Gamma_{0X}^*(\mathcal{V})$ if and only if $\phi(a) \sim \phi(b)$ in $\Gamma_X^*(\mathcal{V})$. Hence $\Gamma_X^*(\mathcal{V})$ and $\Gamma_{0X}^*(\mathcal{V})$ are isomorphic as graphs. □

References

[1] **I. Beck**, *Coloring of commutative rings*, J. Algebra. **116** (1988), 208 – 226.

[2] **A.K. Bhuniya and S. Bera**, *On some characterizations of strong power graphs of finite groups*, Special Matrices **4** (2016), 121 – 129.

[3] **J.A. Bondy and U.S. Murty**, *Graph Theory*, Springer-Verlag London, 2008.

[4] **P.J. Cameron and S. Ghosh**, *The power graph of a finite group*, Discrete Mathematics **311** (2011), no. 13, 1220 – 1222.

[5] **I. Chakrabarty, S. Ghosh and M.K. Sen**, *Undirected power graph of semigroups*, Semigroup Forum **78** (2009), 410 – 426.

[6] **A. Das**, *On non-zero component graph of vector spaces over finite fields*, J. Algebra Appl. **16** (2017), no. 1, 1750007 (10 pages).

[7] **J.S. Golan**, *Semirings and their Applications*, Kluwer, Dordrecht, 1999.

[8] **S. Maity and A.K. Bhuniya**, *On the spectrum of linear dependence graph of a finite dimensional vector space*, Electron. J. Graph Theory Appl. **7** (2019), 43 – 59.

[9] **Q.Y. Shu and X.P. Wang**, *Bases in semilinear spaces over zerosumfree semirings*, Linear Algebra Appl. **435** (2011), 2681 – 2692.

[10] **Y.J. Tan**, *Bases in semimodules over commutative semirings*, Linear Algebra Appl. **443** (2014), 139 – 152.

Received February 3, 2020

Department of Mathematics, Visva-Bharati, Santiniketan-731235, West Bengal, India
E-mail: susbhnmaity@gmail.com; anjankbhuniya@gmail.com

Quasigroups and Related Systems **28** (2020), 251 – 268

Cryptanalysis of some stream ciphers based on n-ary groupoids

Nadezhda N. Malyutina

Abstract. We research generalized Markovski algorithm based on i-invertible n-groupoids. We give lower bounds for cryptoattacks named as chosen ciphertext and plaintext attacks. Also we give modifications of these attacks.

1. Introduction

The use of quasigroups opens new ways in construction of stream and block ciphers [3, 4]. We continue researches of applications of n-ary groupoids that are invertible on i-th place in cryptology [2, 5].

Definition 1.1. n-Ary groupoid (Q, f) is called *invertible on the i-th place*, $i \in \overline{1,n}$, if the equation $f(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n) = a_{n+1}$ has a unique solution for any elements $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n, a_{n+1} \in Q$.

In this case the operation ${}^{(i,n+1)}f(a_1, \dots, a_{i-1}, a_{n+1}, a_{i+1}, \dots, a_n) = x_i$ is defined in a unique way and we have:

$$f(a_1, \dots, a_{i-1}, {}^{(i,n+1)}f(a_1, \dots, a_{i-1}, a_{n+1}, a_{i+1}, \dots, a_n), a_{i+1}, \dots, a_n) = a_{n+1},$$
$${}^{(i,n+1)}f(a_1, \dots, a_{i-1}, f(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n), a_{i+1}, \dots, a_n) = x_i.$$

Algorithm 1.2. Let Q be a non-empty finite alphabet and k be a natural number, $u_j, v_j \in Q$, $j \in \{1, ..., k\}$. Define an n-ary groupoid (Q, f) which is invertible on the i-th place,$i \in \overline{1,n}$. Then the groupoid $(Q, {}^{(i,n+1)}f)$ is defined in a unique way.

Take the fixed elements $l_1^{(n-1)(n-1)}$ ($l_i \in Q$), which are called *leaders*.

Let $u_1u_2...u_k$ be a k-tuple of letters from Q.

2010 Mathematics Subject Classification: 20N15, 20N05, 05B15, 94A60
Keywords: cipher, ciphertext, plaintext, Markovski algorithm, n-ary groupoid.

The following ciphering (encryption) procedure is proposed:

$$\begin{aligned}
&v_1 = f(l_1, \dots, l_{i-1}, u_1, l_i, \dots, l_{n-1}),\\
&v_2 = f(l_n, \dots, l_{n+i-2}, u_2, l_{n+i-1}, \dots, l_{2n-2}),\\
&\dots\dots\dots\dots\dots,\\
&v_{n-1} = f(l_{n^2-3n+3}, \dots, l_{n^2-3n+1+i}, u_{n-1}, l_{n^2-3n+2+i}, \dots, l_{(n-1)^2}),\\
&v_n = f(v_1, \dots, v_{i-1}, u_n, v_i, \dots, v_{n-1}),\\
&v_{n+1} = f(v_2, \dots, v_i, u_{n+1}, v_{i+1}, \dots, v_n),\\
&\dots\dots\dots\dots\dots
\end{aligned} \tag{1}$$

Therefore we obtain the following ciphertext: $v_1 v_2 \dots, v_{n-1}, v_n, v_{n+1}, \dots$
The deciphering algorithm is constructed similarly to the binary case:

$$\begin{aligned}
&u_1 = {}^{(i,n+1)}f(l_1, \dots, l_{i-1}, v_1, l_i, \dots, l_{n-1}),\\
&u_2 = {}^{(i,n+1)}f(l_n, \dots, l_{n+i-2}, v_2, l_{n+i-1}, \dots, l_{2n-2}),\\
&\dots\dots\dots\dots\dots,\\
&u_{n-1} = {}^{(i,n+1)}f(l_{n^2-3n+3}, \dots, l_{n^2-3n+1+i}, v_{n-1}, l_{n^2-3n+2+i}, \dots,\\
&l_{(n-1)^2})\\
&u_n = {}^{(i,n+1)}f(v_1, \dots, v_{i-1}, v_n, v_i, \dots, v_{n-1}),\\
&u_{n+1} = {}^{(i,n+1)}f(v_2, \dots, v_i, v_{n+1}, v_{i+1}, \dots, v_n),\\
&\dots\dots\dots\dots\dots
\end{aligned} \tag{2}$$

2.Results

2.1 Ciphertext attacks

S. Markovski, E. Ochodkova and V. Snashel proposed a new stream cipher to encrypt the file system [3, 4]. M. Vojvoda has given the cryptanalysis of the file encoding system based on binary quasigroups [6, 7] and showed how to break this cipher. These attacks are described by M. Vojvoda [7]. See [1] for the case of n-ary quasigrops.

We studied cryptographic attacks on the cipher using the generalized Markovski algorithm. In this article we will conduct a comparative analysis, identify positive and negative points in these attacks. Given examples provide lower bounds of such attacks.

Consider an attack with text constructed using an n-ary groupoid, which is invertible on the i-th place obtained using the generalized Markovski algorithm.

Assume the cryptanalyst has access to the decryption device loaded with the key. He can then construct the following ciphertext, where n is arity and m the order of an i-invertible groupoid:

$q_1q_1\dots q_1q_1q_1q_1\dots q_1q_2q_1q_1\dots q_1q_m$
$q_1q_1\dots q_2q_1q_1q_1\dots q_2q_2q_1q_1\dots q_2q_m$
$q_1q_1\dots q_3q_1q_1q_1\dots q_3q_2q_1q_1\dots q_3q_m$
. . . . . .
$q_1q_1\dots q_mq_1q_1q_1\dots q_mq_2q_1q_1\dots q_mq_m\dots$

and enter it into the decryption device.

For a complete reconstruction of the table of values of the operation ${}^{(i,n+1)}f$, and hence the table of values of the operation f, it is sufficient to submit at the input: $A = (n \cdot m^{n-1} + 1)(m-1)$ characters to get all the values or $A - 1 = n \cdot m^{n-1}(m-1) + (m-2)$ characters, when the last value is found by the exception method.

We give numerical examples instead of "general case" in order to make the reading of this paper more convenient . We hope that any qualified student can be easy to write "general case" using these examples.

Example 2.1. Take the ternary groupoid (R_3, f), $R_3 = \{0, 1, 2\}$, which is defined over the ring $(R_3, +, \cdot)$ residue classes modulo 3 and which is invertible on first place.

Ternary operation f on the set R_3 is defined as:
$f(x_1, x_2, x_3) = \alpha x_1 + \beta x_2 + \gamma x_3 = x_4$, where

$$\begin{gathered}\alpha 0 = 2, \alpha 1 = 0, \alpha 2 = 1,\\ \beta 0 = 0, \beta 1 = 1, \beta 2 = 1,\\ \gamma 0 = 2, \gamma 1 = 0, \gamma 2 = 0.\end{gathered}$$

Inverse operation for f or (14)-parastrophe is the following operation:
${}^{(1,4)}f(x_4, x_2, x_3) = x_1 = \alpha^{-1}(x_4 + 2 \cdot \beta x_2 + 2 \cdot \gamma x_3)$, where $\alpha^{-1}(0) = 1$, $\alpha^{-1}(1) = 2$, $\alpha^{-1}(2) = 0$.
Check.

$$\begin{aligned}f({}^{(1,4)}f(x_4, x_2, x_3), x_2, x_3) &= \alpha(\alpha^{-1}(x_4 + 2 \cdot \beta x_2 + 2 \cdot \gamma x_3)) + \beta x_2 + \gamma x_3\\ &= x_4 + 2 \cdot \beta x_2 + 2 \cdot \gamma x_3 + \beta x_2 + \gamma x_3 = x_4.\\ {}^{(1,4)}f(f(x_1, x_2, x_3), x_2, x_3) &= \alpha^{-1}(\alpha x_1 + \beta x_2 + \gamma x_3 + 2 \cdot \beta x_2 + 2 \cdot \gamma x_3)\\ &= \alpha^{-1}(\alpha x_1) = x_1.\end{aligned}$$

Elements: $l_1 = 0, l_2 = 2, l_3 = 1, l_4 = 2$ are used as leaders.
We will use Algorithm 1.2. and we can construct the following ciphertext:

$q_1q_1q_1q_1q_1q_2q_1q_1q_3q_1q_2q_1q_1q_2q_2q_1q_2q_3q_1q_3q_1q_1q_3q_2q_1q_3q_3$
$q_2q_1q_1q_2q_1q_2q_2q_1q_3q_2q_2q_1q_2q_2q_2q_2q_2q_3q_2q_3q_1q_2q_3q_2q_2q_3q_3$
q_3q_1
or
000001002010011012020021022
100101102110111112120121122
20

and enter it into the decryption device.

The process of decrypting the text and the results are as follows:

Table 1: Decrypted text

$u_1 =^{(1,4)} f(v_1, l_1, l_2) =^{(1,4)} f(q_1, l_1, l_2)$ $=^{(1,4)} f(0,0,2) = 1$	$u_{29} =^{(1,4)} f(0,2,1) = 0$
$u_2 =^{(1,4)} f(v_2, l_3, l_4) =^{(1,4)} f(q_1, l_3, l_4)$ $=^{(1,4)} f(0,1,2) = 0$	$u_{30} =^{(1,4)} f(0,1,0) = 1$
$u_3 =^{(1,4)} f(v_3, v_1, v_2) =^{(1,4)} f(q_1, q_1, q_1)$ $=^{(1,4)} f(0,0,0) = 2 - (1)$	$u_{31} =^{(1,4)} f(1,0,0) = 0$
$u_4 =^{(1,4)} f(0,0,0) = 2$	$u_{32} =^{(1,4)} f(0,0,1) = 1$
$u_5 =^{(1,4)} f(0,0,0) = 2$	$u_{33} =^{(1,4)} f(1,1,0) = 2$
$u_6 =^{(1,4)} f(1,0,0) = 0 - (10)$	$u_{34} =^{(1,4)} f(1,0,1) = 2$
$u_7 =^{(1,4)} f(0,0,1) = 1 - (2)$	$u_{35} =^{(1,4)} f(0,1,1) = 0$
$u_8 =^{(1,4)} f(0,1,0) = 1 - (4)$	$u_{36} =^{(1,4)} f(2,1,0) = 0$
$u_9 =^{(1,4)} f(2,0,0) = 1 - (19)$	$u_{37} =^{(1,4)} f(1,0,2) = 2$
$u_{10} =^{(1,4)} f(0,0,2) = 1 - (3)$	$u_{38} =^{(1,4)} f(1,2,1) = 1 - (17)$
$u_{11} =^{(1,4)} f(1,2,0) = 2 - (16)$	$u_{39} =^{(1,4)} f(0,1,1) = 0$
$u_{12} =^{(1,4)} f(0,0,1) = 1$	$u_{40} =^{(1,4)} f(1,1,0) = 2$
$u_{13} =^{(1,4)} f(0,1,0) = 1$	$u_{41} =^{(1,4)} f(1,0,1) = 2$
$u_{14} =^{(1,4)} f(1,0,0) = 0$	$u_{42} =^{(1,4)} f(1,1,1) = 1 - (14)$
$u_{15} =^{(1,4)} f(1,0,1) = 2 - (11)$	$u_{43} =^{(1,4)} f(1,1,1) = 1$
$u_{16} =^{(1,4)} f(0,1,1) = 0 - (5)$	$u_{44} =^{(1,4)} f(1,1,1) = 1$
$u_{17} =^{(1,4)} f(1,1,0) = 2 - (13)$	$u_{45} =^{(1,4)} f(2,1,1) = 2 - (23)$
$u_{18} =^{(1,4)} f(2,0,1) = 0 - (20)$	$u_{46} =^{(1,4)} f(1,1,2) = 1 - (15)$
$u_{19} =^{(1,4)} f(0,1,2) = 0 - (6)$	$u_{47} =^{(1,4)} f(2,2,1) = 2 - (26)$
$u_{20} =^{(1,4)} f(2,2,0) = 0 - (25)$	$u_{48} =^{(1,4)} f(0,1,2) = 0$
$u_{21} =^{(1,4)} f(0,0,2) = 1$	$u_{49} =^{(1,4)} f(1,2,0) = 2$
$u_{22} =^{(1,4)} f(0,2,0) = 1 - (7)$	$u_{50} =^{(1,4)} f(2,0,1) = 0$
$u_{23} =^{(1,4)} f(2,0,0) = 1$	$u_{51} =^{(1,4)} f(1,1,2) = 1$
$u_{24} =^{(1,4)} f(1,0,2) = 2 - (12)$	$u_{52} =^{(1,4)} f(1,2,1) = 1$
$u_{25} =^{(1,4)} f(0,2,1) = 0 - (8)$	$u_{53} =^{(1,4)} f(2,1,1) = 2$
$u_{26} =^{(1,4)} f(2,1,0) = 0 - (22)$	$u_{54} =^{(1,4)} f(2,1,2) = 2 - (24)$
$u_{27} =^{(1,4)} f(2,0,2) = 0 - (21)$	$u_{55} =^{(1,4)} f(2,2,2) = 2 - (27)$
$u_{28} =^{(1,4)} f(1,2,2) = 1 - (18)$	$u_{56} =^{(1,4)} f(0,2,2) = 0 - (9)$

At the output we get:

1022201111211020200011120001010122002102211121202011222 0.

Thus, for a complete reconstruction of the table of values of the operation ${}^{(1,4)}f$, and hence the table of values of the operation f, it is enough to supply 55 characters (without the last one) for the ternary groupoid at the input, or 56 characters to restore all values. The table of the decrypting function is hacked:

Table 2: Decryption function

N	Value	N	Value
(1)	${}^{(1,4)}f(0,0,0) = \alpha^{-1}(1) = 2$	(15)	${}^{(1,4)}f(1,1,2) = \alpha^{-1}(0) = 1$
(2)	${}^{(1,4)}f(0,0,1) = \alpha^{-1}(0) = 1$	(16)	${}^{(1,4)}f(1,2,0) = \alpha^{-1}(1) = 2$
(3)	${}^{(1,4)}f(0,0,2) = \alpha^{-1}(0) = 1$	(17)	${}^{(1,4)}f(1,2,1) = \alpha^{-1}(0) = 1$
(4)	${}^{(1,4)}f(0,1,0) = \alpha^{-1}(0) = 1$	(18)	${}^{(1,4)}f(1,2,2) = \alpha^{-1}(0) = 1$
(5)	${}^{(1,4)}f(0,1,1) = \alpha^{-1}(2) = 0$	(19)	${}^{(1,4)}f(2,0,0) = \alpha^{-1}(0) = 1$
(6)	${}^{(1,4)}f(0,1,2) = \alpha^{-1}(2) = 0$	(20)	${}^{(1,4)}f(2,0,1) = \alpha^{-1}(2) = 0$
(7)	${}^{(1,4)}f(0,2,0) = \alpha^{-1}(0) = 1$	(21)	${}^{(1,4)}f(2,0,2) = \alpha^{-1}(2) = 0$
(8)	${}^{(1,4)}f(0,2,1) = \alpha^{-1}(2) = 0$	(22)	${}^{(1,4)}f(2,1,0) = \alpha^{-1}(2) = 0$
(9)	${}^{(1,4)}f(0,2,2) = \alpha^{-1}(2) = 0$	(23)	${}^{(1,4)}f(2,1,1) = \alpha^{-1}(1) = 2$
(10)	${}^{(1,4)}f(1,0,0) = \alpha^{-1}(2) = 0$	(24)	${}^{(1,4)}f(2,1,2) = \alpha^{-1}(1) = 2$
(11)	${}^{(1,4)}f(1,0,1) = \alpha^{-1}(1) = 2$	(25)	${}^{(1,4)}f(2,2,0) = \alpha^{-1}(2) = 0$
(12)	${}^{(1,4)}f(1,0,2) = \alpha^{-1}(1) = 2$	(26)	${}^{(1,4)}f(2,2,1) = \alpha^{-1}(1) = 2$
(13)	${}^{(1,4)}f(1,1,0) = \alpha^{-1}(1) = 2$	(27)	${}^{(1,4)}f(2,2,2) = \alpha^{-1}(1) = 2$
(14)	${}^{(1,4)}f(1,1,1) = \alpha^{-1}(0) = 1$		

Knowing the value table for ${}^{(1,4)}f$ operation, value table is easily restored for f:

Table 3: Encryption function

N	Value	N	Value
(1)	$f(0,0,0) = 1$	(15)	$f(1,1,2) = 1$
(2)	$f(0,0,1) = 2$	(16)	$f(1,2,0) = 0$
(3)	$f(0,0,2) = 2$	(17)	$f(1,2,1) = 1$
(4)	$f(0,1,0) = 2$	(18)	$f(1,2,2) = 1$
(5)	$f(0,1,1) = 0$	(19)	$f(2,0,0) = 0$
(6)	$f(0,1,2) = 0$	(20)	$f(2,0,1) = 1$
(7)	$f(0,2,0) = 2$	(21)	$f(2,0,2) = 1$
(8)	$f(0,2,1) = 0$	(22)	$f(2,1,0) = 1$
(9)	$f(0,2,2) = 0$	(23)	$f(2,1,1) = 2$
(10)	$f(1,0,0) = 2$	(24)	$f(2,1,2) = 2$
(11)	$f(1,0,1) = 0$	(25)	$f(2,2,0) = 1$
(12)	$f(1,0,2) = 0$	(26)	$f(2,2,1) = 2$
(13)	$f(1,1,0) = 0$	(27)	$f(2,2,2) = 2$
(14)	$f(1,1,1) = 1$		

To understand the situation with hacking of the decrypted text and the leaders, consider the plaintext of the form: 101202=$u_1u_2u_3u_4u_5u_6$.
$v_1 = f(u_1, l_1, l_2) = f(1, l_1, l_2) =?$

$v_2 = f(u_2, l_3, l_4) = f(0, l_3, l_4) =?$
$v_3 = f(u_3, v_1, v_2) = f(1, v_1, v_2) =?$
$v_4 = f(u_4, v_2, v_3) = f(2, v_2, v_3) =?$
$v_5 = f(u_5, v_3, v_4) = f(0, v_3, v_4) =?$
$v_6 = f(u_6, v_4, v_5) = f(2, v_4, v_5) =?$

Analyzing the results obtained using the table of values of the function f, we obtain the following options for the text to be decoded ($f(1, *, *)$ and $f(0, *, *)$ take any values):

Table 4: Ciphertext values

v_1	v_2	v_3	v_4	v_5	v_6
0	0	$f(1,0,0) = 2$	$f(2,0,2) = 1$	$f(0,2,1) = 0$	$f(2,1,0) = 1$
0	1	$f(1,0,1) = 0$	$f(2,1,0) = 1$	$f(0,0,1) = 2$	$f(2,1,2) = 2$
1	0	$f(1,1,0) = 0$	$f(2,0,0) = 0$	$f(0,0,0) = 1$	$f(2,0,1) = 1$
1	1	$f(1,1,1) = 1$	$f(2,1,1) = 2$	$f(0,1,2) = 0$	$f(2,2,0) = 1$
2	0	$f(1,2,0) = 0$	$f(2,0,0) = 0$	$f(0,0,0) = 1$	$f(2,0,1) = 1$
0	2	$f(1,0,2) = 0$	$f(2,2,0) = 1$	$f(0,0,1) = 2$	$f(2,1,2) = 2$
2	1	$f(1,2,1) = 1$	$f(2,1,1) = 2$	$f(0,1,2) = 0$	$f(2,2,0) = 1$
1	2	$f(1,1,2) = 1$	$f(2,2,1) = 2$	$f(0,1,2) = 0$	$f(2,2,0) = 1$
2	2	$f(1,2,2) = 1$	$f(2,2,1) = 2$	$f(0,1,2) = 0$	$f(2,2,0) = 1$

We get 9 options for possible decrypted text. Among which the first option is true. The possible values of the ciphertext will be only 9 options, i.e. to determine the true value is not particularly difficult.

The question of identifying leaders in this case loses its relevance. Thus different sets of leaders for a ternary groupoid will be $9^2 = 81$. Essentially, we do not need to determine the exact values of the leaders.

The ciphertext proposed in Example 2.1 is a generalized version of the chiphertext used by M. Vojvoda for binary quasigroups.

In the following example we tried to improve this result.

Example 2.2. Enter the other text into the decryption device:
$q_1q_1q_1q_2q_2q_2q_3q_3q_3$
$q_2q_1q_1q_3q_2q_2q_1q_3q_3$
$q_1q_2q_1q_2q_3q_2q_3q_1q_3$
q_1q_1
or
000111222
100211022
010121202
00

We get the following decryption process:

Table 5: Decrypted text

$u_1 =^{(1,4)} f(0,0,2) = 1$	$u_{16} =^{(1,4)} f(0,1,1) = 0 - (5)$
$u_2 =^{(1,4)} f(0,1,2) = 0$	$u_{17} =^{(1,4)} f(2,1,0) = 0 - (22)$
$u_3 =^{(1,4)} f(0,0,0) = 2 - (1)$	$u_{18} =^{(1,4)} f(2,0,2) = 0 - (21)$
$u_4 =^{(1,4)} f(1,0,0) = 0 - (10)$	$u_{19} =^{(1,4)} f(0,2,2) = 0 - (9)$
$u_5 =^{(1,4)} f(1,0,1) = 2\text{-}(11)$	$u_{20} =^{(1,4)} f(1,2,0) = 2 - (16)$
$u_6 =^{(1,4)} f(1,1,1) = 1 - (14)$	$u_{21} =^{(1,4)} f(0,0,1) = 1 - (2)$
$u_7 =^{(1,4)} f(2,1,1) = 2 - (23)$	$u_{22} =^{(1,4)} f(1,1,0) = 2 - (13)$
$u_8 =^{(1,4)} f(2,1,2) = 2 - (24)$	$u_{23} =^{(1,4)} f(2,0,1) = 0 - (20)$
$u_9 =^{(1,4)} f(2,2,2) = 2 - (27)$	$u_{24} =^{(1,4)} f(1,1,2) = 1 - (15)$
$u_{10} =^{(1,4)} f(1,2,2) = 1 - (18)$	$u_{25} =^{(1,4)} f(2,2,1) = 2 - (26)$
$u_{11} =^{(1,4)} f(0,2,1) = 0 - (8)$	$u_{26} =^{(1,4)} f(0,1,2) = 0 - (6)$
$u_{12} =^{(1,4)} f(0,1,0) = 1 - (4)$	$u_{27} =^{(1,4)} f(2,2,0) = 0 - (25)$
$u_{13} =^{(1,4)} f(2,0,0) = 1 - (19)$	$u_{28} =^{(1,4)} f(0,0,2) = 1 - (3)$
$u_{14} =^{(1,4)} f(1,0,2) = 2 - (12)$	$u_{29} =^{(1,4)} f(0,2,0) = 1 - (7)$
$u_{15} =^{(1,4)} f(1,2,1) = 1 - (17)$	

At the output we get the following 29 characters:

10202122210112100002120120011.

Thus, for a complete reconstruction of the table of values of the operation ${}^{(1,4)}f$ it is enough to supply 28 characters (without the last one) for the ternary groupoid at the input, or 29 to restore all values. This text has the smallest possible length, i.e. is the best option for ternary case.

Let's see what happens in the 4-ary case.

Example 2.3. Take the 4-ary groupoid (R_3, f), $R_3 = \{0,1,2\}$, which is defined over residue ring modulo three $(R_3, +, \cdot)$ and which is invertible on the fourth place.

We define 4-ary operation f on the set R_3 in the following way:
$f(x_1, x_2, x_3, x_4) = \alpha x_1 + \beta x_2 + \gamma x_3 + \delta x_4 = x_5$, where

$$\begin{gathered}\alpha 0 = 1, \alpha 1 = 0, \alpha 2 = 2,\\ \beta 0 = 0, \beta 1 = 0, \beta 2 = 1,\\ \gamma 0 = 2, \gamma 1 = 1, \gamma 2 = 1,\\ \delta 0 = 2, \delta 1 = 0, \delta 2 = 1.\end{gathered}$$

The (45)-parastrophe for f is:

$${}^{(4,5)}f(x_1, x_2, x_3, x_5) = x_4 = \delta^{-1}(2 \cdot \alpha x_1 + 2 \cdot \beta x_2 + 2 \cdot \gamma x_3 + x_5),$$

where $\delta^{-1}(0) = 1, \delta^{-1}(1) = 2, \delta^{-1}(2) = 0$.
Check.

$f(x_1, x_2, x_3, {}^{(4,5)} f(x_1, x_2, x_3, x_5)) =$
$= \alpha x_1 + \beta x_2 + \gamma x_3 + \delta(\delta^{-1}(2 \cdot \alpha x_1 + 2 \cdot \beta x_2 + 2 \cdot \gamma x_3 + x_5)) =$
$= \alpha x_1 + \beta x_2 + \gamma x_3 + 2 \cdot \alpha x_1 + 2 \cdot \beta x_2 + 2 \cdot \gamma x_3 + x_5 = x_5$

$^{(4,5)}f(x_1, x_2, x_3, f(x_1, x_2, x_3, x_4)) =$
$= \delta^{-1}(2 \cdot \alpha x_1 + 2 \cdot \beta x_2 + 2 \cdot \gamma x_3 + \alpha x_1 + \beta x_2 + \gamma x_3 + \delta x_4) = \delta^{-1}(\delta x_4) = x_4.$

We propose the following elements:
$l_1 = 1, l_2 = 0, l_3 = 0, l_4 = 2, l_5 = 1, l_6 = 1, l_7 = 0, l_8 = 0, l_9 = 0$
as leader elements.

We will use Algorithm 1.2 and enter the following text into the decryption device:
00000001000200100011001200200021002 2
01000101010201100111011201200121012 2
02000201020202100211021202200221022 2
10001001100210101011101210201021102 2
11001101110211101111111211201121112 2
12001201120212101211121212201221122 2
20

In the table we give the values of the characters that allow us to determine the values of the $^{(4,5)}f$:

Table 6: Decrypted text (fragment)

$u_1 =^{(4,5)} f(l_1, l_2, l_3, v_1)$ $=^{(4,5)} f(1,0,0,0) = 2$	$u_{63} =^{(4,5)} f(2,0,1,2) = 0 - (60)$
$u_2 =^{(4,5)} f(l_4, l_5, l_6, v_2)$ $=^{(4,5)} f(2,1,1,0) = 1$	$u_{68} =^{(4,5)} f(0,1,2,1) = 0 - (17)$
$u_3 =^{(4,5)} f(l_7, l_8, l_9, v_3)$ $=^{(4,5)} f(0,0,0,0) = 1$	$u_{69} =^{(4,5)} f(1,2,1,0) = 2 - (49)$
$u_4 =^{(4,5)} f(v_1, v_2, v_3, v_4)$ $=^{(4,5)} f(0,0,0,0) = 1 - (1)$	$u_{70} =^{(4,5)} f(2,1,0,1) = 1 - (65)$
$u_8 =^{(4,5)} f(0,0,0,1) = 2 - (2)$	$u_{71} =^{(4,5)} f(1,0,1,2) = 2 - (33)$
$u_9 =^{(4,5)} f(0,0,1,0) = 2 - (4)$	$u_{72} =^{(4,5)} f(0,1,2,2) = 1 - (18)$
$u_{10} =^{(4,5)} f(0,1,0,0) = 1 - (10)$	$u_{73} =^{(4,5)} f(1,2,2,0) = 2 - (52)$
$u_{11} =^{(4,5)} f(1,0,0,0) = 2 - (28)$	$u_{74} =^{(4,5)} f(2,2,0,2) = 1 - (75)$
$u_{12} =^{(4,5)} f(0,0,0,2) = 0 - (3)$	$u_{75} =^{(4,5)} f(2,0,2,0) = 1 - (61)$
$u_{13} =^{(4,5)} f(0,0,2,0) = 2 - (7)$	$u_{84} =^{(4,5)} f(0,2,0,2) = 2 - (21)$
$u_{14} =^{(4,5)} f(0,2,0,0) = 0 - (19)$	$u_{87} =^{(4,5)} f(2,0,2,1) = 2 - (62)$
$u_{15} =^{(4,5)} f(2,0,0,1) = 1 - (56)$	$u_{92} =^{(4,5)} f(0,2,1,1) = 2 - (23)$
$u_{20} =^{(4,5)} f(0,0,1,1) = 0 - (5)$	$u_{93} =^{(4,5)} f(2,1,1,0) = 1 - (67)$
$u_{21} =^{(4,5)} f(0,1,1,0) = 2 - (13)$	$u_{94} =^{(4,5)} f(1,1,0,2) = 1 - (39)$
$u_{22} =^{(4,5)} f(1,1,0,0) = 2 - (37)$	$u_{95} =^{(4,5)} f(1,0,2,1) = 1 - (35)$
$u_{23} =^{(4,5)} f(1,0,0,1) = 0 - (29)$	$u_{96} =^{(4,5)} f(0,2,1,2) = 0 - (24)$
$u_{24} =^{(4,5)} f(0,0,1,2) = 1 - (6)$	$u_{97} =^{(4,5)} f(2,1,2,0) = 1 - (70)$
$u_{25} =^{(4,5)} f(0,1,2,0) = 2 - (16)$	$u_{98} =^{(4,5)} f(1,2,0,2) = 2 - (48)$
$u_{26} =^{(4,5)} f(1,2,0,0) = 1 - (46)$	$u_{99} =^{(4,5)} f(2,0,2,2) = 0 - (63)$

$u_{27} =^{(4,5)} f(2,0,0,2) = 2-(57)$	$u_{104} =^{(4,5)} f(0,2,2,1) = 2-(26)$
$u_{30} =^{(4,5)} f(2,0,0,0) = 0-(55)$	$u_{105} =^{(4,5)} f(2,2,1,0) = 0-(76)$
$u_{32} =^{(4,5)} f(0,0,2,1) = 0-(8)$	$u_{106} =^{(4,5)} f(2,1,0,2) = 2-(66)$
$u_{33} =^{(4,5)} f(0,2,1,0) = 1-(22)$	$u_{107} =^{(4,5)} f(1,0,2,2) = 2-(36)$
$u_{34} =^{(4,5)} f(2,1,0,0) = 0-(64)$	$u_{108} =^{(4,5)} f(0,2,2,2) = 0-(27)$
$u_{35} =^{(4,5)} f(1,0,0,2) = 1-(30)$	$u_{109} =^{(4,5)} f(2,2,2,1) = 1-(80)$
$u_{36} =^{(4,5)} f(0,0,2,2) = 1-(9)$	$u_{146} =^{(4,5)} f(2,2,1,1) = 1-(77)$
$u_{37} =^{(4,5)} f(0,2,2,0) = 1-(25)$	$u_{159} =^{(4,5)} f(2,1,1,1) = 2-(68)$
$u_{38} =^{(4,5)} f(2,2,0,1) = 0-(74)$	$u_{164} =^{(4,5)} f(1,1,1,1) = 1-(41)$
$u_{39} =^{(4,5)} f(2,0,1,0) = 1-(58)$	$u_{168} =^{(4,5)} f(1,1,1,2) = 2-(42)$
$u_{44} =^{(4,5)} f(0,1,0,1) = 2-(11)$	$u_{169} =^{(4,5)} f(1,1,2,1) = 1-(44)$
$u_{45} =^{(4,5)} f(1,0,1,0) = 0-(31)$	$u_{170} =^{(4,5)} f(1,2,1,1) = 0-(50)$
$u_{48} =^{(4,5)} f(0,1,0,2) = 0-(12)$	$u_{171} =^{(4,5)} f(2,1,1,2) = 0-(69)$
$u_{49} =^{(4,5)} f(1,0,2,0) = 0-(34)$	$u_{180} =^{(4,5)} f(1,1,2,2) = 2-(45)$
$u_{50} =^{(4,5)} f(0,2,0,1) = 1-(20)$	$u_{181} =^{(4,5)} f(1,2,2,1) = 0-(53)$
$u_{51} =^{(4,5)} f(2,0,1,10) = 2-(59)$	$u_{182} =^{(4,5)} f(2,2,1,2) = 2-(78)$
$u_{56} =^{(4,5)} f(0,1,1,1) = 0-(14)$	$u_{195} =^{(4,5)} f(2,1,2,1) = 0-(71)$
$u_{57} =^{(4,5)} f(1,1,1,0) = 0-(40)$	$u_{204} =^{(4,5)} f(1,2,1,2) = 1-(51)$
$u_{58} =^{(4,5)} f(1,1,0,1) = 0-(38)$	$u_{207} =^{(4,5)} f(2,1,2,2) = 2-(72)$
$u_{59} =^{(4,5)} f(1,0,1,1) = 1-(32)$	$u_{216} =^{(4,5)} f(1,2,2,2) = 1-(54)$
$u_{60} =^{(4,5)} f(0,1,1,2) = 1-(15)$	$u_{217} =^{(4,5)} f(2,2,2,2) = 2-(81)$
$u_{61} =^{(4,5)} f(1,1,2,0) = 0-(43)$	$u_{218} =^{(4,5)} f(2,2,2,0) = 0-(79)$
$u_{62} =^{(4,5)} f(1,2,0,1) = 2-(47)$	

At the output we get 218 characters.Thus the table of the decrypting function is hacked.

Table 7: Decryption function

N	Value	N	Value	N	Value
(1)	${}^{(4,5)}f(0,0,0,0) = 1$	(28)	${}^{(4,5)}f(1,0,0,0) = 2$	(55)	${}^{(4,5)}f(2,0,0,0) = 0$
(2)	${}^{(4,5)}f(0,0,0,1) = 2$	(29)	${}^{(4,5)}f(1,0,0,1) = 0$	(56)	${}^{(4,5)}f(2,0,0,1) = 1$
(3)	${}^{(4,5)}f(0,0,0,2) = 0$	(30)	${}^{(4,5)}f(1,0,0,2) = 1$	(57)	${}^{(4,5)}f(2,0,0,2) = 2$
(4)	${}^{(4,5)}f(0,0,1,0) = 2$	(31)	${}^{(4,5)}f(1,0,1,0) = 0$	(58)	${}^{(4,5)}f(2,0,1,0) = 1$
(5)	${}^{(4,5)}f(0,0,1,1) = 0$	(32)	${}^{(4,5)}f(1,0,1,1) = 1$	(59)	${}^{(4,5)}f(2,0,1,1) = 2$
(6)	${}^{(4,5)}f(0,0,1,2) = 1$	(33)	${}^{(4,5)}f(1,0,1,2) = 2$	(60)	${}^{(4,5)}f(2,0,1,2) = 0$
(7)	${}^{(4,5)}f(0,0,2,0) = 2$	(34)	${}^{(4,5)}f(1,0,2,0) = 0$	(61)	${}^{(4,5)}f(2,0,2,0) = 1$
(8)	${}^{(4,5)}f(0,0,2,1) = 0$	(35)	${}^{(4,5)}f(1,0,2,1) = 1$	(62)	${}^{(4,5)}f(2,0,2,1) = 2$
(9)	${}^{(4,5)}f(0,0,2,2) = 1$	(36)	${}^{(4,5)}f(1,0,2,2) = 2$	(63)	${}^{(4,5)}f(2,0,2,2) = 0$
(10)	${}^{(4,5)}f(0,1,0,0) = 1$	(37)	${}^{(4,5)}f(1,1,0,0) = 2$	(64)	${}^{(4,5)}f(2,1,0,0) = 0$
(11)	${}^{(4,5)}f(0,1,0,1) = 2$	(38)	${}^{(4,5)}f(1,1,0,1) = 0$	(65)	${}^{(4,5)}f(2,1,0,1) = 1$
(12)	${}^{(4,5)}f(0,1,0,2) = 0$	(39)	${}^{(4,5)}f(1,1,0,2) = 1$	(66)	${}^{(4,5)}f(2,1,0,2) = 2$

(13)	${}^{(4,5)}f(0,1,1,0)=2$	(40)	${}^{(4,5)}f(1,1,1,0)=0$	(67)	${}^{(4,5)}f(2,1,1,0)=1$
(14)	${}^{(4,5)}f(0,1,1,1)=0$	(41)	${}^{(4,5)}f(1,1,1,1)=1$	(68)	${}^{(4,5)}f(2,1,1,1)=2$
(15)	${}^{(4,5)}f(0,1,1,2)=1$	(42)	${}^{(4,5)}f(1,1,1,2)=2$	(69)	${}^{(4,5)}f(2,1,1,2)=0$
(16)	${}^{(4,5)}f(0,1,2,0)=2$	(43)	${}^{(4,5)}f(1,1,2,0)=0$	(70)	${}^{(4,5)}f(2,1,2,0)=1$
(17)	${}^{(4,5)}f(0,1,2,1)=0$	(44)	${}^{(4,5)}f(1,1,2,1)=1$	(71)	${}^{(4,5)}f(2,1,2,1)=0$
(18)	${}^{(4,5)}f(0,1,2,2)=1$	(45)	${}^{(4,5)}f(1,1,2,2)=2$	(72)	${}^{(4,5)}f(2,1,2,2)=2$
(19)	${}^{(4,5)}f(0,2,0,0)=0$	(46)	${}^{(4,5)}f(1,2,0,0)=1$	(73)	${}^{(4,5)}f(2,2,0,0)=2$
(20)	${}^{(4,5)}f(0,2,0,1)=1$	(47)	${}^{(4,5)}f(1,2,0,1)=2$	(74)	${}^{(4,5)}f(2,2,0,1)=0$
(21)	${}^{(4,5)}f(0,2,0,2)=2$	(48)	${}^{(4,5)}f(1,2,0,2)=0$	(75)	${}^{(4,5)}f(2,2,0,2)=1$
(22)	${}^{(4,5)}f(0,2,1,0)=1$	(49)	${}^{(4,5)}f(1,2,1,0)=2$	(76)	${}^{(4,5)}f(2,2,1,0)=0$
(23)	${}^{(4,5)}f(0,2,1,1)=2$	(50)	${}^{(4,5)}f(1,2,1,1)=0$	(77)	${}^{(4,5)}f(2,2,1,1)=1$
(24)	${}^{(4,5)}f(0,2,1,2)=0$	(51)	${}^{(4,5)}f(1,2,1,2)=1$	(78)	${}^{(4,5)}f(2,2,1,2)=2$
(25)	${}^{(4,5)}f(0,2,2,0)=1$	(52)	${}^{(4,5)}f(1,2,2,0)=2$	(79)	${}^{(4,5)}f(2,2,2,0)=0$
(26)	${}^{(4,5)}f(0,2,2,1)=2$	(53)	${}^{(4,5)}f(1,2,2,1)=0$	(80)	${}^{(4,5)}f(2,2,2,1)=1$
(27)	${}^{(4,5)}f(0,2,2,2)=0$	(54)	${}^{(4,5)}f(1,2,2,2)=1$	(81)	${}^{(4,5)}f(2,2,2,2)=2$

Thus, for a complete reconstruction of the table of values of the operation ${}^{(4,5)}f$, and hence the table of values of the operation f it is sufficient to supply 218 (or 217) characters for the 4-ary groupoid at the input.

Knowing Cayley table for operation ${}^{(4,5)}f$, we easily restored the operation f:

Table 8: Encryption function

N	Value	N	Value	N	Value
(1)	$f(0,0,0,0)=2$	(28)	$f(1,0,0,0)=1$	(55)	$f(2,0,0,0)=0$
(2)	$f(0,0,0,1)=0$	(29)	$f(1,0,0,1)=2$	(56)	$f(2,0,0,1)=1$
(3)	$f(0,0,0,2)=1$	(30)	$f(1,0,0,2)=0$	(57)	$f(2,0,0,2)=2$
(4)	$f(0,0,1,0)=1$	(31)	$f(1,0,1,0)=0$	(58)	$f(2,0,1,0)=2$
(5)	$f(0,0,1,1)=2$	(32)	$f(1,0,1,1)=1$	(59)	$f(2,0,1,1)=0$
(6)	$f(0,0,1,2)=0$	(33)	$f(1,0,1,2)=2$	(60)	$f(2,0,1,2)=1$
(7)	$f(0,0,2,0)=1$	(34)	$f(1,0,2,0)=0$	(61)	$f(2,0,2,0)=2$
(8)	$f(0,0,2,1)=2$	(35)	$f(1,0,2,1)=1$	(62)	$f(2,0,2,1)=0$
(9)	$f(0,0,2,2)=0$	(36)	$f(1,0,2,2)=2$	(63)	$f(2,0,2,2)=1$
(10)	$f(0,1,0,0)=2$	(37)	$f(1,1,0,0)=1$	(64)	$f(2,1,0,0)=0$
(11)	$f(0,1,0,1)=0$	(38)	$f(1,1,0,1)=2$	(65)	$f(2,1,0,1)=1$
(12)	$f(0,1,0,2)=1$	(39)	$f(1,1,0,2)=0$	(66)	$f(2,1,0,2)=2$
(13)	$f(0,1,1,0)=1$	(40)	$f(1,1,1,0)=0$	(67)	$f(2,1,1,0)=2$
(14)	$f(0,1,1,1)=2$	(41)	$f(1,1,1,1)=1$	(68)	$f(2,1,1,1)=0$
(15)	$f(0,1,1,2)=0$	(42)	$f(1,1,1,2)=2$	(69)	$f(2,1,1,2)=1$
(16)	$f(0,1,2,0)=1$	(43)	$f(1,1,2,0)=0$	(70)	$f(2,1,2,0)=2$
(17)	$f(0,1,2,1)=2$	(44)	$f(1,1,2,1)=1$	(71)	$f(2,1,2,1)=0$
(18)	$f(0,1,2,2)=0$	(45)	$f(1,1,2,2)=2$	(72)	$f(2,1,2,2)=1$

(19)	$f(0,2,0,0)=0$	(46)	$f(1,2,0,0)=2$	(73)	$f(2,2,0,0)=1$
(20)	$f(0,2,0,1)=1$	(47)	$f(1,2,0,1)=0$	(74)	$f(2,2,0,1)=2$
(21)	$f(0,2,0,2)=2$	(48)	$f(1,2,0,2)=1$	(75)	$f(2,2,0,2)=0$
(22)	$f(0,2,1,0)=2$	(49)	$f(1,2,1,0)=1$	(76)	$f(2,2,1,0)=0$
(23)	$f(0,2,1,1)=0$	(50)	$f(1,2,1,1)=2$	(77)	$f(2,2,1,1)=1$
(24)	$f(0,2,1,2)=1$	(51)	$f(1,2,1,2)=0$	(78)	$f(2,2,1,2)=2$
(25)	$f(0,2,2,0)=2$	(52)	$f(1,2,2,0)=1$	(79)	$f(2,2,2,0)=0$
(26)	$f(0,2,2,1)=0$	(53)	$f(1,2,2,1)=2$	(80)	$f(2,2,2,1)=1$
(27)	$f(0,2,2,2)=1$	(54)	$f(1,2,2,2)=0$	(81)	$f(2,2,2,2)=2$

Currently, we are looking for the type of text of minimum length for a 4-ary groupoid.

To understand the situation with burglary of the decrypted text and the leaders, consider the plaintext of the form: 101202$=u_1u_2u_3u_4u_5u_6$. For this text we have:

$v_1 = f(l_1,l_2,l_3,u_1) = f(l_1,l_2,l_3,1) =?$
$v_2 = f(l_4,l_5,l_6,u_2) = f(l_4,l_5,l_6,0) =?$
$v_3 = f(l_7,l_8,l_9,u_3) = f(l_7,l_8,l_9,1) =?$
$v_4 = f(v_1,v_2,v_3,u_4) = f(v_1,v_2,v_3,2) =?$
$v_5 = f(v_2,v_3,v_4,u_5) = f(v_2,v_3,v_4,0) =?$
$v_6 = f(v_3,v_4,v_5,u_6) = f(v_3,v_4,v_5,2) =?$

Analyzing the results obtained using the table of values of the function f, we obtain the following: $f(*,*,*,1)$ and $f(*,*,*,2)$ take any values.

Table 9: Ciphertext values

v_1	v_2	v_3	v_4	v_5	v_6
0	0	0	$f(0,0,0,2)=1$	$f(0,0,1,0)=1$	$f(0,1,0,2)=1$
0	0	1	$f(0,0,1,2)=0$	$f(0,0,0,0)=2$	$f(0,0,2,2)=0$
0	0	2	$f(0,0,2,2)=0$	$f(0,2,2,0)=2$	$f(2,0,2,2)=1$
0	1	0	$f(0,1,0,2)=1$	$f(1,0,1,0)=0$	$f(0,1,0,2)=1$
0	1	1	$f(0,1,1,2)=0$	$f(1,1,0,0)=1$	$f(1,0,1,2)=2$
0	1	2	$f(0,1,2,2)=0$	$f(1,2,0,0)=2$	$f(2,0,2,2)=1$
0	2	0	$f(0,2,0,2)=2$	$f(2,0,2,0)=2$	$f(0,2,2,2)=1$
0	2	1	$f(0,2,1,2)=1$	$f(2,1,1,0)=2$	$f(1,1,2,2)=2$
0	2	2	$f(0,2,2,2)=1$	$f(2,2,1,0)=0$	$f(2,1,0,2)=2$
1	0	0	$f(1,0,0,2)=0$	$f(0,0,0,0)=2$	$f(0,0,2,2)=0$
1	0	1	$f(1,0,1,2)=2$	$f(0,1,2,0)=1$	$f(1,2,1,2)=0$
1	0	2	$f(1,0,2,2)=2$	$f(0,2,2,0)=2$	$f(2,2,2,2)=2$
1	1	0	$f(1,1,0,2)=0$	$f(1,0,0,0)=1$	$f(0,0,1,2)=0$
1	1	1	$f(1,1,1,2)=2$	$f(1,1,2,0)=0$	$f(1,2,0,2)=1$

1	1	2	$f(1,1,2,2)=2$	$f(1,2,2,0)=1$	$f(2,2,1,2)=2$
1	2	0	$f(1,2,0,2)=1$	$f(2,0,1,0)=2$	$f(0,1,2,2)=0$
1	2	1	$f(1,2,1,2)=0$	$f(2,1,0,0)=0$	$f(1,0,0,2)=0$
1	2	2	$f(1,2,2,2)=0$	$f(2,2,0,0)=1$	$f(2,0,1,2)=1$
2	0	0	$f(2,0,0,2)=2$	$f(0,0,2,0)=1$	$f(0,2,1,2)=1$
2	0	1	$f(2,0,1,2)=1$	$f(0,1,1,0)=1$	$f(1,1,1,2)=2$
2	0	2	$f(2,0,2,2)=1$	$f(0,2,1,0)=2$	$f(2,1,2,2)=1$
2	1	0	$f(2,1,0,2)=2$	$f(1,0,2,0)=0$	$f(0,2,0,2)=2$
2	1	1	$f(2,1,1,2)=1$	$f(1,1,1,0)=0$	$f(1,1,0,2)=0$
2	1	2	$f(2,1,2,2)=1$	$f(1,2,1,0)=1$	$f(2,1,1,2)=1$
2	2	0	$f(2,2,0,2)=0$	$f(2,0,0,0)=0$	$f(0,0,0,2)=1$
2	2	1	$f(2,2,1,2)=2$	$f(2,1,2,0)=2$	$f(1,2,2,2)=0$
2	2	2	$f(2,2,2,2)=2$	$f(2,2,2,0)=0$	$f(2,2,0,2)=0$

We get 27 options for possible decrypted text, among which the 25-th option is true.

Thus, we confirmed the result that for an n-ary groupoid, the required number of characters is: $(n \cdot m^{n-1}+1)(m-1)$ characters to get all the values or $n \cdot m^{n-1}(m-1)+(m-2)$ characters, when the last value is found by the exception method.

So the minimum number of characters in a modified attack will be: $m^n+(n-1)$.

The main question is the choice of text of minimum length for groupoids of different arity and order.

2.2 Plaintext attacks

Consider an attack with the plaintext constructed using an n-ary groupoid, which is invertible on the i-th place obtained using the generalized Markovski algorithm.

Assume the cryptanalyst has access to the encryption device loaded with the key. He can then construct the following plaintext:

$$
\begin{aligned}
&q_1q_1\dots q_1q_1q_1q_1\dots q_1q_2q_1q_1\dots q_1q_m\\
&q_1q_1\dots q_2q_1q_1q_1\dots q_2q_2q_1q_1\dots q_2q_m\\
&q_1q_1\dots q_3q_1q_1q_1\dots q_3q_2q_1q_1\dots q_3q_m\\
&\dots\dots\dots\dots\\
&q_1q_1\dots q_mq_1q_1q_1\dots q_mq_2q_1q_1\dots q_mq_m\dots
\end{aligned}
$$

and enter it into the encryption device.

The number of characters required to restore the encryption table depends on the values of the selected leaders. Therefore, the question of determining the length of the plaintext used remains open.

Example 2.4. We consider the plaintext attack for the Example 2.1 and we chose the following plaintext:

$q_1q_1q_1q_1q_1q_2q_1q_1q_3q_1q_2q_1q_1q_2q_2q_1q_2q_3q_1q_3q_1q_1q_3q_2q_1q_3q_3$
$q_2q_1q_1q_2q_1q_2q_2q_1q_3q_2q_2q_1q_2q_2q_2q_2q_3q_2q_3q_1q_2q_3q_2q_2q_3q_3$
$q_3q_1q_1q_3q_1q_2q_3q_1q_3q_3q_2q_1q_3q_2q_2q_3q_2q_3q_3q_3q_1q_3q_3q_2q_3q_3q_3$
or
00000100201001101202002102 2
10010110211011111212012112 2
20020120221021121222022122 2

The process of encrypting the text and the results are as follows:

Table 10: Encrypted text

$v_1 = f(u_1, l_1, l_2) = f(q_1, l_1, l_2)$ $= f(0, 0, 2) = 2$	$v_{42} = f(1, 0, 2) = 0$
$v_2 = f(u_2, l_3, l_4) = f(q_1, l_3, l_4)$ $= f(0, 1, 2) = 0$	$v_{43} = f(1, 2, 0) = 0$
$v_3 = f(u_3, v_1, v_2) = f(q_1, v_1, v_2)$ $= f(0, 2, 0) = 2 - (7)$	$v_{44} = f(1, 0, 0) = 2$
$v_4 = f(u_4, v_2, v_3) = f(0, 0, 2) = 2 - (3)$	$v_{45} = f(2, 0, 2) = 1$
$v_5 = f(0, 2, 2) = 0 - (9)$	$v_{46} = f(1, 2, 1) = 1$
$v_6 = f(1, 2, 0) = 0 - (16)$	$v_{47} = f(2, 1, 1) = 2 - (23)$
$v_7 = f(0, 0, 0) = 1 - (1)$	$v_{48} = f(0, 1, 2) = 0 - (6)$
$v_8 = f(0, 0, 1) = 2 - (24)$	$v_{49} = f(1, 2, 0) = 0$
$v_9 = f(2, 1, 2) = 2 - (24)$	$v_{50} = f(2, 0, 0) = 0$
$v_{10} = f(0, 2, 2) = 0$	$v_{51} = f(1, 0, 0) = 2$
$v_{11} = f(1, 2, 0) = 0$	$v_{52} = f(1, 0, 2) = 0$
$v_{12} = f(0, 0, 0) = 1$	$v_{53} = f(2, 2, 0) = 1 - (25)$
$v_{13} = f(0, 0, 1) = 2$	$v_{54} = f(2, 0, 1) = 1$
$v_{14} = f(1, 1, 2) = 1 - (15)$	$v_{55} = f(2, 1, 1) = 2$
$v_{15} = f(1, 2, 1) = 1 - (17)$	$v_{56} = f(0, 1, 2) = 0$
$v_{16} = f(0, 1, 1) = 0 - (5)$	$v_{57} = f(0, 2, 0) = 2$
$v_{17} = f(1, 1, 0) = 0 - (13)$	$v_{58} = f(2, 0, 2) = 1$
$v_{18} = f(2, 0, 0) = 0 - (19)$	$v_{59} = f(0, 2, 1) = 0 - (8)$
$v_{19} = (0, 0, 0) = 1$	$v_{60} = f(1, 1, 0) = 0$
$v_{20} = f(2, 0, 1) = 1 - (20)$	$v_{61} = f(2, 0, 0) = 0$
$v_{21} = f(0, 0, 1) = 0$	$v_{62} = f(0, 0, 0) = 1$
$v_{22} = f(0, 1, 0) = 2 - (4)$	$v_{63} = f(2, 0, 1) = 1$
$v_{23} = f(2, 0, 2) = 1 - (21)$	$v_{64} = f(2, 1, 1) = 2$
$v_{24} = f(1, 2, 1) = 1$	$v_{65} = f(1, 1, 2) = 1$
$v_{25} = f(0, 1, 1) = 0$	$v_{66} = f(0, 2, 1) = 0$
$v_{26} = f(2, 1, 0) = 1 - (22)$	$v_{67} = f(2, 1, 0) = 1$
$v_{27} = f(2, 0, 1) = 1$	$v_{68} = f(1, 0, 1) = 0 - (11)$
$v_{28} = f(1, 1, 1) = 1 - (14)$	$v_{69} = f(1, 1, 0) = 0$
$v_{29} = f(0, 1, 1) = 0$	$v_{70} = f(2, 0, 0) = 0$

$v_{30} = f(0,1,0) = 2$	$v_{71} = f(1,0,0) = 2$
$v_{31} = f(1,0,2) = 0 - (12)$	$v_{72} = f(2,0,2) = 1$
$v_{32} = f(0,2,0) = 2$	$v_{73} = f(2,2,1) = 2 - (26)$
$v_{33} = f(1,0,2) = 0$	$v_{74} = f(2,1,2) = 2$
$v_{34} = f(1,2,0) = 0$	$v_{75} = f(0,2,2) = 0$
$v_{35} = f(0,0,0) = 1$	$v_{76} = f(2,2,0) = 1$
$v_{36} = f(2,0,1) = 1$	$v_{77} = f(2,0,1) = 1$
$v_{37} = f(1,1,1) = 1$	$v_{78} = f(1,1,1) = 1$
$v_{38} = f(1,1,1) = 1$	$v_{79} = f(2,1,1) = 2$
$v_{39} = f(0,1,1) = 0$	$v_{80} = f(2,1,2) = 2$
$v_{40} = f(1,1,0) = 0$	$v_{81} = f(2,2,2) = 2 - (27)$
$v_{41} = f(1,0,0) = 2 - (10)$	

At the output of the encryption device, we get the following 81 characters:
202200122001211000110211011102020011110020021120002011202100011210100021220111222.

These characters will be enough to restore the table of values of the function f (Table 3). Knowing Cayley table for operation f, we easily restored the operation ${}^{(1,4)}f$ (Table 2).

Take some encrypted text and try to crack it. For example, we have the following ciphertext: 002101$=v_1v_2v_3v_4v_5v_6$. Then we have:

$u_1 =^{(1,4)} f(v_1,l_1,l_2) = (0,l_1,l_2) =? \Rightarrow u_1 =?$
$u_2 =^{(1,4)} f(v_2,l_3,l_4) =^{(1,4)} f(0,l_3,l_4) =? \Rightarrow u_2 =?$
$u_3 =^{(1,4)} f(v_3,v_1,v_2) =^{(1,4)} f(2,0,0) = 1 \Rightarrow u_3 = 1,$
$u_4 =^{(1,4)} f(v_4,v_2,v_3) =^{(1,4)} f(1,0,2) = 2 \Rightarrow u_4 = 2,$
$u_5 =^{(1,4)} f(v_5,v_3,v_4) =^{(1,4)} f(0,2,1) = 0 \Rightarrow u_5 = 0,$
$u_6 =^{(1,4)} f(v_6,v_4,v_5) =^{(1,4)} f(1,1,0) = 2 \Rightarrow u_6 = 2.$

Analyzing the results obtained using the table of values of the function f, we obtain the following: $f(0,*,*)$ takes any values. The possible values of the ciphertext will be only of 9 options:

Table 11: Plaintext values

u_1	u_2	u_3	u_4	u_5	u_6
0	0	1	2	0	2
0	1	1	2	0	2
1	0	1	2	0	2
1	1	1	2	0	2
2	0	1	2	0	2
0	2	1	2	0	2
2	1	1	2	0	2
1	2	1	2	0	2

2	2	1	2	0	2

Among them only the third option is correct.

For an n-ary groupoid in plaintext of length k, the first $(n-1)$ characters are not cracked. The rest are unequivocally.

Example 2.5. We consider the plaintext attack for the Example 2.3 and we chose the following plaintext:
00000001000200100011001200200021002 2
01000101010201100111011201200121012 2
02000201020202100211021202200221022 2
10001001100210101011101210201021102 2
11001101110211101111111211201121112 2
12001201120212101211121212201221122 2
20002001200220102011201220202021202 2
21002101210221102111211221202121212 2
22002201220222102211221222202221222 2
0000000100020010

The process of encrypting the text and the results are as follows:

Table 12: Encrypted (fragment)

$v_4 = f(1,2,2,0) = 1-(52)$	$v_{86} = f(1,2,0,2) = 1-(48)$
$v_5 = f(2,2,1,0) = 0-(76)$	$v_{93} = f(2,0,1,0) = 2-(58)$
$v_6 = f(2,1,0,0) = 0-(64)$	$v_{94} = f(0,1,2,2) = 0-(18)$
$v_7 = f(1,0,0,0) = 1-(28)$	$v_{96} = f(2,0,0,2) = 2-(57)$
$v_8 = f(0,0,1,1) = 2-(5)$	$v_{97} = f(0,0,2,0) = 1-(7)$
$v_9 = f(0,1,2,0) = 1-(16)$	$v_{98} = f(0,2,1,2) = 1-(24)$
$v_{10} = f(1,2,1,0) = 1-(49)$	$v_{99} = f(2,1,1,2) = 1-(69)$
$v_{11} = f(2,1,1,0) = 2-(67)$	$v_{101} = f(1,1,0,0) = 1-(37)$
$v_{12} = f(1,1,2,2) = 2-(45)$	$v_{102} = f(1,0,1,2) = 2-(33)$
$v_{15} = f(2,1,0,1) = 1-(65)$	$v_{109} = f(1,0,1,1) = 1-(32)$
$v_{16} = f(1,0,1,0) = 0-(31)$	$v_{116} = f(1,1,0,1) = 2-(38)$
$v_{17} = f(0,1,0,0) = 2-(10)$	$v_{117} = f(1,0,2,1) = 1-(35)$
$v_{18} = f(1,0,2,0) = 0-(34)$	$v_{118} = f(0,2,1,0) = 2-(22)$
$v_{19} = f(0,2,0,1) = 1-(20)$	$v_{119} = f(2,1,2,0) = 2-(70)$
$v_{20} = f(2,0,1,1) = 0-(59)$	$v_{121} = f(2,2,0,1) = 2-(74)$
$v_{24} = f(2,0,1,2) = 1-(60)$	$v_{128} = f(0,2,1,1) = 0-(23)$
$v_{25} = f(0,1,1,0) = 1-(13)$	$v_{131} = f(0,1,0,1) = 0-(11)$
$v_{26} = f(1,1,1,0) = 0-(40)$	$v_{132} = f(1,0,0,2) = 0-(30)$
$v_{27} = (1,1,0,2) = 0-(39)$	$v_{133} = f(0,0,0,1) = 0-(2)$
$v_{29} = f(0,0,1,0) = 1-(4)$	$v_{134} = f(0,0,0,0) = 2-(1)$

$v_{31} = f(1,1,1,2) = 2-(42)$	$v_{135} = f(0,0,2,2) = 0-(9)$
$v_{32} = f(1,1,2,1) = 1-(44)$	$v_{139} = f(0,1,1,2) = 0-(15)$
$v_{36} = f(1,2,2,2) = 0-(54)$	$v_{143} = f(2,1,2,2) = 1-(72)$
$v_{37} = f(2,2,0,0) = 1-(73)$	$v_{144} = f(1,2,1,2) = 0-(51)$
$v_{41} = f(0,2,0,0) = 0-(19)$	$v_{161} = f(1,0,0,1) = 2-(29)$
$v_{42} = f(2,0,0,1) = 1-(56)$	$v_{162} = f(0,0,2,1) = 2-(8)$
$v_{44} = f(0,1,1,1) = 2-(14)$	$v_{173} = f(2,2,1,1) = 1-(77)$
$v_{45} = f(1,1,2,0) = 0-(43)$	$v_{174} = f(2,1,1,1) = 0-(68)$
$v_{46} = f(1,2,0,1) = 0-(47)$	$v_{179} = f(2,2,0,2) = 0-(75)$
$v_{47} = f(2,0,0,0) = 0-(55)$	$v_{182} = f(0,2,2,2) = 1-(27)$
$v_{48} = f(0,0,0,2) = 1-(3)$	$v_{192} = f(2,0,2,2) = 1-(63)$
$v_{55} = f(1,2,1,1) = 2-(50)$	$v_{194} = f(2,1,0,2) = 2-(66)$
$v_{56} = f(2,1,2,1) = 0-(71)$	$v_{212} = f(0,1,2,1) = 2-(17)$
$v_{57} = f(1,2,0,0) = 2-(46)$	$v_{213} = f(1,2,2,1) = 2-(53)$
$v_{58} = f(2,0,2,1) = 0-(62)$	$v_{214} = f(2,2,2,2) = 2-(81)$
$v_{62} = f(1,1,1,1) = 1-(41)$	$v_{218} = f(2,2,2,0) = 0-(79)$
$v_{67} = f(0,2,0,2) = 2-(21)$	$v_{227} = f(0,0,0,0) = 2-(1)$
$v_{71} = f(0,0,1,2) = 0-(6)$	$v_{288} = f(1,0,2,2) = 2-(36)$
$v_{72} = f(0,1,0,2) = 1-(12)$	$v_{290} = f(2,2,1,2) = 2-(78)$
$v_{79} = f(2,0,2,0) = 2-(61)$	$v_{338} = f(0,2,2,0) = 2-(25)$
$v_{80} = f(0,2,2,1) = 0-(26)$	$v_{339} = f(2,2,2,1) = 1-(80)$

At the output of the encryption device we get 339 characters.They will be enough to restore the table of values of the function f (Table 8). Knowing Cayley table for the operation f, we easily restored the operation ${}^{(4,5)}f$ (Table 7).

Take some encrypted text and try to crack it. For example, we have the following ciphertext: 220001$=v_1v_2v_3v_4v_5v_6$. Then we have:

$u_1 =^{(4,5)} f(l_1,l_2,l_3,v_1,) =^{(4,5)} f(l_1,l_2,l_3,2) =? \Rightarrow u_1 =?$
$u_2 =^{(4,5)} f(l_4,l_5,l_6,v_2,) =^{(4,5)} f(l_4,l_5,l_6,2) =? \Rightarrow u_2 =?$
$u_3 =^{(4,5)} f(l_7,l_8,l_9,v_3) =^{(4,5)} f(l_7,l_8,l_9,0) =? \Rightarrow u_3 =?$
$u_4 =^{(4,5)} f(v_1,v_2,v_3,v_4) =^{(4,5)} f(2,2,0,0) = 2 \Rightarrow u_4 = 2,$
$u_5 =^{(4,5)} f(v_2,v_3,v_4,v_5) =^{(4,5)} f(2,0,0,0) = 0 \Rightarrow u_5 = 0,$
$u_6 =^{(4,5)} f(v_3,v_4,v_5,v_6) =^{(4,5)} f(0,0,0,1) = 2 \Rightarrow u_6 = 2.$

Analyzing the results obtained using the table of values of the function ${}^{(4,5)}f$, we obtain the following: $f(*,*,*,2)$ and $f(*,*,*,0)$ take any values.The possible values of the ciphertext will be 27 options:

Table 13: Plaintext values

u_1	u_2	u_3	u_4	u_5	u_6
0	0	0	2	0	2
0	0	1	2	0	2

0	0	2	2	0	2
0	1	0	2	0	2
0	1	1	2	0	2
0	1	2	2	0	2
0	2	0	2	0	2
0	2	1	2	0	2
0	2	2	2	0	2
1	0	0	2	0	2
1	0	1	2	0	2
1	0	2	2	0	2
1	1	0	2	0	2
1	1	1	2	0	2
1	1	2	2	0	2
1	2	0	2	0	2
1	2	1	2	0	2
1	2	2	2	0	2
2	0	0	2	0	2
2	0	1	2	0	2
2	0	2	2	0	2
2	1	0	2	0	2
2	1	1	2	0	2
2	1	2	2	0	2
2	2	0	2	0	2
2	2	1	2	0	2
2	2	2	2	0	2

Among them the 11th option is correct.

3. Conclusion

A cryptanalysis is done on cipher and there are analyzed cryptoattacks, built by M. Vojvoda for quasigroups, chosen ciphertext and plaintext.

In this article, we looked at some types of attacks on the Markovski cipher with the help of open and encrypted texts.

Thus, for a complete reconstruction of the table of values of the operation ${}^{(i,n+1)})f$ and hence, the table of values of the operation f using cryptotext attack, it is sufficient to submit at the input: $A = (n \cdot m^{n-1} + 1)(m-1)$ characters to get all the values.

The minimum number of characters in a modified cryptotext attack will be $m^n + (n-1)$ symbols, where n is arity and m the order of an i-invertible groupoid. As for the plaintext attack, it was possible to establish the lower limit value of the necessary characters to restore the table of the values of function f.

But the following question remains. What kind of text to give at the input of the encrypting device so as not to exceed the received limit of characters and will it always be possible?

We plan to continue attacks on the cipher built with the help of generalized Markovski algorithms on i-invertible groupoids.

Acknowledgement. The author thanks Referee for his helpful comments.

References

[1] **P. Csorgo, V.A. Shcherbacov**, *On some quasigroup cryptographical primitives*, arXiv:1110.6591, 11 pages.

[2] **N.N. Malyutina, A.V. Scerbacova, V.A. Shcherbacov**, *Markovsky algorithm on i-invertibile groupoids*, arXiv:1806.02267, 3 pages.

[3] **S. Markovski, D. Gligoroski, S. Andova**, *Using quasigroups for one-one secure encoding*, Proc. VIII Conf. Logic and Computer Science "LIRA'97", Novi Sad, 1997, 157–167.

[4] **E. Ochodková, V. Snashel**, *Using quasigroups for secure encoding of file system*, Proc. Intern. Sci. NATO PfP/PWP Conf. "Security and Information Protection 2001", Brno, Czech Republic, 175–181.

[5] **V.A. Shcherbacov, N.N. Malyutina**, *Role of quasigroups in cryptosystems. Generalization of Markovski algorithm*, Bull. Transnistrian Univ., **60** (2018), no.3, 53–57.

[6] **M. Vojvoda**, *Cryptanalysis of a file encoding system based on quasigroup*, J. Electr. Engineering, **54** (2003), No. 12/S, 69–71.

[7] **M. Vojvoda**, *Stream ciphers and hash functions – analysis of some new design approaches*, PhD thesis, Slovak University of Technology, July, 2004.

Received March 15, 2019
Revised February 25, 2020

Department of Mathematics
State University Dimitrie Cantemir
Academiei str. 3/2
MD-2028 Chişinău
Moldova
E-mail: 231003.Bab.Nadezhda@mail.ru

Quasigroups and Related Systems **28** (2020), 269 – 284

An enhanced version of the hidden discrete logarithm problem and its algebraic support

Dmitriy N. Moldovyan, Alexandr A. Moldovyan, Nikolay A. Moldovyan

Abstract. A new approach is proposed to the development of the signature schemes based on the computational difficulty of the hidden discrete logarithm problem, which is characterized in the adoption of the criterion of elimination of periodicity associated with the value of the discrete logarithm in the construction of periodic functions based on the public parameters of the signature scheme. In line with the approach, a new signature scheme is proposed as candidate for post-quantum public-key cryptoscheme. Its algebraic support represents a 6-dimensional finite non-commutative associative algebra set over the field $GF(p)$, which contains p^2 global right-sided units. Every one of the lasts is the unit of one of p^2 isomorphic finite non-commutative groups contained in the algebra. Every of the said groups contains commutative subgroups possessing 2-dimensional cyclicity and this feature is exploited to implement the enhanced criterion of providing security to the known and potential future quantum attacks.

1. Introduction

In the last few years the development of practical post-quantum (PQ) public-key (PK) cryptosystems has attracted considerable attention from the cryptographic community [11, 12]. Post-quantum are called cryptographic algorithms and protocols that run efficiently on classical computers but will resist attacks performed with using hypothetic quantum computers (quantum attacks). Currently, the most widely used in practice cryptographic algorithms and protocols are based on computationally difficult problems of finding discrete logarithm and factorization, however, in the PQ era, such cryptosystems are insecure. The latter is due to the fact that polynomial algorithms for solving the said computational problems are known for a quantum computer [14].

Quantum algorithms for solving both the factoring problem (FP) [1] and the discrete logarithm problem (DLP) [14, 15] are based on the extremely high efficiency of a quantum computer to perform a discrete Fourier transform [2], which is used to calculate the period length of periodic functions. In particular, to solve the problem of finding the value of a discrete logarithm, one constructs a peri-

2010 Mathematics Subject Classification: 94A60, 16Z05, 14G50, 11T71, 16S50
Keywords: non-commutative algebra, finite associative algebra, single-sided units, post-quantum cryptography, public-key cryptoscheme, signature scheme, discrete logarithm problem, hidden logarithm problem
This work was supported by the budget theme No. 0060-2019-010.

odic function whose values lie in an explicitly given cyclic group, which contains a period with the length depending on the value of the logarithm.

Developers of the PQ PK cryptoschemes usually use difficult computational problems that are different from the FP and DLP. An interesting approach to the designing of the PQ PK cryptoschemes and PQ commutative ciphers relates to using so called hidden DLP (HDLP) [3, 6, 7]. Different versions of the HDLP are used in the design of different PK cryptosystems. In the case of development of the signature schemes [9], the idea of that approach consists in selecting a cyclic group having sufficiently large prime order, which is generated by some vector N as a subset of elements of a finite non-commutative associative algebra (FNAA) followed by computing the PK in the form of the pair of the vectors $Q = \psi_1(N)$ and $Y = \psi_2(N^x)$, where x is private key; ψ_1 and ψ_2 are masking operations representing two different homomorphism-map (or automorphism-map) operations.

Due to using the masking operations ψ_1 and ψ_2 the vectors Q and Y are elements of two different cyclic groups each of which is different from the group generated by the vector N. Since the masking operations defines homormorphism maps, every one of them is mutually comutative with the exponentiation operation. Due to the last, one can use a DLP-based signature (for example, well known Schnorr signature algorithm [13]) and replace in it the signature verification procedure using the values N and N^x by the the signature verification procedure using the values Q and Y. To compute a signature a potential forger needs to know only the value x that is a discrete logarithm value in a hidden cyclic group, no element of which is known to the forger. The rationale of the security of the HDLP-based signature schemes consists in the fact that a periodic function $f(i,j)$ constructed as computation of product of the values Q^i and Y^j (for example, $f(i,j) = Q^i Y^j$) take on the values contained in numerous different groups contained in the FNAA used as algebraic support of the signature scheme. Therefore, the Shor quantum algorithm is not directly applicable to compute the value x, the function $f(i,j)$ contains a period depending on the value x though.

However, the question arises about the possibility of developing new quantum algorithms that allow us to calculate the period length for periodic functions that take values in algebraic sets that are not groups. In future, the emergence of such quantum algorithms will mean breaking the known HDLP-based signature schemes.

In this paper, we propose to adopt a strengthened criterion for ensuring security of the HDLP-based cryptoschemes to hypothetic quantum attacks based on the said advanced quantum algorithms for computing the lenth of the periods of periodic funcions related to a wider class of such functions. Namey, we propose the following advanced criterion of designing the HDLP-based PK cryptosystems: construction of the periodic functions on the base of the publicly know parameters of the cryptoscheme, which contain a period with the length depending on the value of the discrete logarithm in the hidden group, should be a computationally intractable problem.

To develop algorithms that meet this criterion, we propose to use the idea of masking periodicity with a period length different from the value of the prime order q of the cyclic group in which the hidden discrete logarithm problem is given. Namely, one is to design a signature scheme with such public parameters that using them to build periodic functions will give the period length equal to the order of the hidden cyclic group. As a concrete way to implement this idea, we propose to define a base cyclic group as a subgroup of a hidden commutative group having 2-dimensional cyclicity (i.e., group generated by a minimum generator system of two elements U and N having the same order value; in our case, the order is equal to the prime q). This makes it possible to form such a PK that the construction of periodic functions using its elements will define the value of the period equal to the value q. The latter is achieved by the fact that the elements of the PK are calculated by the formulas $Q = \psi_1(NU)$ and $Y = \psi_2(N^x)$.

The use of the multiplier U allows one to fix the length q of the period of the constructed periodic functions, but the presence of such a multiplier should be taken into account when developing the verification equation of the signature scheme. In general, the HDLP-based cryptosystems developed taking into account the proposed enhanced design criterion have lower performance, longer PK and signature. However, they are significantly more attractive as candidates for PQ signature schemes.

The rest of the paper is organized as follows. Section 2 describes the suitable algebraic support of the developed signature scheme, which represents the 6-dimensional FNAA defined over the ground finite field $GF(p)$ and containing p^2 different global right-sided units and p^2 finite non-commutative groups every one of which contains commutative subgroups with 2-dimensional cyclicity. Section 3 introduces the developed candidate for PQ signature scheme, characterized in using a commutative group with 2-dimensional cyclicity as a hidden group.

2. The used 6-dimensional FNAA

2.1. Preliminaries

In general, the m-dimensional finite algebra represents the m-dimensional vector space over some finite field, in which the vector multiplication operation (that is distributive at the left and at the right) is defined. If the vector multiplication is non-commutative and associative we have the FNAAs. The FNAA used as the algebraic support of the developed PQ signature scheme is defined over the ground field $GF(p)$ the characteristic of which is equal to the prime $p = 2q + 1$, where q is a 256-bit prime. The multiplication operation (denoted as $\circ$) in the considered FNAA is defined using the following formula descibing the result of the multiplying two 6-dimensional vectors $A = \sum_{i=0}^{5} a_i \mathbf{e}_i$, and $B = \sum_{j=0}^{5} b_j \mathbf{e}_j$, where $\mathbf{e}_0, \mathbf{e}_1, \ldots \mathbf{e}_5$ are formal basis vectors, as follows:

$$A \circ B = \left(\sum_{i=0}^{5} a_i \mathbf{e}_i \right) \circ \left(\sum_{j=0}^{5} b_j \mathbf{e}_j \right) = \sum_{j=0}^{5} \sum_{i=0}^{5} a_i b_j \left(\mathbf{e}_i \circ \mathbf{e}_j \right), \qquad (1)$$

where coordinates a_0, $a_1, \ldots a_5$ of the vector A and coordinates b_0, $b_1, \ldots b_5$ of the vector B are elements of the field $GF(p)$. One assumes the product of every pair of the basis vectors $\mathbf{e}_i \circ \mathbf{e}_j$ is to be replaced by some single-component vector $\lambda \mathbf{e}_k$ that is taken from the so called basis vector multiplication table (BVMT), namely, from the cell at the intersection of the ith row and the jth column. In present paper the BVMT shown as Table 1 is used to define the 6-dimensional FNAA with the required properties. This algebra contains p^2 isomorphic non-commutative groups every of which contains commutative subgroups having 2-dimensional cyclicity.

Table 1. The BVMT setting the FNAA with p^2 global right-sided units ($\lambda \geqslant 2$)

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\mathbf{e}_3$
$\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\lambda\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_1$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_1$
$\mathbf{e}_3$	$\lambda\mathbf{e}_0$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\lambda\mathbf{e}_3$	$\mathbf{e}_0$	$\mathbf{e}_3$
$\mathbf{e}_4$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_5$	$\lambda\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_4$	$\lambda\mathbf{e}_5$	$\mathbf{e}_4$	$\mathbf{e}_5$

2.2. Finite commutative group with 2-dimensional cyclicity

The finite 2-dimentional commutative algebra with the associative multiplication operation defined by Table 2 was considered in the paper [10], where it had been shown that the multiplicative group Γ of the algebra is cyclic, if the structural coefficient λ is a quadratic non-residue in $GF(p)$. In this case this algebra represents a finite field $GF(p^2)$.

If the structural coefficient λ is a quadratic residue in $GF(p)$, then the order of the group Γ has order equal to the value $\Omega = (p-1)^2$. Besides, Γ is generated by the minimum generator system $< G'_1, G'_2 >$, including two vectors of the same order equal to the value $(p-1)$. In [8] it was proposed to call a commutative finite group containg the minimum generator system of m vectors having the same order the group having m-dimensional cyclicity. In this paper the said term is used.

For the case $p = 2q + 1$, where q is a prime, one can consider the commutative primary group of the order q^2 that has 2-dimensional cyclicity and is generated by the generator system $< G_1, G_2 >$, where each of the vectors G_1 and G_2 has order q: $G_1 = {G'_1}^2$ and $G_2 = {G'_2}^2$. Independenly of the value of the structural coefficient λ the multiplicative group of the considered 2-dimentional algebra contains the unit equal to the vector $(1, 0)$. The said primary group can be considered as a set of $q+1$ different cyclic groups of the prime order q all possible pairs of which contain only one common element, namely, the unit vector $(1, 0)$. Evidently, some fixed

pair of the integers i and j $(0 < i < q;\ 0 < j < q)$ define the vector $G_{ij} = G_1^i \circ G_1^j$ having order equal to q, which is a generator of some cyclic group Γ_c of the prime order q. One can easily see that the following proposition holds true.

Table 2. The BVMT setting 2-dimensional commutative associative algebra over $GF(p)$

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$

Proposition 1. *For $k = 0, 1, \ldots, q-1$ each of the the formulas $G_k = G_{ij} \circ G_1^k$ and $G_k = G_{ij} \circ G_2^k$, where $i, j = 1, 2, \ldots, q-1$, defines q generators of q different cyclic groups having order q.*

Arbitrary two elements $N \neq (1, 0)$ and $U \neq (1, 0)$ of the said primary group, which are contained in different cyclic subgroups, represent the generator system of the primary group. Therefore, due to the Proposition 1, for arbitrary fixed integer i $(0 < i < q)$ q different cyclic groups are defined by the generators $U_k = N_i \circ U^k$, where $k = 0, 1, \ldots, q-1$. The last fact is used in the design of the proposed HDLP-based signature scheme.

2.3. Properties of the algebraic support

The FNAA defined over the field $GF(p)$ by Table 1, where $\lambda \neq 1$; $\lambda \neq 0$, contains p^2 global right-sided units R that can be computed from the vector equation

$$A \circ X = A \tag{2}$$

with the unknown 6-dimensional vector $X = (x_0, x_1, \ldots, x_5)$. Using Table 1 the equation (2) can be represented in the form of the following system of four linear equations:

$$\begin{cases} a_0 (x_0 + x_2 + x_4) + a_3 (\lambda x_0 + x_2 + x_4) = a_0; \\ a_1 (x_1 + \lambda x_3 + x_5) + a_2 (x_1 + x_3 + x_5) = a_1; \\ a_1 (\lambda x_0 + x_2 + x_4) + a_2 (x_0 + x_2 + x_4) = a_2; \\ a_0 (x_1 + x_3 + x_5) + a_3 (x_1 + \lambda x_3 + x_5) = a_3; \\ a_4 (x_0 + x_2 + x_4) + a_5 (\lambda x_0 + x_2 + x_4) = a_4; \\ a_4 (x_1 + x_3 + x_5) + a_5 (x_1 + \lambda x_3 + x_5) = a_5. \end{cases} \tag{3}$$

Performing the variable substitution $u_1 = x_0 + x_2 + x_4$, $u_2 = \lambda x_0 + x_2 + x_4$, $u_3 = x_1 + x_3 + x_5$, and $u_4 = x_1 + \lambda x_3 + x_5$, one can represent the system (3) in the following form:

$$\begin{cases} a_0u_1 + a_3u_2 = a_0; \\ a_1u_4 + a_2u_3 = a_1; \\ a_2u_1 + a_1u_2 = a_2; \\ a_0u_3 + a_3u_4 = a_3; \\ a_4u_1 + a_5u_2 = a_4; \\ a_4u_3 + a_5u_4 = a_5. \end{cases}$$

The solution $(u_1, u_2, u_3, u_4) = (1, 0, 0, 1)$ satisfies the last system for all 6-dimensional vectors, therefore, the conditions

$$\begin{cases} u_1 = x_0 + x_2 + x_4 = 1; \\ u_2 = \lambda x_0 + x_2 + x_4 = 0; \end{cases} \tag{4}$$

$$\begin{cases} u_3 = x_1 + x_3 + x_5 = 0; \\ u_4 = x_1 + \lambda x_3 + x_5 = 1. \end{cases} \tag{5}$$

define the ful set of the global right-sided units $R = (r_0, r_1, r_2, r_3, r_4, r_5)$ that satisfy the equation (2). Solving the systems of linear equations (4) and (5) one can get the following formula describing p^2 different global right-sided units:

$$R = \left(\frac{1}{1-\lambda}, \frac{h(\lambda-1)+1}{1-\lambda}, \frac{d(\lambda-1)-\lambda}{1-\lambda}, \frac{-1}{1-\lambda}, d, h \right), \tag{6}$$

where $d, h = 0, 1, \ldots, p-1$. Evidently, the considered algebra contains no global left-sided unit nor global two-sided unit, however it contains numerous local left-sided units L acting in some subsets of the 6-dimensional vectors. The local left-sided unit L_A corresponding to the set of the algebraic elements, which includes all possible powers of some fixed vector A, can be computed as solution of the vector equation

$$X \circ A = A. \tag{7}$$

Using Table 1 one can represent (7) in the form of the following three independent systems of two linear equations with the pairs of the unknowns (x_0, x_1), (x_2, x_5), and (x_3, x_4) :

$$\begin{cases} (a_0 + a_2 + a_4)\, x_0 + (a_0 + \lambda a_2 + a_4)\, x_1 = a_0; \\ (a_1 + a_3 + a_5)\, x_0 + (a_1 + a_3 + \lambda a_5)\, x_1 = a_1; \end{cases} \tag{8}$$

$$\begin{cases} (a_0 + a_2 + a_4)\, x_2 + (a_0 + \lambda a_2 + a_4)\, x_5 = a_2; \\ (a_1 + a_3 + a_5)\, x_2 + (a_1 + a_3 + \lambda a_5)\, x_5 = a_5; \end{cases} \tag{9}$$

$$\begin{cases} (a_1 + a_3 + \lambda a_5)\, x_3 + (a_1 + a_3 + a_5)\, x_4 = a_3; \\ (a_0 + \lambda a_2 + a_4)\, x_3 + (a_0 + a_2 + a_4)\, x_4 = a_4; \end{cases} \tag{10}$$

The same main determinant Δ_A corresponds to each of the systems (8), (9), and (10):

$$\Delta_A = (a_0a_5 + a_4a_5 - a_1a_2 - a_2a_3)(\lambda - 1). \tag{11}$$

If $\Delta_A \neq 0$, then every of the systems (8), (9), and (10) has unique solution, i. e., the vector equation (7) has unique solution as the local left-sided unit L_A related to the vector A. Solving the systems (8), (9), and (10) one gets the following formulas describing the value $L_A = (l_0, l_1, l_2, l_3, l_4, l_5)$:

$$\begin{aligned} l_0 &= \frac{1}{1-\lambda}; \quad l_1 = \frac{a_0a_1 + a_1a_4 - a_2a_3 - a_2a_5}{\Delta_A}; \\ l_2 &= \frac{\lambda a_2a_3 + a_2a_5 - \lambda a_0a_1 - a_1a_4}{\Delta_A}; \quad l_3 = \frac{-1}{1-\lambda}; \\ l_4 &= \frac{a_0a_4 + \lambda a_3a_4 - \lambda a_0a_5 - a_2a_5}{\Delta_A}; \; l_5 = \frac{a_0a_5 + a_2a_5 - a_1a_4 - a_3a_4}{\Delta_A}. \end{aligned} \tag{12}$$

Proposition 2. *Suppose the vector A is such that $\Delta_A \neq 0$. Then the local left-sided unit L_A is simultaneously the local two-sided unit E_A relating to the vector A.*

Proof. It is sufficient to show that the vector L_A is contained in the set (6) of the global right-sided units. Suppose in (6) we have $d = l_4$ and $h = l_5$. Then one can compute

$$r_1 = \frac{h(\lambda - 1) + 1}{1 - \lambda} = l_1; \quad r_2 = \frac{d(\lambda - 1) - \lambda}{1 - \lambda} = l_2.$$

Since $r_0 = l_0$ and $r_3 = l_3$, the local left-sided unit L_A is equal to the global right-sided unit corresponding to the integer values $d = l_4$ and $h = l_5$ in (6) and the vector L_A is the local two-sided unit E_A relating to the vector A. □

Due to the last proposition, one can conclude that the vector L_A acts on every vector form the set $A, A^2, \ldots, A^i, \ldots$ as local two-sided unit. Since $\Delta_A \neq 0$, for the fixed value A one has unique value L_A and the said sequence is periodic with the period length equal to some integer ω. The set of all vectors included in a fixed period compose a finite cyclic group (generated by the vector A) with the unit element equal to $E_A = L_A$, i. e., the element L_A can be computed using the formula $L_A = E_A = A^\omega$. For the integer value i $(0 < i < \omega)$the vector $A^{\omega - i}$ is the inverse value of the vector A^i relatively the local two-sided unit E_A, therefore, the vector A can be called a locally invertible vector. One can easily prove the following proposition:

Proposition 3. *Suppose the vector A is such that $\Delta_A \neq 0$. Then there exists some integer ω such that $A^\omega = E_A$ and the local two sided-unit E_A is simultaneously the unit of the cyclic group generated by the vector A.*

Proposition 4. *If the vector equation $A \circ X = B$ has solution $X = S$ such that $\Delta_S \neq 0$, then p^2 different values $X_i = R_i \circ S$, where R_i takes on all values from the set* (6)*, also represents solutions of the given equation.*

Proof. $A \circ (R_i \circ S) = (A \circ R_i) \circ S = A \circ S = B$. Suppose $R_i \circ S = R_j \circ S$, then $(R_i - R_j) \circ S = (0,0,0,0,0,0)$ and $R_i = R_j$, i. e., the number of different solutions $X_i = R_i \circ S$ is equal to the number of different global right-sided units, which is equal to p^2. The Proposition 4 is proven. □

Proposition 5. *Suppose the vector R is a global right-sided unit. Then the map of the FNAA, which is defined by the formula $\varphi_R(X) = R \circ X$, where the vector X takes on all values in the considered FNAA, is a homomorphism.*

Proof. For two arbitrary vectors X_1 and X_2 we have

$$\varphi_R(X_1 \circ X_2) = R \circ (X_1 \circ X_2) = (R \circ X_1) \circ (R \circ X_2) = \varphi_R(X_1) \circ \varphi_R(X_2);$$

$$\varphi_R(X_1 + X_2) = R \circ (X_1 + X_2) = R \circ X_1 + R \circ X_2 = \varphi_R(X_1) + \varphi_R(X_2). \quad \square$$

Proposition 6. *All locally invertible vectors of the considered 6-dimensional FNAA compose p^2 different groups with p^2 different units*

$$E = R = \left(\frac{1}{1-\lambda},\ \frac{h(\lambda-1)+1}{1-\lambda},\ \frac{d(\lambda-1)-\lambda}{1-\lambda},\ \frac{-1}{1-\lambda},\ \ d,\ \ h \right),$$

where $d, h = 0, 1, 2, \ldots p-1$.

Proof. Suppose the set $\{A_1, A_2, \ldots A_i, \ldots A_\Omega\}$ of locally invertible vectors includes all vectors relating to a fixed local two-sided unit E (including the vector E) and only such vectors. One can easily see that the said set is the group Γ_E with the unit E. Every fixed global right-sided unit R' from the set (6) is the unit E' of some group $\Gamma_{E'}$ representing a set locally invertible vectors $\{A'_1, A'_2, \ldots A'_i, \ldots A'_\Omega\}$. Indeed, due to the Proposition 5 we have $A'_i = R' \circ A_i$ for $i = 1, 2, \ldots \Omega$, and $E' = R' \circ E = R'$. We have p^2 different global right-sided units R described by the formula (6). Every of these units defines a unique group of the order Ω. The Proposition 6 is proven. □

Consider the order Ω of every of the said isomorphic groups. Evidently $\Omega = \Omega' p^{-2}$, where Ω' is the number of all locally invertible vectors contained in the algebra. One can compute the last value as $\Omega' = p^6 - \Omega''$, where Ω'' is the number of all non-invertible vectors, i. e., vectors satisfying the condition $\Delta_A = 0$. The last condition reduces to the following equation:

$$a_0 a_5 + a_4 a_5 - a_1 a_2 - a_2 a_3 = 0.$$

If $a_5 \neq 0$, then for arbitrary values a_1, a_2, a_3, a_4 there exists unique value a_0 that satisfies the last equality (in this case we have $p^4(p-1)$ different non-invertible vectors). For the case $a_5 = 0$ the equality holds true for arbitrary values a_0 and a_4, if $a_1 a_2 + a_2 a_3 = 0$. Consideration of two subcases i) $a_2 \neq 0$ and ii) $a_2 = 0$ gives respectively $p^3(p-1)$ and p^4 different non-invertible vectors. Totally the algebra contains $\Omega'' = p^4(p-1) + p^3(p-1) + p^4 = p^5 + p^4 - p^3$ non-invertible vectors.

Proposition 7. *Every one of p^2 isomorphic groups, which relates to some fixed global right-sided unit R and includes all invertible vectors relating to R, has order $\Omega = p(p-1)^2(p-1)$.*

Proof. We have $\Omega' = p^6 - \Omega'' = p^6 - \left(p^5 + p^4 - p^3\right) = p^3(p-1)\left(p^2-1\right)$ and $\Omega = \Omega' p^{-2} = p(p-1)\left(p^2-1\right)$. □

One can easily see that the set of all 6-dimensional vectors of the form $A' = (a_0, a_1, a_2, a_3, 0, 0)$ compose the 4-dimensional non-commutative subalgebra with the multiplication operation set by the BVMT shown as Table 3. This subalgebra contains one global two-sided unit E_{00} that is contained in the set (6) and corresponds to the integer values $d = 0$ and $h = 0$:

$$E_{00} = \left(\frac{1}{1-\lambda}, \frac{1}{1-\lambda}, \frac{-\lambda}{1-\lambda}, \frac{-1}{1-\lambda}, 0, 0\right).$$

Actually, this subalgebra represents the 4-dimensional FNAA described in [4] and used as algebraic support of the HDLP-based signature schemes. The multiplicative group Γ_{00} of the subalgebra is one of the p^2 isomorphic groups contained in the considered 6-dimensional FNAA.

The group Γ_{00} includes a large number of commutative subgroups possessing 2-dimensional cyclicity. Indeed, for arbitrary value $\alpha \in GF(p)$ the vector $V_\alpha = \alpha E_{00}$ (scalar multiplication) is permutable with every vector in the group Γ_{00}. If α is a primitive element in $GF(p)$, then the vector V_α generates a cyclis subgroup Γ_α of the order $p-1$. Suppose $G \notin \Gamma_{00}$ ($G \notin \Gamma_\alpha$) is a vector of the order $p-1$. Then the generator system $< V_\alpha, G >$ generates the commutative subgroup possessing the order $(p-1)^2$ and having 2-dimensional cyclicity.

Table 3. The BVMT of the 4-dimensional subalgebra containing a global two-sided unit

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\mathbf{e}_3$	–	–
$\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\lambda\mathbf{e}_1$	–	–
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_1$	–	–
$\mathbf{e}_3$	$\lambda\mathbf{e}_0$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\lambda\mathbf{e}_3$	–	–
$\mathbf{e}_4$	–	–	–	–	–	–
$\mathbf{e}_5$	–	–	–	–	–	–

Suppose the vector A is such that $\Delta_A \neq 0$ and R is a random global right-sided unit. One can compute the single vector B that satisfies the condition

$$B \circ A = R. \tag{13}$$

Evidently, the main determinant of the system of linear equations, which corresponds to the vector equation (13) is equal to $\Delta_A \neq 0$, therefore, the equation (13) has unique solution.

Proposition 8. *Suppose $B \circ A = R$. Then the formula*

$$\psi_R(X) = A \circ X \circ B,$$

where the vector X takes on all values in the considered 6-dimensional FNAA, sets the homomorphism map.

Proof. For two random 6-dimensional vectors X_1 and X_2 one can get the following:

$$\begin{aligned}\psi_R(X_1 \circ X_2) &= A \circ (X_1 \circ X_2) \circ B = A \circ (X_1 \circ R \circ X_2) \circ B \\ &= (A \circ X_1 \circ B) \circ (A \circ X_2 \circ B) = \psi_R(X_1) \circ \psi_R(X_2); \\ \psi_R(X_1 + X_2) &= A \circ (X_1 + X_2) \circ B = (A \circ X_1 \circ B) + (A \circ X_2 \circ B) \\ &= \psi_R(X_1) + \psi_R(X_2).\end{aligned}$$

□

Proposition 9. *The homomorphism-map operation $\psi_R(X) = A \circ X \circ B$ and the exponentiation operation X^k are mutually commutative, i.e., the equality $A \circ X^k \circ B = (A \circ X \circ B)^k$ holds true.*

Proof. Due to Proposition 8 we have $\psi_R(X^k) = (\psi_R(X))^k$, i. e., $A \circ X^k \circ B = (A \circ X \circ B)^k$. □

3. The proposed HDLP-based signature scheme

3.1. Setting the hidden commutative group

The algebraic support of the introduced signature scheme represents the 6-dimensional FNAA described in Subsection 2.3 and defined over the field $GF(p)$ with characteristic $p = 2q + 1$, where q is a 256-bit prime. In the BVMT defining the multiplication operation (see Table 1) it is used the structural coefficient $\lambda \geqslant 2$, for example, $\lambda = 2$. Computation of the private and public parameters of the signature scheme begins with setting a private hidden finite commutative group $\Gamma_{<N,U>}$. The group $\Gamma_{<N,U>}$ is set as computation of its generator system $< N, U >$ that includes two vectors N and U each of which has order equal to the prime q. The generator system $< N, U >$ can be computed as follows:

1. Generate at random a locally invertible vector $U = (u_0, u_1, \ldots, u_5)$ of the order equal to q and, using the formulas (12), compute the global left-sided unit $L_U = (l_{U0}, l_{U1}, \ldots, l_{U5})$.

2. If the condition $\frac{u_0}{l_{U0}} = \frac{u_i}{l_{Ui}}$ holds true for all $i = 1, 2, \ldots, 5$, then go to step 1 (probability of this event is equal to $\approx q^{-1}$).

3. Select at random an integer value α $(1 < \alpha < p - 1)$ that is a primitive element modulo p. The primitive element α defines a locally invertible vector $G = \alpha^2 L_U$ having order equal to the prime q.

4. Generate a random integer k $(1 < k < q)$ and compute the vectors $N = G \circ U^k$.

One can easily see that each of the vectors N and U has order equal to the value q and the generator system $< N, U >$ defines a commutative primary group

$\Gamma_{<N,U>}$ the unit element of which is equal to L_U. The group $\Gamma_{<N,U>}$ has structure with the 2-dimensional cyclicity and the group order is equal to $\Omega = q^2$.

3.2. Computing parameters of the masking operations

The main contribution to the security of the developed signature scheme is introduced by two exponentiation operations performed in two different cyclic groups contained in the hidden commutative group $\Gamma_{<N,U>}$. The vector N sets the first of the said cyclic groups. The second cyclic group is set by the generator J that is computed as follows:

$$J = N^t \circ U^w,$$

where t and w ($1 < t < q$; $1 < w < q$) are two integer values selected at random. The vectors N, J, N^x, and $J^{x/2}$, where $x < q$ is an integer representing one of the elements of the private key, are used for computing the vectors $\psi_1(N \circ U)$, $\psi_2(N^x)$, $\psi_3\left(J \circ U^2\right)$, and $\psi_4\left(J^{x/2}\right)$ that are elements of the PK. Four different homomorphism-map operations ψ_1, ψ_2, ψ_3, and ψ_4 are used to compute four elements of the PK, which are elements of four different commutative groups contained in the algebra.

Parameters of the homomorphism-map operations $\psi_1(X) = A_1 \circ X \circ B_1$, $\psi_2(X) = A_2 \circ X \circ B_2$, $\psi_3(X) = A_1 \circ X \circ B_3$, and $\psi_4(X) = A_4 \circ X \circ B_4$, are computed as follows:

1. Select at random a global right-sided unit R_1 (for example, using the formula (6)), generate at random a locally invertible vector A_1, and compute the vector B_1 as solution of the vector equation $B_1 \circ A_1 = R_1$ (that has unique solution B_1, since $\Delta_{A_1} \neq 0$).
2. Select at random a global right-sided unit R_2, generate at random a locally invertible vector A_2, and compute the vector B_2 as solution of the vector equation $B_2 \circ A_2 = R_2$.
3. Select at random a global right-sided unit R_3 and compute the vector B_3 as solution of the vector equation $B_3 \circ A_1 = R_3$, where the vector A_1 has been generated at step 1.
4. Select at random a global right-sided unit R_4, generate at random a locally invertible vector A_4, and compute the vector B_4 as solution of the vector equation $B_4 \circ A_4 = R_4$.

3.3. Computation of the public key

The PK represents a set of six 6-dimensional vectors $(Z_1, Y_1, T_1; Z_2, Y_2, T_2)$ which are computed as follows:

1. $Z_1 = A_1 \circ N \circ U \circ B_1$ and $Y_1 = A_2 \circ N^x \circ B_2$.
2. $T_1 = R \circ A_1 \circ B_2$, where R is a random global right-sided unit.
3. $Z_2 = A_1 \circ J \circ U^2 \circ B_3$ and $Y_2 = A_4 \circ J^{x/2} \circ B_4$.
4. $T_2 = R' \circ A_1 \circ B_4$, where R' is a random global right-sided unit.

One can consider the private key as the set of all of secret elements that are needed to compute the signature. With such interpretation in the developed signature scheme the private key represents the set of the values x, N, J, U, A_1, B_2, and B_4.

3.4. Algorithm for signature generation

Suppose one should sign an electronic document M, using some fixed secure 256-bit hash-function f_H. The signature includes the following three elements: two 256-bit integers e and s and a 6-dimensional vector S. The elements of the signature are computed using the following signature generation algorithm:

1. Generate a random integer $k < q$ and a random locally invertible 6-dimensional vector K. Then compute the vectors V_1 and V_2:

$$\begin{cases} V_1 = K \circ N^k \circ B_2; \\ V_2 = K \circ J^{k/2} \circ B_4. \end{cases}$$

2. Calculate the first signature element e as the hash-function value computed from the document M to which the vectors V_1 and V_2 are concatenated:

$$e = f_H\left(M, V_1, V_2\right).$$

3. Calculate the second signature element s as follows: $s = k + xe \bmod q$.

4. Calculate the third signature element S as solution of the following vector equation:

$$S \circ A_1 \circ U^s = K.$$

In the last vector equation every of the values U^s, A_1, and K is a locally invetible vector, therefore, the equation has unique solution. At the output of the last algorithm one gets the signature (e, s, S) to the document M.

3.5. Algorithm for signature verification

Using the PK $(Y_1, Z_1, T_1;\ Y_2, Z_2, T_2)$, one can verify the signature (e, s, S) to the document M with the following signature verification algorithm:

1. Using the PK, compute the vectors V_1' and V_2':

$$\begin{cases} V_1' = S \circ Z_1^s \circ T_1 Y_1^{-e}; \\ V_2' = S \circ Z_2^{s/2} \circ T_2 \circ Y_2^{-e}. \end{cases}$$

2. Calculate the hash-function value e' from the document M to which the vectors V_1' and V_2' are concatenated: $e' = f_H\left(M, V_1', V_2'\right)$.

3. Using the formula (10), calculate the value Δ_S corresponding to the locally invertible vector $S = (s_0, s_1, s_2, s_3)$.

4. If $e' = e$ and $\Delta_S \neq 0$, then the signature is genuine. Otherwise the signature is rejected as false one.

3.6. Correctness proof

Correctness proof of the sigature scheme consists in proving that the signature (e, s, S) computed correctly will pass the verification procedure as genuine signature. Taking into account the mutual commutativity of the ψ-map operation with the exponentiation operation, for the vectors V_1' and V_2' computed at the first step of the signature verification procedure we have the following:

$$\begin{aligned} V_1' &= S \circ Z_1^s \circ T_1 \circ Y_1^{-e} \\ &= S \circ (A_1 \circ N \circ U \circ B_1)^s \circ R \circ A_1 \circ B_2 \circ (A_2 \circ N^x \circ B_2)^{-e} \\ &= S \circ A_1 \circ U^s \circ N^s \circ B_1 \circ A_1 \circ B_2 \circ A_2 \circ N^{-es} \circ B_2 \\ &= K \circ N^s \circ R_1 \circ R_2 \circ N^{-es} \circ B_2 = K \circ N^{k+ex} \circ N^{-ex} \circ B_2 \\ &= K \circ N^k \circ B_2 = V_1; \end{aligned}$$

$$\begin{aligned} V_2' &= S \circ Z_2^{s/2} \circ T_2 \circ Y_2^{-e} \\ &= S \circ \left(A_1 \circ J \circ U^2 \circ B_3\right)^{s/2} \circ R' \circ A_1 \circ B_4 \circ \left(A_4 \circ J^{x/2} \circ B_4\right)^{-e} \\ &= S \circ A_1 \circ U^s \circ J^{s/2} \circ B_3 \circ A_1 \circ B_4 \circ A_4 \circ (J^{-ex/2}) \circ B_4 \\ &= K \circ J^{(k+ex)/2} \circ R_3 \circ R_4 \circ J^{-ex/2} \circ B_4 = K \circ J^{(k+ex)/2-ex/2} \circ B_4 \\ &= K \circ J^{k/2} \circ B_4 = V_2. \end{aligned}$$

For $V_1' = V_1$ and $V_2' = V_2$ we have $f_H\,(M, V_1', V_2') = f_H\,(M, V_1, V_2)$ and the equality $e' = e$ holds true. For the signature (e, s, S) computed correctly inequality $\Delta_S \neq 0$ is satisfied. Thus, the signature scheme performes correctly.

4. Discussion

In the known signature schemes based on the computational difficulty of the HDLP, security to potential quantum attacks is provided by such design that sets the public signature-scheme parameters contained in different finite groups of some FNAA used as algebraic support of the cryptoscheme. Therefore, the use of the public parameters of the signature scheme in constructing periodic function causes the lasts to take values from many different groups, so the known quantum algorithms for finding the discret logarithm cannot be applied, the functions with the period length depending on the discrete logarithm value can be easily constructed though. The emergence of each new quantum algorithm will require a separate consideration of the security issue.

To obtain stronger guarantees of security to quantum attacks based on quantum algorithms for finding the length of periods of periodic functions, which can be developed in the future, it is reasonable to construct such signature schemes that periodic functions constructed using public parameters of the signature scheme will

be free of periods whose length is associated with the value of the discrete logarithm. The signature scheme described in Section 3 is an attempt of implementing this idea.

The proposed design can be considered as modification of the signature scheme described in [9], in which the PK represents three vectors $Z = \psi'(N)$, $Y = \psi''(N^x)$, and T, where ψ' and ψ'', are different homomorphism-map operations satisfying the condition $Y^i \circ T \circ Z^j = W_1 \circ N^{xj+i} \circ W_2$ for some fixed vectors W_1 and W_2 defining a map-operation of arbitrary type. Due to the last condition the periodic function $f(i,j) = Y^i \circ T \circ Z^j$ contains a period that is determined by the value of the discrete logarithm x. Indeed, the condition $Y^i \circ T \circ Z^j = Y^{i-1} \circ T \circ Z^{j+x}$ holds true. To eliminate periodicity connected with the value x, in the present paper for computing the vector Z it is proposed to use the formula $Z = \psi'(N \circ U)$, where the vectors N and U have the same prime order and are selected from hidden commutative group, besides these two vectors are contained in different cyclic groups. After such modification the periodic function $f(i,j) = Y^i \circ T \circ Z^j$ becomes free from periods connected with the value x, since $Y^i \circ T \circ Z^j = W_1 \circ N^{xj+i} \circ U^j \circ W_2$, where U cannot be represented in the form of some power of the vector N. Indeed, if the equation $N^{xj+i} \circ U^j = N^{xj'+i'} \circ U^{j'}$ holds true, then we have $j' \equiv j \bmod q$ and $i' \equiv i \bmod q$.

The said modification requires to introduce corresponding modification of the signature verification equation and such modfication has been performed as introducing the left-sided multiplication by the vector S that is the third signature element. This modification gives the following signature verification equation: $V' = S \circ Z^s \circ Y^{-e}$. However, after the modification a potential attacker can easily forge a signature using the value S as a fitting parameter, for example, using the following algorithm:

1. Generate at random a locally invertible vector V and compute $e = f_H(M, V)$.
2. Select at random a 256-bit number $s < q$.
3. Compute the vector S from the vector equation $S \circ Z^s \circ Y^{-e} = V$.

In order to prevent attacks based on using the signature element S as a fitting parameter in the introduced signature scheme the signature verification procedure includes two different verification equations.

Up to this point, we have focused attention on the fact that the calculation of the value x by public parameters of the HDLP-based schemes cannot be performed using known quantum algorithms for calculating the discrete logarithm. However, suppose a forger knows the value x. In the case of the HDLP-based signature schemes described in [5, 9] one can easily compose the signature generation algorithm using the value x and public parameters. In the case of the introduced signature scheme, knowledge of the value of x is not sufficient to simply calculate a genuine signature. In this connection one has an interesting research item on estimation of the computationally difficulty of forging a signature, when the private value x is known to the forger.

In comparison with the known HDLP-based signature schemes [5, 9], disadvantages of the proposed new signature scheme is the increased size of the signature

(about 3 times), the increased size of the PK (about 3 times), the reduced performance of the signature generation procedure (about 3 times) and signature verification procedure (about 2 times). However, these disadvantages are offset by the main advantage of the new scheme, which consists in the proposed significantly higher security to future quantum attacks and a more rigorous justification of such expectation.

5. Conclusion

This paper introduces a new approach to the design of the HDLP-based signature schemes and describes a signature scheme that illustrates a method used to satisfy the adopted criterion of eliminating periods having length connected with the value of discrete logarithm in construction of the periodic functions on the base of the public parameters of the signature scheme. The main difference of the proposed design from the earlier known deigns of the HDLP-based signature schemes is the use of the hidden commutative group possessing 2-dimensional cyclicity instead of using a hidden cyclic group. The 6-dimensial FNAA used as algebraic support of the developed signature scheme contains very large number of isomorphic commutative groups with 2-dimensional cyclicity.

One can suppose that FNAAs containing a large set of commutative groups with 3-dimensional cyclicity provide more space in designing the HDLP-based candidates for PQ signatures. This assumption sets the theme of a new study in the development of the proposed approach, but it is associated with the use of the FNAAs possessing a suitable structure. New designs in the line with the introduced approach, which are based on using 4-dimensional FNAAs with global two-sided unit, also represent practical interest.

Acknowledgement. The authors thank anonymous Referee for valuable remarks.

References

[1] **A. Ekert, R. Jozsa**, *Quantum computation and Shor's factoring algorithm*, Rev. Mod. Phys. **68** (1996), 733.

[2] **R. Jozsa**, *Quantum algorithms and the fourier transform*, Proc. Roy. Soc. London Ser A, **454** (1998), 323 – 337.

[3] **A.S. Kuzmin, V.T. Markov, A.A. Mikhalev, A.V. Mikhalev, A.A. Nechaev**, *Cryptographic algorithms on groups and algebras*, J. Math. Sci. **223** (2017), no. 5, 629 – 641.

[4] **A.A. Moldovyan, N.A. Moldovyan**, *Post-quantum signature algorithms based on the hidden discrete logarithm problem*, Computer Sci. J. Moldova. **26** (2018), 301 – 313.

[5] **A.A. Moldovyan, N.A. Moldovyan**, *Finite non-commutative associative algebras as carriers of hidden discrete logarithm problem*, Bull. South Ural State Univ. Ser. Math. Modelling, Programming & Computer Software. **12** (2019), 66 – 81.

[6] **D.N. Moldovyan**, *Non-commutative finite groups as primitive of public-key cryptoschemes*, Quasigroups and Related Systems, **18** (2010), 165 – 176.

[7] **D.N. Moldovyan**, *A unified method for setting finite none-commutative associative algebras and their properties*, Quasigroups and Related Systems, **27** (2019), 293 – 308.

[8] **N.A. Moldovyan**, *Fast signatures based on non-cyclic finite groups*, Quasigroups and Related Systems, **18** (2010), 83 – 94.

[9] **N.A. Moldovyan**, *Finite non-commutative associative algebras for setting the hidden discrete logarithm problem and post-quantum cryptoschemes on its base*, Bul. Acad. Stiinte Republ. Moldova. Matematica, **1(89)** (2019), 71 – 78.

[10] **N.A. Moldovyan, P.A. Moldovyanu**, *New primitives for digital signature algorithms*, Quasigroups and Related Systems, **17** (2009), 271 – 282.

[11] *Post-quantum cryptography*, Lecture Notes Comp. Sci. **10786** (2018).

[12] *Post-quantum cryptography*, Lecture Notes Comp. Sci. **11505**, (2019).

[13] **C.P. Schnorr** *Efficient signature generation by smart cards*, J. Cryptology, **4** (1991), 161 – 174.

[14] **P.W. Shor**, *Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer*, SIAM J. Computing, **26** (1997), 1484 – 1509.

[15] **S.Y. Yan**, *Quantum Attacks on Public-Key Cryptosystems*, Springer (2014).

Received December 16, 2019

St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences,
14-th line 39, 199178, St. Petersburg, Russia
E-mails: maa1305@yandex.ru, mdn.spectr@mail.ru, nmold@mail.ru

Quasigroups and Related Systems **28** (2020), 285 – 299

Division on semigroups that are semilattices of groups

Robert A. R. Monzo

Abstract. The binary products of right, left or double division on semigroups that are semilattices of groups give interesting groupoid structures that are in one-one correspondence with semigroups that are semilattices of groups. This work is inspired by the well-known one-one correspondence between groups and Ward quasigroups.

1. Introduction

It appears in the literature that in 1930 M. Ward was the first to find a set of axioms on $(S, *)$ (a set S with a binary operation $*$, called here a *groupoid*) that ensure the existence of a group binary operation $\circ$ on S such that $x * y = x \circ y^{-1}$ cf. [12]. Such a groupoid was called a *division groupoid* by Polonijo (cf. [10]) and it is clear that division groupoids are quasigroups.

Over the next 63 years many other sets of axioms on a groupoid were found that make it a division groupoid, now commonly known as a Ward quasigroup (see for example: [1, 2, 4, 6, 7, 8, 9, 10, 11]). Perhaps the most impressive of these characterisations of Ward quasigroups is that of Higman and Neumann who found a single law making a groupoid a Ward quasigroup (cf. [6]). It is now known that a quasigroup is a Ward quasigroup if and only if it satisfies the law of right transitivity, $(x * z) * (y * z) = x * y$ (cf. [9]). It follows that a quasigroup is the dual of a Ward quasigroup, which we will call a Ward dual quasigroup, if and only if it satisfies the identity $(z * x) * (z * y) = x * y$.

Starting from any group $(G, \circ)$ we can form a Ward quasigroup $(G, *)$ by defining $x * y = x \circ y^{-1}$; that is, $*$ is the operation of right division in the group $(G, \circ)$. Conversely, any Ward quasigroup $(W, *)$ is unipotent and its only idempotent $e = e * e = x * x$ (for any $x \in W$), is a right identity element. If we then define $(W, \circ)$ as $x \circ y = x * (e * y)$, $(W, \circ)$ is a group, $x^{-1} = e * x$ and $x * y = x \circ y^{-1}$. These mappings, $(G, \circ) \mapsto (G, *)$ and $(W, *) \mapsto (W, \circ)$ are inverse mappings, which implies that groups are in one-to-one correspondence with Ward quasigroups. (This is all well known.) In addition, a Ward quasigroup is an inverse groupoid, with the unique inverse of x being $x^{-1} = e * x$. That is, the inverse of an element of a Ward quasigroup is the inverse element in the group it *induces*.

2010 Mathematics Subject Classification: 20N02; 20N05; 20N99
Keywords: Semigroup semilattice of groups; Ward dual quasigroup; double Ward quasigroups.

In 2007 N.C. Fiala proved (cf. [5]) that a quasigroup $(S, *)$ satisfies the identity $[(e * e) * (x * z)] * [(e * y) * z] = x * y$ (for some $e \in S$) if and only if there is a group $(S, \circ)$ with identity element e such that $x * y = x^{-1} \circ y^{-1}$. Fiala called such groupoids *double Ward quasigroups*. He noted that the binary operation $\circ$ on a double Ward quasigroup S defined by $x \circ y = (e * x) * (e * y)$ is a group operation and that double Ward quasigroups are in one-to-one correspondence with groups. Double Ward quasigroups are also inverse quasigroups, with $x^{-1} = x$.

Our intention here is to explore the operations $x * y = x \cdot y^{-1}$ (called *right division*), $x * y = x^{-1} \cdot y$ (called *left division*) and $x * y = x^{-1} \cdot y^{-1}$ (called *double division*) when $(S, \cdot)$ is a semigroup and a semilattice of groups, where x^{-1} is the inverse of x in the group to which it belongs. We will prove that each collection of all such structures are in one-one correspondence with the collection of all semigroups that are semilattices of groups and, in this sense, we extend the result that Ward quasigroups are in one-to-one correspondence with groups.

2. Preliminary definitions and results

The set of all idempotent elements of a groupoid $(S, *)$ is denoted by $E(S, *)$, i.e., $E(S, *) = \{x \in S \mid x*x = x\}$. Note that the set $E(S, *)$ may not be closed under the operation $*$. The groupoid $(S, *)$ is called an *idempotent groupoid* (a *semilattice groupoid*) if all of its elements are idempotent (idempotent and commute). A semilattice groupoid $(S, *)$ is called a *semigroup semilattice* if it is a semigroup. A groupoid $(S, *)$ is called an (*idempotent*) *groupoid* $(T, \cdot)$ *of groupoids* $(S_\alpha, *_{|_{S_\alpha}})$ $(\alpha \in T)$ if S is a disjoint union of the S_α $(\alpha \in T)$ and $S_\alpha * S_\beta \subseteq S_{\alpha \cdot \beta} = S_{\alpha\beta}$ for all $\alpha, \beta \in T$. Note that this definition does not require either of the binary operations $\cdot$ or $*$ to be associative.

We call the groupoid $(S, *)$ *right* (*left*) *solvable* if for any $a, b \in S$ there exists a unique $x \in S$ such that $a * x = b$ $(x * a = b)$. The groupoid $(S, *)$ is a *quasigroup* if it is right and left solvable, in which case it is right and left cancellative. We call the quasigroup $(S, *)$ a *Ward quasigroup* (*Ward dual quasigroup*) if it satisfies the identity $(x*z)*(y*z) = x*y$ $((z*x)*(z*y) = x*y)$. The quasigroup $(S, *)$ is called a *double Ward quasigroup* if it satisfies the identity $((e * e) * (x * z)) * ((e * y) * z) = x * y$ for some fixed $e \in S$. A groupoid $(S, *)$ is called an *inverse groupoid* if for all $x \in S$ there exists a unique element x^{-1} such that $(x * x^{-1}) * x = x$ and $(x^{-1} * x) * x^{-1} = x^{-1}$. The fact that $(S, *)$ and $(T, \circ)$ are isomorphic groupoids is denoted by $(S, *) \cong (T, \circ)$. The groupoid $(S, \bar{*})$ is dual to the groupoid $(S, *)$ if $x \bar{*} y = y * x$. The collection $\overline{\mathbf{C}}$ is the collection of all groupoids $(S, \bar{*})$, where $(S, *) \in \mathbf{C}$. Clearly, $\mathbf{C}$ is in one-one correspondence with $\overline{\mathbf{C}}$.

Below we list a few identities that we will use later. The proofs of these identities one can find in [2] and [9].

A Ward quasigroup $(S, *)$ satisfies the following identities:

(1) $x * x = y * y = r$,

(2) $x * r = x$,

(3) $r * (x * y) = y * x$,

(4) $r * (r * x) = x$,

(5) $(x * y) * z = x * (z * (r * x))$.

Note that a Ward (Ward dual) quasigroup $(S, *)$ has a unique right (left) identity element r. So, we will denote this by $(W, *, r)$ (resp. $(WD, *, r)$). We will denote a double Ward quasigroup by $(DW, *, e)$, although we note that the element e may not be unique.

A double Ward quasigroup $(S, *)$ satisfies the following identities:

(6) $e * e = e$,

(7) $(e * (x * z)) * ((e * y) * z) = x * y$,

(8) $(y * x) * y = y * (x * y) = x$,

(9) $e * x = x * e$,

(10) $x * (x * e) = (e * x) * x = e$,

(11) $x * y = e * ((e * y) * (e * x))$.

The following facts on connections of groups with various types of Ward quasigroups are well-known, or follow readily from [2], [5] and [9].

$(F1)$ $(W, *, r)$ is a Ward quasigroup if and only if there is a group $(W, \circ, r)$ such that $x * y = x \circ y^{-1}$ for all $x, y \in W$.

$(F2)$ $(WD, *, r)$ is a Ward dual quasigroup if and only if there is a group $(WD, \circ, r)$ such that $x * y = y \circ x^{-1}$ for all $x, y \in WD$.

$(F3)$ $(DW, *, e)$ is a double Ward quasigroup if and only if there is a group $(DW, \circ, e)$ such that $x * y = x^{-1} \circ y^{-1}$ for all $x, y \in DW$.

$(F4)$ If $(W, *, r)$ is a Ward quasigroup, then $(W, \circ)$ defined as $x \circ y = x * (r * y)$ is a group with identity r and $x^{-1} = r * x$.

$(F5)$ If $(WD, *, r)$ is a Ward dual quasigroup, then $(WD, \circ)$ defined as $x \circ y = (x * r) * y$ is a group with identity r and $x^{-1} = x * r$.

$(F6)$ If $(DW, *, e)$ is a double Ward quasigroup, then $(DW, \circ)$ defined as $x \circ y = (e * x) * (e * y)$ is a group with identity e and $x^{-1} = e * x$.

The fact $(F6)$ was noted in [5] without proof. Below we give a short proof.

By definition we have

$$(x \circ y) \circ z = (e * ((e * x) * (e * y)) * (e * z) \overset{(11)}{=} (y * x) * (e * z)$$

and

$$x \circ (y \circ z) = (e * x) * (e * ((e * y) * (e * z))) \overset{(11)}{=} (e * x) * (z * y).$$

Since, by (8) and (9), $x = (y * x) * y$ and $z = e * (e * z)$, we have

$$\begin{aligned} x \circ (y \circ z) &= (e * x) * (z * y) = (e * ((y * x) * y)) * ((e * (e * z)) * y) \\ &\overset{(7)}{=} (y * x) * (e * z) = (x \circ y) \circ z. \end{aligned}$$

So, $(DW, *)$ is a semigroup.

Now suppose that $a, b \in DW$. Since $(DW, *, e)$ is a quasigroup, there exists a unique $x \in DW$ such that $x * a = e * b$. So

$$a \circ x = (e * a) * (e * x) \overset{(8,9,11)}{=} e * (x * a) = e * (e * b) \overset{(8,9)}{=} b.$$

If $a \circ y = b$, then $b = (e * a) * (e * y) \overset{(8,9,11)}{=} e * (y * a)$ and so, by (8) and (9), $e * b = b * e = (e * (y * a)) * e = y * a$. But x was unique, so $x = y$. Similarly, there exists a unique element $z \in DW$ such that $z \circ a = b$. So, $(DW, \circ)$ is a group. The facts that e is the identity and $x^{-1} = e * x$ follow from (8) and (10).

As a consequence of $(F1) - (F6)$, we have the following corollaries:

Corollary 2.1. (cf. [2] and [9]) *The collection of all Ward quasigroups is in one-to-one correspondence with the collection of all groups.*

Corollary 2.2. *The collection of all Ward dual quasigroups is in one-to-one correspondence with the collection of all groups.*

Corollary 2.3. (cf. [5]) *The collection of all double Ward quasigroups is in one-to-one correspondence with the collection of all groups.*

The following two facts follow readily from $(F1)$ and $(F3)$ and proofs are omitted.

$(F10)$ If $(W, *, r)$ is a Ward quasigroup, then $(W, \cdot, r)$, where $x \cdot y = (r * x) * y$, is a double Ward quasigroup.

$(F11)$ If $(DW, *, e)$ is a double Ward quasigroup, then $(DW, \cdot, e)$, where $x \cdot y = (e * x) * y$, is a Ward quasigroup.

Also the following fact is true.

($F12$) If $(S,*)$ is a semigroup semilattice V of Ward quasigroups $(W_\alpha, *_{|_{W_\alpha}}, e_\alpha)$ $(\alpha \in V)$ and satisfies the identity $(x*y)*(z*w) = (x*(w^{-1}*y^{-1}))*z$, then $E(S,*) = \{e_\alpha \mid \alpha \in V\}$, $e_\alpha * e_\beta = e_{\alpha\beta}$ and the mapping $\Psi(e_\alpha) = \alpha$ restricted to $E(S,*)$ is an isomorphism between $(E(S,*), *_{|_{E(S,*)}})$ and V.

Proof. First, we note that each $(W_\alpha, *_{|_{W_\alpha}}, e_\alpha)$ is an inverse groupoid, with $x_\alpha^{-1} = e_\alpha * x_\alpha$. Since a semigroup semilattice groupoid of inverse groupoids is an inverse groupoid, $(S,*)$ is an inverse groupoid. Hence, the identity $(x*y)*(z*w) = (x*(w^{-1}*y^{-1}))*z$ has a clear meaning. We call this identity $(\star)$.

Now, by definition, $e_\alpha * e_\beta \in W_{\alpha\beta}$. Therefore, $e_{\alpha\beta} \overset{(1)}{=} (e_\alpha * e_\beta) * (e_\alpha * e_\beta) \overset{(\star)}{=} (e_\alpha * e_\beta) * e_\alpha$. Then, $(e_\alpha * e_\beta) * e_\beta \overset{(\star)}{=} (e_\alpha * (e_\beta * e_\alpha)) * e_\beta \overset{(\star)}{=} (e_\alpha * e_\alpha) * (e_\beta * e_\beta) = e_\alpha * e_\beta = (e_\alpha * e_\beta) * e_{\alpha\beta} = (e_\alpha * e_\beta) * ((e_\alpha * e_\beta) * e_\alpha) \overset{(\star)}{=} (e_\alpha * (e_\alpha * e_\beta)) * (e_\alpha * e_\beta) \overset{(\star)}{=} ((e_\alpha * (e_\beta * e_\alpha)) * e_\alpha) * (e_\alpha * e_\beta) \overset{(\star)}{=} ((e_\alpha * e_\beta) * e_\alpha) * (e_\alpha * e_\beta) = e_{\alpha\beta} * (e_\alpha * e_\beta)$. So, $(e_\alpha * e_\beta) * e_\beta = e_\alpha * e_\beta = e_{\alpha\beta} * (e_\alpha * e_\beta) = ((e_\alpha * e_\beta) * e_\alpha) * ((e_\alpha * e_\beta) * e_\beta) \overset{(\star)}{=} ((e_\alpha * e_\beta) * (e_\beta * e_\alpha)) * (e_\alpha * e_\beta)$. But, since $(e_\alpha * e_\beta) * (e_\beta * e_\alpha) \in W_{\alpha\beta}$, $W_{\alpha\beta}$ is a Ward quasigroup and $e_{\alpha\beta} * (e_\alpha * e_\beta) = ((e_\alpha * e_\beta) * (e_\beta * e_\alpha)) * (e_\alpha * e_\beta)$, $e_{\alpha\beta} = (e_\alpha * e_\beta) * (e_\beta * e_\alpha) \overset{(1)}{=} (e_\alpha * e_\beta) * (e_\alpha * e_\beta)$ and $e_\alpha * e_\beta = e_\beta * e_\alpha$. But this implies $e_\alpha * (e_\beta * e_\sigma) = e_\alpha * (e_\sigma * e_\beta) = (e_\alpha * e_\alpha) * (e_\sigma * e_\beta) \overset{(\star)}{=} (e_\alpha * (e_\beta * e_\alpha)) * e_\sigma \overset{(\star)}{=} (e_\alpha * e_\beta) * e_\sigma$. Then, $e_{\alpha\beta} = (e_\alpha * e_\beta) * (e_\alpha * e_\beta) \overset{(\star)}{=} (e_\alpha * e_\beta) * e_\alpha = e_\alpha * (e_\beta * e_\alpha) = e_\alpha * (e_\alpha * e_\beta) = (e_\alpha * e_\alpha) * e_\beta = e_\alpha * e_\beta$. It follows that the mapping $e_\alpha \mapsto \alpha$ is an isomorphism between $E(S,*)$ and V. □

Dually, we have

($F13$) If $(S,*)$ is a semigroup semilattice V of Ward dual quasigroups $(W_\alpha, *_{|_{W_\alpha}}, e_\alpha)$ $(\alpha \in V)$ and satisfies the identity $(x*y)*(z*w) = y*((z^{-1}*x^{-1})*w)$, then $E(S,*) = \{e_\alpha \mid \alpha \in V\}$, $e_\alpha * e_\beta = e_{\alpha\beta}$ and the mapping $\Psi(e_\alpha) = \alpha$ restricted to $E(S,*)$ is an isomorphism between $(E(S,*), *_{|_{E(S,*)}})$ and V.

($F10$) and ($F11$) are easily proved using ($F1$) and ($F3$). For example, if $(W,*,r)$ is a Ward quasigroup then by ($F1$) $x \cdot y = (r*x)*y = (r \circ x^{-1}) \circ y^{-1} = x^{-1} \circ y^{-1}$ and so $(W,\cdot,r)$ is a double Ward quasigroup.

Proposition 2.4. *If $(S,*)$ is a semigroup semilattice V of double Ward quasigroups $(DW_\alpha, *_{|_{DW_\alpha}}, e_\alpha)$, $(\alpha \in V)$, then the following conditions are equivalent*

(i) $\{e_\alpha \mid \alpha \in V\} \cong V$,

(ii) *for all* $\alpha,\beta,\gamma,\sigma \in V$, $(e_\alpha * e_\beta) * (e_\gamma * e_\sigma) = e_\beta * ((e_\gamma * e_\sigma) * e_\alpha)$,

(iii) *the mapping* $e_\alpha \mapsto \alpha$ *is an isomorphism from* $(\{e_\alpha \mid \alpha \in V\}, *_{|_{\{e_\alpha \mid \alpha \in V\}}})$ *to* V.

Proof. $(i) \Rightarrow (ii)$: Let $\Psi : (\{e_\alpha \mid \alpha \in V\}, *_{|\{e_\alpha \mid \alpha \in V\}}) \to V$ be an isomorphism. Then $\Psi((e_\alpha * e_\beta) * (e_\gamma * e_\sigma)) = \Psi(e_\alpha)\Psi(e_\beta)\Psi(e_\gamma)\Psi(e_\sigma) = \Psi(e_\beta)[[\Psi(e_\sigma)\Psi(e_\gamma)]\Psi(e_\alpha)] = \Psi(e_\beta * ((e_\sigma * e_\gamma) * e_\alpha))$, because V is a semigroup semilatice. Since Ψ is one-one, the last implies (ii).

$(ii) \Rightarrow (iii)$: First, we prove that $e_\alpha * e_\beta = e_\beta * e_\alpha$. By hypothesis, we have

$$(12) \quad (e_\alpha * e_\beta) * (e_\gamma * e_\sigma) = e_\beta * ((e_\sigma * e_\gamma) * e_\alpha).$$

From this we obtain

$$(13) \quad (e_\alpha * e_\beta) * e_\sigma = e_\beta * (e_\sigma * e_\alpha),$$

which implies

$$(14) \quad (e_\beta * e_\alpha) * e_\beta = e_\alpha * e_\beta = e_\alpha * (e_\beta * e_\alpha).$$

Now, $e_{\alpha\beta} \overset{(8)}{=} ((e_\alpha * e_\beta) * e_{\alpha\beta}) * (e_\alpha * e_\beta) \overset{(13)}{=} (e_\beta * (e_{\alpha\beta} * e_\alpha)) * (e_\alpha * e_\beta) \overset{(12)}{=} (e_\beta * ((e_\alpha * e_{\alpha\beta}) * e_\beta)) * (e_\alpha * e_\beta) \overset{(13)}{=} (e_\beta * (e_{\alpha\beta} * (e_\beta * e_\alpha))) * (e_\alpha * e_\beta) \overset{(12)}{=} (e_\beta * (e_{\alpha\beta} * (e_\beta * e_\alpha))) * (e_\alpha * e_\beta)) \overset{(12)}{=} (e_\beta * ((e_{\alpha\beta} * (e_\alpha * e_\beta)) * e_{\alpha\beta})) * (e_\alpha * e_\beta) \overset{(8)}{=} (e_\beta * (e_\alpha * e_\beta)) * (e_\alpha * e_\beta) \overset{(14)}{=} (e_\beta * e_\alpha) * (e_\alpha * e_\beta) \overset{(12)}{=} e_\alpha * ((e_\beta * e_\alpha) * e_\beta) \overset{(14)}{=} e_\alpha * (e_\alpha * e_\beta) \overset{(12)}{=} e_\alpha * ((e_\beta * e_\alpha) * e_\alpha) \overset{(14)}{=} e_\alpha * (e_\alpha * (e_\alpha * e_\beta)) = e_\alpha * e_{\alpha\beta}$.

Then,

$$(15) \quad e_{\alpha\beta} * e_\alpha \overset{(14)}{=} e_{\alpha\beta} * (e_\alpha * e_{\alpha\beta}) = e_{\alpha\beta} * e_{\alpha\beta} = e_{\alpha\beta} = e_\alpha * (e_\alpha * e_\beta).$$

Since we have proved above that $e_{\alpha\beta} = (e_\beta * e_\alpha) * (e_\alpha * e_\beta)$, it follows from (8) that $(e_\alpha * e_\beta) * e_{\alpha\beta} = e_\beta * e_\alpha$. So, $e_\beta * e_\alpha = (e_\alpha * e_\beta) * e_{\alpha\beta} \overset{(14)}{=} e_\beta * (e_{\alpha\beta} * e_\alpha) \overset{(15)}{=} e_\beta * e_{\alpha\beta} \overset{(15)}{=} e_\beta * (e_\alpha * (e_\alpha * e_\beta)) \overset{(14)}{=} e_\beta * ((e_\beta * e_\alpha) * e_\alpha) \overset{(12)}{=} (e_\alpha * e_\beta) * (e_\alpha * e_\beta)$, which means that $(e_\alpha * e_\beta) * (e_\alpha * e_\beta) = (e_\alpha * e_\beta) * e_{\alpha\beta}$. Since $(DW_{\alpha\beta}, *_{|DW_{\alpha\beta}}, e_{\alpha\beta})$ is a quasigroup, $e_{\beta\alpha} = e_{\alpha\beta} = e_\alpha * e_\beta = e_\beta * e_\alpha$. Also, $(e_\alpha * e_\beta) * e_\gamma = e_{\alpha\beta} * e_\gamma = e_{(\alpha\beta)\gamma} = e_{\alpha(\beta\gamma)} = e_\alpha * (e_\beta * e_\gamma)$. Finally, the mapping $\Psi : (\{e_\alpha \mid \alpha \in V\}, *) \to V$ defined as $\Psi(e_\alpha) = \alpha$ satisfies $\Psi(e_\alpha * e_\beta) = \Psi(e_{\alpha\beta}) = \alpha\beta = \Psi(\alpha)\Psi(\beta)$ and so, since it is clearly one-one and onto V, Ψ is an isomorphism.

$(iii) \Rightarrow (i)$: This is obvious. □

3. Semigroup semilattices of groups

We have seen that Ward quasigroups, Ward dual quasigroups and double Ward quasigroups are in one-to-one correspondence with groups. In this section, we extend these results to semigroups that are semilattices of groups. Note that in semigroup theory a *semilattice*, a *union of groups* and a *semilattice of groups* are, by definition, semigroups. However, the definition of a semilattice (or idempotent

groupoid) $(S,\cdot)$ of groupoids $(S_\alpha, *_{|_{S_\alpha}})$ $(\alpha \in T)$ results in structures that are not necessarily associative, even when the S_α $(\alpha \in T)$ are all groups. Therefore, we use the terms *semigroup semilattice*, *semigroup union of groups* and *semigroup semilattice of groups*, terms that are redundant for semigroup theorists. The idea is a straightforward one. We simply "extend" the binary product that gives the bijection between groups and Ward quasigroups, for example, to the semigroup semilattice of groups and to the resultant structure(s). So, we are working with structures that result from defining binary operations on a semigroup semilattice of groups $(S,\cdot)$ as follows: $x * y = x \cdot y^{-1}$ (called *right division*), $x * y = x^{-1} \cdot y$ (called *left division*) and $x * y = x^{-1} \cdot y^{-1}$ (called *double division*). This is possible because a semigroup semilattice of groups is an inverse semigroup; that is, each element $x \in S$ has a unique inverse x^{-1} that is the inverse of the element x in the group to which it belongs [3, Theorem 4.11].

On the resultant structures $(S,*)$ we define binary operations as follows, respectively:

$$x_\alpha \otimes y_\beta = x_\alpha * (e_{\alpha\beta} * y_\beta),$$
$$x_\alpha \otimes y_\beta = (x_\alpha * e_{\alpha\beta}) * y_\beta,$$
$$x_\alpha \otimes y_\beta = (e_{\alpha\beta} * x_\alpha) * (e_{\alpha\beta} * y_\beta).$$

These structures $(S,\otimes)$ turn out to be semigroup semilattices of groups. In each of these three cases, the mappings $(S,\cdot) \to (S,*)$ and $(S,*) \to (S,\otimes)$ are inverse mappings. Hence, we find three different collections of structures, each of which is in one-to-one correspondence with the collection **SLG** of all semigroup semilattices of groups.

Lemma 3.1. (cf. [3, Theorem 4.11]) *A semigroup $(S,\cdot)$ is a semigroup semilattice V of groups $(G_\alpha, \cdot_{|_{G_\alpha}}, e_\alpha)$ $(\alpha \in V)$ if and only if $(S,\cdot)$ is a semigroup union of groups and has commuting idempotents if and only if $(S,\cdot)$ is an inverse semigroup that is a semigroup union of groups if and only if $(S,\cdot)$ is a semigroup and a semigroup semilattice $V \cong E(S,\cdot)$ of groups.*

Note that the following identity holds in inverse semigroups:

(16) $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$.

If $(S,\cdot)$ is a semigroup and a semilattice V of groups then it follows from Lemma 3.1 that

(17) $e_\alpha \cdot e_\beta = e_{\alpha\beta} = e_{\beta\alpha} = e_\beta \cdot e_\alpha$

for all $\alpha, \beta \in V$.

Lemma 3.2. *Suppose that $(S,\cdot)$ is a semigroup semilattice V of groups (G_α, e_α) $(\alpha \in V)$ and that $x_\alpha * y_\beta = x_\alpha \cdot y^{-1}$ for all $x_\alpha \in G_\alpha$, $y_\beta \in G_\beta$ and $\alpha, \beta \in V$. Then*

(18) *$(S,*)$ is an inverse groupoid with $x_\alpha^{-1} = e_\alpha * x_\alpha$ $(\alpha \in V)$,*

(19) $E(S,*) \cong E(S,\cdot) \cong V$,

(20) $(S,*)$ *is a semigroup semilattice* V *of Ward quasigroups* $(G_\alpha, *_{|G_\alpha}, e_\alpha)$ $(\alpha \in V)$,

(21) $(x_\alpha * y_\beta) * (z_\sigma * w_\gamma) = [x_\alpha * (w_\gamma^{-1} * y_\beta^{-1})] * z_\sigma$,

(22) $x_\alpha * (e_{\alpha\beta} * y_\beta) = x_\alpha * y_\beta^{-1}$,

(23) $x_\alpha * y_\beta = (y_\beta * x_\alpha)^{-1}$.

Proof. (18): It is straightforward to calculate that x_α^{-1}, the inverse of x_α in the group to which it belongs, is the unique inverse of x_α in $(S,*)$. That is, $x_\alpha^{-1} = e_\alpha * x_\alpha$.

(19): $x_\alpha = x_\alpha * x_\alpha$ if and only if $x_\alpha = x_\alpha \cdot x_\alpha^{-1} = e_\alpha$, the identity of the group to which x_α belongs. Then, $e_\alpha * e_\beta = e_\alpha \cdot e_\beta^{-1} = e_\alpha \cdot e_\beta \overset{(17)}{=} e_{\alpha\beta}$. Since, by Lemma 3.1, in $(S,\cdot)$ we have $E(S,\cdot) \cong V$, $E(S,*) \cong E(S,\cdot) \cong V$.

(20): Since $x_\alpha * y_\beta = x_\alpha \cdot y_\beta^{-1} \in G_\alpha \cdot G_\beta \subseteq G_{\alpha\beta}$. Since $x_\alpha * y_\alpha = x_\alpha \cdot y_\alpha^{-1}$ in each $(G_\alpha, *_{|G_\alpha}, e_\alpha)$, by fact $(F1)$, $(G_\alpha, *_{|G_\alpha}, e_\alpha)$ is a Ward quasigroup for all $\alpha \in V$. By definition then, $(S,*)$ is a semigroup semilattice V of Ward quasigroups $(G_\alpha, *_{|G_\alpha}, e_\alpha)$ $(\alpha \in V)$.

(21): Using the facts that $x_\alpha * y_\beta = x_\alpha \cdot y_\beta^{-1}$ and $(x_\alpha \cdot y_\beta)^{-1} \overset{(16)}{=} y_\beta^{-1} \cdot x_\alpha^{-1}$ it is straightforward to calculate that $(x_\alpha * y_\beta) * (z_\sigma * w_\gamma) = x_\alpha \cdot y_\beta^{-1} \cdot w_\gamma \cdot z_\sigma^{-1} = [x_\alpha * (w_\gamma^{-1} * y_\beta^{-1})] * z_\sigma$.

(22): $x_\alpha * (e_{\alpha\beta} * y_\beta) = x_\alpha \cdot (e_{\alpha\beta} \cdot y_\beta^{-1})^{-1} \overset{(16)}{=} x_\alpha \cdot (y_\beta \cdot e_{\alpha\beta}^{-1}) = (x_\alpha \cdot y_\beta) \cdot e_{\alpha\beta} = x_\alpha \cdot y_\beta = x_\alpha * y_\beta^{-1}$.

(23): $(x_\alpha * y_\beta)^{-1} = (x_\alpha \cdot y_\beta^{-1})^{-1} \overset{(16)}{=} y_\beta \cdot x_\alpha^{-1} = y_\beta * x_\alpha$. □

Definition 3.3. If $(S,\cdot)$ is a semigroup semilattice V of groups (G_α, e_α) $(\alpha \in V)$ and $x * y = x \cdot y^{-1}$, then we denote $(S,*)$ by $SLWQ(S,\cdot)$. We define **SLWQ** as the collection of all semigroup semilattices V of Ward quasigroups $(G_\alpha, *_{|G_\alpha}, e_\alpha)$ $(\alpha \in V)$ that satisfy (21). In particular, $SLWQ(S,\cdot) \in$ **SLWQ**.

Note once again that a semigroup semilattice of inverse groupoids is an inverse groupoid. So, conditions (21), (22) and (23) have a clear meaning.

Lemma 3.4. *Suppose that* $(S,*)$ *is a semigroup semilattice* V *of Ward quasigroups* $(W_\alpha, *_{|W_\alpha}, e_\alpha)$ $(\alpha \in V)$ *and satisfies* (21). *Define* $x_\alpha \cdot y_\beta = x_\alpha * (e_{\alpha\beta} * y_\beta)$. *Then* $(S,\cdot)$ *is a semigroup and a semigroup semilattice* V *of groups* $(W_\alpha, *_{|W_\alpha}, e_\alpha)$ $(\alpha \in V)$ *with* $V \cong E(S,\cdot) \cong E(S,*)$.

Proof. As previously noted in the proof of $(F12)$, since each $(W_\alpha, *_{|_{W_\alpha}}, e_\alpha)$ is an inverse groupoid, with $x_\alpha^{-1} = e_\alpha * x_\alpha$and since a semigroup semilattice of inverse groupoids is an inverse groupoid, $(S, *)$ is an inverse groupoid.

We prove that (21) implies (22). We have

$x_\alpha*(e_{\alpha\beta}*y_\beta) = (x_\alpha*e_\alpha)*(e_{\alpha\beta}*y_\beta) \overset{(21)}{=} [x_\alpha*(y_\beta^{-1}*e_\alpha^{-1})]*e_{\alpha\beta} = [x_\alpha*(y_\beta^{-1}*e_\alpha)] =$

$(x_\alpha * e_\alpha) * (y_\beta^{-1} * e_\alpha) \overset{(21)}{=} [x_\alpha * (e_\alpha * e_\alpha)] * y_\beta^{-1} = (x_\alpha * e_\alpha) * y_\beta^{-1} = x_\alpha * y_\beta^{-1},$

so, (22) is valid.

Next, we prove that (21) implies (23). Since we have $x_\alpha * y_\beta = x_\alpha * (y_\beta^{-1})^{-1} \overset{(22)}{=} x_\alpha * (e_{\alpha\beta} * y_\beta^{-1})$, then $x_\alpha * y_\beta = x_\alpha * (e_{\alpha\beta} * y_\beta^{-1}) \overset{(5)}{=} [e_\alpha * (e_\alpha * x_\alpha)] * (e_{\alpha\beta} * y_\beta^{-1}) \overset{(21)}{=} [e_\alpha*(y_\beta*x_\alpha)]*e_{\alpha\beta} = [e_\alpha*(y_\beta*x_\alpha)]*(e_{\alpha\beta}*e_{\alpha\beta}) \overset{(21)}{=} (e_\alpha*[e_{\alpha\beta}*(y_\beta*x_\alpha)^{-1}])*e_{\alpha\beta} = e_\alpha * (y_\beta * x_\alpha) = (e_\alpha * e_\alpha) * [(y_\beta * x_\alpha) * e_{\alpha\beta}] \overset{(21)}{=} [e_\alpha * (e_{\alpha\beta} * e_\alpha)] * (y_\beta * x_\alpha) \overset{(F12)}{=} e_{\alpha\beta} * (y_\beta * x_\alpha) = (y_\beta * x_\alpha)^{-1}$, so, (23) is valid.

Now $x_\alpha = x_\alpha \cdot x_\alpha$ if and only if $x_\alpha = x_\alpha * (e_\alpha * x_\alpha) = x_\alpha * e_\alpha$ if and only if $e_\alpha = e_\alpha*x_\alpha = x_\alpha*x_\alpha$ if and only if $x_\alpha = e_\alpha$. Also, $e_\alpha*e_\beta = [e_\alpha*(e_\alpha*e_\alpha)]*e_\beta) \overset{(21)}{=} e_\alpha * (e_\beta * e_\alpha)$. Then, $e_\alpha \cdot e_\beta = e_\alpha * (e_{\alpha\beta} * e_\beta) = (e_\alpha * e_\alpha) * (e_{\alpha\beta} * e_\beta) \overset{(21)}{=} [e_\alpha * (e_\beta * e_\alpha)] * e_{\alpha\beta} = e_\alpha * (e_\beta * e_\alpha) \overset{(21)}{=} e_\alpha * e_\beta$. So, the operations $\cdot$ and $*$ coincide on $E(S, *)$. Thus, $E(S, \cdot) \cong E(S, *)$. Using $(F12)$, $E(S, \cdot) \cong E(S, *) \cong V$ is a semigroup semilattice. Since, for each $(W_\alpha, *_{|_{W_\alpha}}, e_\alpha)$, $x_\alpha \cdot y_\alpha = x_\alpha * (e_\alpha * y_\alpha)$, by $(F4)$, each $(W_\alpha, \cdot_{|_{W_\alpha}}, e_\alpha)$ is a group. Since $x_\alpha \cdot y_\beta = x_\alpha*(e_{\alpha\beta} * y_\beta) \in W_{\alpha\beta}$, $W_\alpha \cdot W_\beta \subseteq W_{\alpha\beta}$, and so $(S, \cdot)$ is a semigroup semilattice V of groups. So, we only need to prove that $(S, \cdot)$ is a semigroup.

We have $(x_\alpha \cdot y_\beta) \cdot z_\gamma = [x_\alpha*(e_{\alpha\beta}*y_\beta)]*(e_{\alpha\beta\gamma}*z_\gamma) \overset{(22)}{=} (x_\alpha*y_\beta^{-1})*(e_{\alpha\beta\gamma}*z_\gamma) \overset{(21)}{=} [x_\alpha * (z_\gamma^{-1} * y_\beta)] * e_{\alpha\beta\gamma} = [x_\alpha * (z_\gamma^{-1} * y_\beta)] \overset{(23)}{=} x_\alpha * (y_\beta * z_\gamma^{-1})^{-1} \overset{(22)}{=} x_\alpha * [e_{\alpha\beta\gamma} * (y_\beta * z_\gamma^{-1})] \overset{(22)}{=} x_\alpha * [e_{\alpha\beta\gamma} * [y_\beta * (e_{\beta\gamma} * z_\gamma)]) = x_\alpha \cdot (y_\beta \cdot z_\gamma)$. □

Corollary 3.5. *Let $(S, *)$ be a semigroup semilattice V of Ward quasigroups $(W_\alpha, *_{|_{W_\alpha}}, e_\alpha)$ $(\alpha \in V)$. If $(S, *)$ satisfies* (21)*, then*

(*i*) *it satisfies* (22) *and* (23)*,*

(*ii*) *there exists $(S, \cdot) \in$ **SLG** such that $x * y = x \cdot y^{-1}$ for all $x, y \in S$.*

Proof. Part (*i*) was proved in Lemma 3.4. For part (*ii*), let $(S, \cdot)$ be as in our Lemma 3.4. Then, as proved in Lemma 3.4, $(S, \cdot) \in$ **SLG**. Also, $x_\alpha \cdot y_\beta^{-1} = (x_\alpha*e_\alpha)*(e_{\alpha\beta}*y_\beta^{-1}) \overset{(21)}{=} [x_\alpha*(y_\beta*e_\alpha)]*e_{\alpha\beta} = [x_\alpha*(y_\beta*e_\alpha)] = [(x_\alpha*e_\alpha)*(y_\beta*e_\alpha)] \overset{(21)}{=} (x_\alpha * e_\alpha) * y_\beta = x_\alpha * y_\beta$. □

Definition 3.6. Let $(S,*)$ be a semigroup semilattice V of Ward quasigroups $(W_\alpha, *_{|_{W_\alpha}}, e_\alpha)$ $(\alpha \in V)$ that satisfies (21), and if we define $x_\alpha \cdot y_\beta = x_\alpha * (e_{\alpha\beta} * y_\beta)$, then we denote the semigroup semilattice V of groups $(S,\cdot)$ as $SLG(S.*)$.

Theorem 3.7. *For all* $(S,*) \in$ **SLWQ**, $SLWQ(SLG(S,*)) = (S,*)$ *and for all* $(S,\cdot) \in$ **SLG**, $SLG(SLWQ(S,\cdot)) = (S,\cdot)$.

Proof. In $SLG(S,*)$ the product is $x_\alpha \cdot y_\beta = x_\alpha * (e_{\alpha\beta} * y_\beta)$. The product $\otimes$ in $SLWQ(SLG(S,*))$ is $x_\alpha \otimes y_\beta = x_\alpha \cdot y_\beta^{-1}$. So, $x_\alpha * y_\beta = (x_\alpha * y_\beta) * (e_{\alpha\beta} * e_{\alpha\beta}) \overset{(22)}{=} (x_\alpha * (e_{\alpha\beta}^{-1} * y_\beta^{-1})) * e_{\alpha\beta} = x_\alpha * (e_{\alpha\beta} * y_\beta^{-1}) = x_\alpha \cdot y_\beta^{-1} = x_\alpha \otimes y_\beta$ and consequently, $SLWQ(SLG(S,*)) = (S,*)$.

In $SLWQ(S,\cdot)$ the product is $x*y = x\cdot y^{-1}$. The product $\oplus$ in $SLG(SLWQ(S,\cdot))$ is $x_\alpha \oplus y_\beta = x_\alpha * (e_{\alpha\beta} * y_\beta) = x_\alpha \cdot (e_{\alpha\beta} \cdot y_\beta^{-1})^{-1} \overset{(12)}{=} x_\alpha \cdot y_\beta \cdot e_{\alpha\beta}^{-1} = x_\alpha \cdot y_\beta$. Hence, $SLG(SLWQ(S,\cdot)) = (S,\cdot)$. □

The second part of the following Corollary can be viewed as an "extension" of $(F1)$.

Corollary 3.8. *There is a one-to-one correspondence between semigroup semilattices of groups* **SLG** *and groupoids* $(S,*)$ *that are semigroup semilattices* V *of Ward quasigroups* $(W_\alpha, *_{|_{W_\alpha}}, e_\alpha)$ *and that satisfy* (21). *Also,* $(S,*) \in$ **SLWQ** *if and only if there exists* $(S,\cdot) \in$ **SLG** *such that* $x * y = x \cdot y^{-1}$ *for all* $x, y \in S$.

Corollary 3.9. *There is a one-to-one correspondence between semigroup semilattices of abelian groups and groupoids* $(S,*)$ *that are semigroup semilattices* V *of medial Ward quasigroups* $(W_\alpha, *_{|_{W_\alpha}}, e_\alpha)$ $(\alpha \in V)$ *and that satisfy* (21).

Proof. The proof here follows that of Lemmas 3.2, 3.4 and Theorem 3.7, using the additional fact that a groupoid is a medial Ward quasigroup if and only if it is induced by an abelian group. □

Lemma 3.10. *Let* $(S,\cdot)$ *be a semigroup semilattice* V *of groups* $(G_\alpha, *_{|_{G_\alpha}}, e_\alpha)$ $(\alpha \in V)$ *and let* $x * y = x^{-1} \cdot y$. *Then*

(24) $(S,*)$ *an inverse groupoid with* $x_\alpha^{-1} = x_\alpha * e_\alpha$, $(\alpha \in V)$,

(25) $E(S,*) \cong E(S,\cdot) \cong V$,

(26) $(S,*)$ *is a semigroup semilattice* V *of Ward dual quasigroups* $(S_\alpha, *_{|_{S_\alpha}}, e_\alpha)$ $(\alpha \in V)$,

(27) $(x_\alpha * y_\beta) * (z_\gamma * w_\sigma) = y_\beta * ((z_\gamma^{-1} * x_\alpha^{-1}) * w_\sigma)$,

(28) $(x_\alpha * e_{\alpha\beta}) * y_\beta = x_\alpha^{-1} * y_\beta$,

(29) $x_\alpha * y_\beta = (y_\beta * x_\alpha)^{-1}$.

Proof. Note that it follows from Lemma 3.1 that $\mathbf{SLG} = \overline{\mathbf{SLG}}$. Since $x\bar{*}y = y * x = y^{-1} \cdot x = x\bar{\cdot}y^{-1}$ and $(S, \bar{\cdot}) \in \mathbf{SLG}$, $(S, \bar{*})$ satisfies (18) to (23). Hence, $(S, *)$ satisfies (24) to (29). □

Definition 3.11. $SLWD(S, \cdot)$ will denote $(S, *)$ in Lemma 3.10 above. We denote the collection of all groupoids $(S, *)$ that are semigroup semilattices V of Ward dual quasigroups $(WD_\alpha, *_{|_{WD_\alpha}}, e_\alpha)$ $(\alpha \in V)$ that satisfy (27) as **SLWDQ**. So, $SLWD(S, \cdot) = (S, *) \in \mathbf{SLWDQ}$.

Lemma 3.12. *Suppose that $(S, *)$ is a semigroup semilattice V of Ward dual quasigroups $(WD_\alpha, *_{|_{WD_\alpha}}, e_\alpha)$ $(\alpha \in V)$ and satisfies* (27)*. Then $(S, \cdot)$ with the operation $x_\alpha \cdot y_\beta = (x_\alpha * e_{\alpha\beta}) * y_\beta$, is a semigroup and a semigroup semilattice V of groups.*

Proof. It is clear that $(S, \bar{*})$ is a semigroup semilattice V of Ward quasigroups $(WD_\alpha, *_{|_{WD_\alpha}}, e_\alpha)$ $(\alpha \in V)$ and satisfies (21). Also, $x_\alpha \bar{\cdot} y_\beta = (y_\beta * e_{\alpha\beta}) * x_\alpha = x_\alpha \bar{*} (e_{\alpha\beta} \bar{*} y_\beta)$. By Lemma 3.4, $(S, \bar{\cdot})$ is a semigroup and a semigroup semilattice V of groups with $V \cong E(S, \bar{\cdot}) \cong E(S, \bar{*})$. Hence, $(S, \cdot)$ is a semigroup and a semigroup semilattice V of groups with $V \cong E(S, \cdot) \cong E(S, *)$. □

Definition 3.13. $SLG(S, *)$ will denote $(S, \cdot)$ in Lemma 3.12 above.

Theorem 3.14. *For all $(S, \cdot) \in \mathbf{SLG}$, $SLG(SLWD(S, \cdot)) = (S, \cdot)$ and for all $(S, *) \in \mathbf{SLWDQ}$, $SLWD(SLG(S, *)) = (S, *)$.*

Proof. Observe that the product in $SLWD(S, \cdot)$ is $x * y = x^{-1} \cdot y$. The product in $SLG(SLWD(S, \cdot))$ is

$$x_\alpha \otimes y_\beta = (x_\alpha * e_{\alpha\beta}) * y_\beta = (x_\alpha^{-1} \cdot e_{\alpha\beta}) * y_\beta \overset{(12)}{=} e_{\alpha\beta} \cdot x_\alpha \cdot y_\beta = x_\alpha \cdot y_\beta.$$

Hence, $SLG(SLWD(S, \cdot)) = (S, \cdot)$.

The product in $SLG(S, *)$ is $x_\alpha \cdot y_\beta = (x_\alpha * e_{\alpha\beta}) * y_\beta$. Hence, the product in $SLWD(SLG(S, *))$ is $x_\alpha \oplus y_\beta = x^{-1} \cdot y = ((x_\alpha * e_\alpha) * e_{\alpha\beta}) * y_\beta \overset{(27)}{=} x_\alpha * y_\beta$ and so $SLWD(SLG(S, *)) = (S, *)$. □

Corollary 3.15. *There is a one-to-one correspondence between semigroup semilattices of groups* **SLG** *and groupoids $(S, *)$ that are semigroup semilattices V of Ward dual quasigroups $(WD_\alpha, *_{|_{WD_\alpha}}, e_\alpha)$ $(\alpha \in V)$ and that satisfy* (24)*,* (26) *and* (27)*. Also, $(S, *) \in \mathbf{SLWDQ}$ if and only if there exists $(S, \cdot) \in \mathbf{SLG}$ such that $x * y = x^{-1} \cdot y$ for all $x, y \in S$.*

Corollary 3.16. *There is a one-to-one correspondence between semigroup semilattices of abelian groups and groupoids $(S, *)$ that are semigroup semilattices V of unipotent, left-unital right modular quasigroups $(Q_\alpha, *_{|_\alpha}, e_\alpha)$ satisfying* (27)*.*

Proof. A Ward dual quasigroup is a unipotent, left-unital right modular quasigroup if and only if it is medial if and only if it is induced by an abelian group. Using this fact, the proof of Corollary 3.16 exactly follows those of Lemmas 3.10, 3.12 and Theorem 3.14. □

Lemma 3.17. *Let $(S,\cdot)$ be a semigroup semilattice V of groups $(G_\alpha, *_{|_{G_\alpha}}, e_\alpha)$ $(\alpha \in V)$ such that $x_\alpha * y_\beta = x^{-1} \cdot y_\beta^{-1}$. Then*

(30) $(\{e_\alpha \mid \alpha \in V\}, *) \cong (\{e_\alpha \mid \alpha \in V\}, \cdot) \cong V$ *is a semigroup semilattice,*

(31) $(S,*)$ *is a semigroup semilattice V of double Ward quasigroups $(G_\alpha, *_{|_{G_\alpha}}, e_\alpha)$ $(\alpha \in V)$,*

(32) $(S,*)$ *satisfies the identity*

$$(e_{\alpha\beta\gamma} * ((e_{\alpha\beta} * x_\alpha) * (e_{\alpha\beta} * y_\beta))) * (e_{\alpha\beta\gamma} * z_\gamma) = (e_{\alpha\beta\gamma} * x_\alpha) * (e_{\alpha\beta\gamma} * ((e_{\beta\gamma} * y_\beta) * (e_{\beta\gamma} * z_\gamma))),$$

(33) $(S,*)$ *satisfies the identity* $x_\alpha * y_\beta = (e_{\alpha\beta} * (e_\alpha * x_\alpha)) * (e_{\alpha\beta} * (e_\beta * y_\beta))$.

Proof. (30): For any $e_\alpha, e_\beta \in V$, $e_\alpha * e_\beta = e_\alpha^{-1} \cdot e_\beta^{-1} = e_\alpha \cdot e_\beta$. Then, $e_\alpha * e_\beta = e_\alpha \cdot e_\beta = e_\beta \cdot e_\alpha = e_{\alpha\beta}$, by Lemma 3.1. Hence, $(e_\alpha * e_\beta) * e_\gamma = e_{\alpha\beta} * e_\gamma = e_{(\alpha\beta)\gamma} = e_{\alpha(\beta\gamma)} = e_\alpha * (e_\beta * e_\gamma)$. By Lemma 3.1, $(\{e_\alpha \mid \alpha \in V\}, *) \cong V$ is a semigroup semilattice and so (30) is valid.

(31): Each $(G_\alpha, *_{|_{G_\alpha}}, e_\alpha)$ has product $x_\alpha * y_\alpha = x_\alpha^{-1} \cdot y_\alpha^{-1}$ and therefore, by $(F3)$, each $(G_\alpha, *_{|_{G_\alpha}}, e_\alpha)$ is a double Ward quasigroup. Since $x_\alpha * y_\beta = x_\alpha^{-1} \cdot y_\beta^{-1} \in G_{\alpha\beta}$, (31) is valid.

(32): We have

$$\begin{aligned}
&(e_{\alpha\beta\gamma} * ((e_{\alpha\beta} * x_\alpha) * (e_{\alpha\beta} * y_\beta))) * (e_{\alpha\beta\gamma} * z_\gamma) = \\
&(e_{\alpha\beta\gamma} * ((e_{\alpha\beta}^{-1} \cdot x_\alpha^{-1}) * (e_{\alpha\beta}^{-1} \cdot y_\beta^{-1}))) * (e_{\alpha\beta\gamma}^{-1} \cdot z_\gamma^{-1}) = \\
&(e_{\alpha\beta\gamma} * (x_\alpha \cdot y_\beta)) * (e_{\alpha\beta\gamma}^{-1} \cdot z_\gamma^{-1}) = (e_{\alpha\beta\gamma}^{-1} \cdot y_\beta^{-1} \cdot x_\alpha^{-1})^{-1} \cdot z_\gamma \cdot e_{\alpha\beta\gamma} = \\
&(x_\alpha \cdot y_\beta) \cdot (e_{\alpha\beta\gamma} \cdot (z_\gamma \cdot e_{\alpha\beta\gamma})) = (x_\alpha \cdot y_\beta) \cdot (z_\gamma \cdot e_{\alpha\beta\gamma}) = \\
&(x_\alpha \cdot y_\beta \cdot z_\gamma) \cdot e_{\alpha\beta\gamma} = x_\alpha \cdot y_\beta \cdot z_\gamma.
\end{aligned}$$

Also,

$$\begin{aligned}
&(e_{\alpha\beta\gamma} * x_\alpha) * (e_{\alpha\beta\gamma} * ((e_{\beta\gamma} * y_\beta) * (e_{\beta\gamma} * z_\gamma))) = \\
&(e_{\alpha\beta\gamma}^{-1} \cdot x_\alpha^{-1})^{-1} * (e_{\alpha\beta\gamma}^{-1} \cdot ((e_{\beta\gamma}^{-1} \cdot y_\beta^{-1})^{-1})^{-1})^{-1} = \\
&(x_\alpha \cdot e_{\alpha\beta\gamma}) \cdot e_{\alpha\beta\gamma} \cdot (y_\beta \cdot e_{\beta\gamma}) \cdot (z_\gamma \cdot e_{\beta\gamma}) = \\
&x_\alpha \cdot (e_\alpha \cdot e_{\beta\gamma}) \cdot (y_\beta \cdot (e_{\beta\gamma} \cdot (z_\gamma \cdot e_{\beta\gamma}))) = \\
&(x_\alpha \cdot e_\alpha) \cdot (e_{\beta\gamma} \cdot ((y_\beta \cdot z_\gamma) \cdot e_{\beta\gamma})) = x_\alpha \cdot y_\beta \cdot z_\gamma.
\end{aligned}$$

This proves (32).

(33): By the definition of the operation $*$,

$$(e_{\alpha\beta} * (e_\alpha * x_\alpha)) * (e_{\alpha\beta} * (e_\beta * y_\beta)) =$$
$$(e_{\alpha\beta}^{-1} \cdot (e_\alpha^{-1} \cdot x_\alpha^{-1})^{-1}) * (e_{\alpha\beta}^{-1} \cdot (e_\beta^{-1} \cdot y_\beta^{-1})^{-1}) =$$
$$e_\alpha \cdot x_\alpha^{-1} \cdot (e_{\alpha\beta} \cdot (e_\beta \cdot y_\beta^{-1} \cdot e_{\alpha\beta})) = e_\alpha \cdot x_\alpha^{-1} \cdot e_\beta \cdot y_\beta^{-1} \cdot e_{\alpha\beta} =$$
$$e_\alpha \cdot x_\alpha^{-1} \cdot e_\beta \cdot y_\beta^{-1} = x_\alpha^{-1} \cdot y_\beta^{-1} = x_\alpha * y_\beta.$$

This proves (33) and completes the proof of Lemma 3.17. □

Definition 3.18. $SLDWQ(S, \cdot)$ denotes $(S, *)$ of Lemma 3.17. The collection of all semilattices of double Ward quasigroups that satisfy (30)− (34) is denoted by **SLDWQ**.

Lemma 3.19. *Suppose that $(S, *)$ is a semigroup semilattice V of double Ward quasigroups $(DW_\alpha, *_{|_{DW_\alpha}}, e_\alpha)$ $(\alpha \in V)$, that $(\{e_\alpha \mid \alpha \in V\}, *) \cong V$ and that $(S, *)$ satisfies* (32) *and* (33). *Define $x_\alpha \cdot y_\beta = (e_{\alpha\beta} * x_\alpha) * (e_{\alpha\beta} * y_\beta)$. Then*

(34) $(\{e_\alpha \mid \alpha \in V\}, \cdot) \cong (\{e_\alpha \mid \alpha \in V\}, *)$ *is a semigroup semilattice,*

(35) $(S, \cdot)$ *is a semigroup and a semigroup semilattice of groups $(DW_\alpha, *_{|_{DW_\alpha}}, e_\alpha)$ $(\alpha \in V)$,*

(36) *for all $\alpha, \beta \in V$ and all $x_\alpha \in DW_\alpha$, $y_\beta \in DW_\beta$, $x_\alpha * y_\beta = x_\alpha^{-1} \cdot y_\beta^{-1}$.*

Proof. We have

$$e_\alpha \cdot e_\beta = (e_{\alpha\beta} * e_\alpha) * (e_{\alpha\beta} * e_\beta) = (e_{\alpha\beta} * (e_\alpha * e_\alpha)) * (e_{\alpha\beta} * (e_\beta * e_\beta)) \overset{(33)}{=} e_\alpha * e_\beta$$

and so, (34) is valid.

For each $(DW_\alpha, *_{|_{DW_\alpha}}, e_\alpha)$ the product is $x_\alpha \cdot y_\beta = (e_\alpha * x_\alpha) * (e_\alpha * y_\alpha)$, by $(F6)$ each $(DW_\alpha, *_{|_{DW_\alpha}}, e_\alpha)$ is a group. By (32), $(S, \cdot)$ is a semigroup and, by Lemma 3.1, (35) is valid. Finally, by $(F6)$, $x_\alpha^{-1} = e_\alpha * x_\alpha$ in $(S, \cdot)$. Then, by (33),

$$x_\alpha^{-1} \cdot y_\beta^{-1} = (e_\alpha * x_\alpha) \cdot (e_\beta * y_\beta) = (e_{\alpha\beta} * (e_\alpha * x_\alpha)) * (e_{\alpha\beta} * (e_\beta * y_\beta)) = x_\alpha * y_\beta,$$

which completes the proof. □

Definition 3.20. $SLG(S, *)$ denotes $(S, \cdot)$ of Lemma 3.19.

Theorem 3.21. *For all $(S, \cdot) \in$ **SLG**, $SLG(SLDWQ(S, \cdot)) = (S, \cdot)$ and for all $(S, *) \in$ **SLDWQ**, $SLDWQ(SLG(S, *)) = (S, *)$.*

Proof. The product in $SLDWQ(S, \cdot)$ is $x_\alpha * y_\beta = x_\alpha^{-1} \cdot y_\beta^{-1}$. So, the product in $SLG(SLDWQ(S, \cdot))$ is $x_\alpha \otimes y_\beta = (e_{\alpha\beta} * x_\alpha) * (e_{\alpha\beta} * y_\beta) = (e_{\alpha\beta}^{-1} \cdot x_\alpha^{-1})^{-1} \cdot (e_{\alpha\beta}^{-1} \cdot y_\beta^{-1})^{-1}$ $= x_\alpha \cdot (e_{\alpha\beta} \cdot (y_\beta \cdot e_{\alpha\beta})) = (x_\alpha \cdot y_\beta) \cdot e_{\alpha\beta} = x_\alpha \cdot y_\beta$. Hence, $SLG(SLDWQ(S, \cdot)) = (S, \cdot)$.

The product in $SLG(S, *)$ is $x_\alpha \cdot y_\beta = (e_{\alpha\beta} * x_\alpha) * (e_{\alpha\beta} * y_\beta)$. The product in $SLDWQ(SLG(S, *))$ is $x_\alpha \oplus y_\beta = x_\alpha^{-1} \cdot y_\beta^{-1} = (e_{\alpha\beta} * (e_\alpha * x_\alpha)) * (e_{\alpha\beta} * (e_\beta * e y_\beta)) \overset{(33)}{=}$ $x_\alpha * y_\beta$. So, $SLDWQ(SLG(S, *)) = (S, *)$. □

Corollary 3.22. *There is a one-to-one correspondence between elements of* **SLG** *and* **SLDWQ**.

Note that since **SLG** is in one-one correspondence with **SLWQ**, **SLWDQ** and **SLDWQ**, **SLWQ** and **SLWDQ** are in one-one correspondence with each other, as are **SLDWQ** and **SLWQ**. The next results give the explicit forms of these bijective mappings.

Theorem 3.23. $\overline{\mathbf{SLG}} = \mathbf{SLG}$.

Proof. The dual groupoid of a semigroup union of groups with commuting idempotents is a semigroup union of groups with commuting idempotents. As previously noted, the required result then follows from Lemma 3.1. □

Theorem 3.24. . $\overline{\mathbf{SLWQ}} = \mathbf{SLWDQ}$.

Proof. If $(S,*) \in \mathbf{SLWQ}$, then $x * y = x \cdot y^{-1}$ for some $(S,\cdot) \in \mathbf{SLG}$. So, if $(T,\bar{\circ}) \in \overline{\mathbf{SLWQ}}$, then, using Theorem 3.23, $x \bar{\circ} y = x^{-1} \bar{\cdot} y$ for some $(T,\bar{\cdot})$ from **SLG**. As in the proof of Lemma 3.10, $(T,\bar{\circ})$ satisfies (24) − (27). Therefore, $(T,\bar{\circ}) \in \mathbf{SLWDQ}$. Hence, $\overline{\mathbf{SLWQ}} \subseteq \mathbf{SLWDQ}$.

If $(S,*) \in \mathbf{SLWDQ}$, then $x * y = x^{-1} \cdot y$ for some $(S,\cdot) \in \mathbf{SLG}$. So, using Theorem 3.23, $x \bar{*} y = x \bar{\cdot} y^{-1}$ for some $(S,\bar{\cdot}) \in \mathbf{SLG}$. Therefore, as in the proof of Lemma 3.2, $(S,\bar{*})$ satisfies (17). Hence, $(S,\bar{*}) \in \mathbf{SLWQ}$ and $(S,*) \in \overline{\mathbf{SLWQ}}$. So, $\mathbf{SLWDQ} \subseteq \overline{\mathbf{SLWQ}}$. □

Corollary 3.25. $(S,*) \in \mathbf{SLWDQ}$ *if and only if* $(S,*)$ *is a semilattice of Ward dual quasigroups and satisfies the identity* $(x * y) * (z * w) = y * ((z^{-1} * x^{-1}) * w)$.

Theorem 3.26. $\overline{\mathbf{SLDWQ}} = \mathbf{SLDWQ}$.

Proof. If $(S,*) \in \overline{\mathbf{SLDWQ}}$, then $x * y = y \bar{*} x$ for some $(S,\bar{*}) \in \mathbf{SLDWQ}$. So, $x * y = y \bar{*} x = x^{-1} \bar{\cdot} y^{-1}$ for some $(S,\bar{\cdot}) \in \mathbf{SLG}$. Therefore, by the proof of Lemma 3.17, $(S,*) \in \mathbf{SLDWQ}$. Hence, $\overline{\mathbf{SLDWQ}} \subseteq \mathbf{SLDWQ} \subseteq \overline{\mathbf{SLDWQ}}$. □

Theorem 3.27. **SLDWQ** *and* **SLWQ** *are in one-one correspondence.*

Proof. For $(S,*) \in \mathbf{SLDWQ}$ we define $SLWQ(S,*) = (S,\circ)$, where $x_\alpha \circ y_\beta = (e_{\alpha\beta} * x_\alpha) * y_\beta$. If $(S,\otimes) \in \mathbf{SLWQ}$, we define $SLDWQ(S,\otimes) = (S,\oplus)$, where $x_\alpha \oplus y_\beta = (e_{\alpha\beta} \otimes x_\alpha) \otimes y_\beta$. Note that, since $(S,*) \in \mathbf{SLDWQ}$, $x * y = x^{-1} \cdot y^{-1}$ for some $(S,\cdot) \in \mathbf{SLG}$. Therefore, $x_\alpha \circ y_\beta = (e_{\alpha\beta} * x_\alpha) * y_\beta = (e_{\alpha\beta}^{-1} \cdot x_\alpha^{-1})^{-1} \cdot y_\beta^{-1} = x_\alpha \cdot e_{\alpha\beta} \cdot y_\beta^{-1} = x_\alpha \cdot e_\alpha \cdot e_\beta \cdot y_\beta^{-1} = x_\alpha \cdot y_\beta^{-1}$. By Lemma 3.2, $SLWQ(S,*) = (S,\circ)$ is in **SLWQ**. Therefore, $SLDWQ(S,\circ) = (S,\oplus)$, where $x_\alpha \oplus y_\beta = (e_{\alpha\beta} \circ x_\alpha) \circ y_\beta = (e_{\alpha\beta} \cdot x_\alpha^{-1}) \cdot y_\beta^{-1} = x_\alpha^{-1} \cdot y_\beta^{-1}$ and so $(S,\oplus) \in \mathbf{SLDWQ}$.

Then, the product in $SLDWQ(SLWQ(S,*))$ is $x_\alpha \oplus y_\beta = (e_{\alpha\beta} \circ x_\alpha) \circ y_\beta = (e_{\alpha\beta} * (e_{\alpha\beta} \circ x_\alpha)) * y_\beta = (e_{\alpha\beta}^{-1} \cdot (e_{\alpha\beta}^{-1} \cdot x_\alpha^{-1})^{-1})^{-1} \cdot y_\beta^{-1} = ((e_{\alpha\beta}^{-1} \cdot x_\alpha^{-1})^{-1})^{-1} \cdot y_\beta^{-1} = (e_{\alpha\beta}^{-1} \cdot x_\alpha^{-1}) \cdot y_\beta^{-1} = x_\alpha^{-1} \cdot y_\beta^{-1} = x_\alpha * y_\beta$. Therefore, $SLDWQ(SLWQ(S,*)) = (S,*)$.

Similarly, $SLWQ(SLDWQ(S,\otimes)) = (S,\otimes)$. □

Questions. Suppose that $(S, *)$ is a semigroup semilattice V of double Ward quasigroups $(DW_\alpha, *_{|_{DW_\alpha}}, e_\alpha)$ $(\alpha \in V)$ and that $(S, *)$ satisfies (32) and (33). Then, is $(\{e_\alpha \mid \alpha \in V\}, *) \cong V$.

1. Can groupoids in **SLDWQ** be described by a single identity, in place of (32) and (33)?

2. Is there a structure theorem for groupoids in **SLWQ**, **SLWDQ** and **SLDWQ** analogous to the structure theorem for semigroups that are semigroup semilattices of groups [3, Theorem 4.11]?

A remaining area for investigation is right, left and double division on completely simple semigroups, where x^{-1} is the inverse of x in the group to which it belongs.

References

[1] **J.M. Cardoso and C.P. da Silva**, *On Ward quasigroups*, An. Ştiinţ. Univ. Al. I. Cuza Iaşi. Secţ. I a Mat. (N.S.) **24** (1978), 231 – 233.

[2] **S.K. Chatterjea**, *On Ward quasigroups*, Pure Math. Manuscript **6** (1987), 31 – 34.

[3] **A.H. Clifford and G.B. Preston**, *The algebraic theory of semigroups*, vol.1. In: Math. Survey, vol.7. Providence (1961).

[4] **W.A. Dudek and R.A.R. Monzo**, *Double magma associated with Ward and double Ward quasigroups*, Quasigroups and Related Systems **27** (2019), 33 – 52.

[5] **N.C. Fiala**, *Double Ward quasigroups*, Quasigroups and Related Systems **15** (2007), 261 – 262.

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

[7] **K.W. Johnson**, *The construction of loops using right division and Ward quasigroups*, Quasigroups and Related Systems **14** (2006), 27 – 41.

[8] **K.W. Johnson and P. Vojtěchovský**, *Right division in groups, Dedikind-Frobenius group matrices and Ward quasigroups*, Abh. Math. Sem. Univ. Hamburg **75** (2005), 121 – 136.

[9] **M. Polonijo**, *A note on Ward quasigroups*, An. Ştiinţ. Univ. Al. I. Cuza Iaşi. Secţ. I a Mat. (N.S.) **32** (1986), no.2, 5 – 10.

[10] **M. Polonijo**, *Transitive groupoids*, Portugaliae Math. **50** (1993), 63 – 74.

[11] **C.P. da Silva and F.K. Miyaóka**, *Relations among some classes of quasigroups*, Revista Colomb. Mat. **13** (1979), 11 – 21.

[12] **M. Ward**, *Postulates for the inverse operations in a group*, Trans. Amer. Math. Soc. **32**, (1930), 520 – 526.

Received August 15, 2020

Flat 10, Albert Mansions, Crouch Hill, London N8 9RE, United Kingdom
E-mail: bobmonzo@talktalk.net

Quasigroups and Related Systems **28** (2020), 301 – 308

Semigroups in which the radical of every quasi-ideal is a subsemigroup

Jatuporn Sanborisoot and Thawhat Changphas

Abstract. For a non-empty subset A of a semigroup S, $\sqrt{A}$ denotes the radical of A, i.e., $\sqrt{A} = \{x \in S \mid x^n \in A \text{ for some positive integer } n\}$. This paper characterizes when the radical $\sqrt{Q}$ is a subsemigroup of S for every quasi-ideal Q of S.

1. Introduction and Preliminaries

Let S be a semigroup. For $a, b \in S$, the subsemigroup of S generated by $\{a, b\}$ is denoted by $\langle a, b\rangle$. A non-empty subset A of S is called a *left* (respectively, *right*) *ideal* of S if $SA \subseteq A$ (respectively, $AS \subseteq A$). And, A is called a *two-sided ideal* (or *ideal*) of S if it is both a left and a right ideal of S. A non-empty subset Q of S is called a *quasi-ideal* of S if $QS \cap SQ \subseteq Q$. A subsemigroup B of S is called a *bi-ideal* of S if $BSB \subseteq B$ (cf. [2], [3]).

For a non-empty subset A of a semigroup S, $\sqrt{A}$ denotes the *radical* of S, i.e.,

$$\sqrt{A} = \{a \in S \mid a^n \in A \text{ for some positive integer } n\}.$$

In [1], M. Ćirić and S. Bogdanović characterized when the radical $\sqrt{A}$ is a subsemigroup of S for every ideals A of S. Indeed, the authors studied when the radical of every ideal of S is a subsemigroup of S; and when the radical of every bi-ideal of S is a subsemigroup of S. The notion of quasi-ideals generalizes ideals, and the notion of bi-ideals generalizes quasi-ideals, but quasi-ideals have been widely studied; see [3]. In the line of [1], this paper considers the case of quasi-ideals. Indeed, we characterize when the radical $\sqrt{Q}$ of every quasi-ideal Q of S is a subsemigroup of S.

Let $\mathbb{N} = \{1, 2, 3, \ldots\}$ denote the set of all positive integers. Let a, b be any

2010 Mathematics Subject Classification: 20M20, 06F05
Keywords: semigroup, radical, subsemigroup, ideal, quasi-ideal, bi-ideal
The first author is supported by Research Fund for Supporting Lecturer to Admit High Potential Student to Study and Research on His Expert Program Year 2018. The second author is supported by grant number 6200056 of the National Research Council of Thailand: NRCT.

elements of a semigroup S with identity. Define

$$\begin{aligned} a \mid b &\iff b = xay \text{ for some } x, y \in S; \\ a \mid_r b &\iff b = ax \text{ for some } x \in S; \\ a \mid_l b &\iff b = ya \text{ for some } y \in S; \\ a \mid_t b &\iff a \mid_r b \wedge a \mid_l b; \\ a \to b &\iff a \mid b^n \text{ for some } n \in \mathbb{N}; \text{ and} \\ a \xrightarrow{h} b &\iff a \mid_h b^n \text{ for some } n \in \mathbb{N} \text{ where } h \text{ is } r, l \text{ or } t. \end{aligned}$$

2. Main results

In [3], a non-empty subset Q of a semigroup S is a quasi-ideal of S if and only if it is an intersection of a left and a right ideal of S. We begin the section with the following theorem.

Theorem 2.1. *Let S be a semigroup with identity. Then the radical of every quasi-ideal of S is a subsemigroup of S if and only if*

$$\forall a, b \in S \ \forall i, j \in \mathbb{N} \ \exists n \in \mathbb{N} \ [(ab)^n \in \{a^i, b^j\}S \cap S\{a^i, b^j\}].$$

Proof. Assume that the radical of every quasi-ideal of S is a subsemigroup of S. Let $a, b \in S$, and let $i, j \in \mathbb{N}$. Put

$$Q = \{a^i, b^j\}S \cap S\{a^i, b^j\}.$$

Then Q is a quasi-ideal of S such that $a, b \in \sqrt{Q}$. By assumption, $ab \in \sqrt{Q}$. Hence $(ab)^n \in \{a^i, b^j\}S \cap S\{a^i, b^j\}$ for some $n \in \mathbb{N}$.

Conversely, assume that for all a, b in S and i, j in $\mathbb{N}$ there exists $n \in \mathbb{N}$ such that $(ab)^n \in \{a^i, b^j\}S \cap S\{a^i, b^j\}$. Let Q be a quasi-ideal of S, and let $a, b \in \sqrt{Q}$. Then $a^i \in Q$ and $b^j \in Q$ for some $i, j \in \mathbb{N}$. By assumption, there exists $n \in \mathbb{N}$ such that $(ab)^n \in \{a^i, b^j\}S \cap S\{a^i, b^j\}$. Thus $ab \in \sqrt{Q}$, because

$$(ab)^n \in \{a^i, b^j\}S \cap S\{a^i, b^j\} \subseteq QS \cap SQ \subseteq Q.$$

Hence $\sqrt{Q}$ is a subsemigroup of S. □

Let $S = \{a, b, c, d, 1\}$ be a semigroup with the multiplication:

$\cdot$	a	b	c	d	1
a	a	a	a	a	a
b	a	a	a	a	b
c	a	a	b	a	c
d	a	a	b	b	d
1	a	b	c	d	1

The quasi-ideal of S is $\{\{a\},\{a,b\},\{a,b,c\},\{a,b,d\},\{a,b,c,d\},S\}$. Observe that $\sqrt{\{a\}}=\{a,b\}$, $\sqrt{\{a,b\}}=\sqrt{\{a,b,c\}}=\sqrt{\{a,b,d\}}=\sqrt{\{a,b,c,d\}}=\{a,b,c,d\}$ and $\sqrt{S}=S$; then the radical of every quasi-ideal of S is a subsemigroup of S.

In general, the radical of quasi-ideals of a semigroup with identity need not be subsemigroups, as the following example shows:

Let $S=\{a,b,c,d,f,1\}$ be a semigroup with the multiplication:

$\cdot$	a	b	c	d	f	1
a	a	a	a	a	a	a
b	a	b	a	d	a	b
c	a	f	c	c	f	c
d	a	b	d	d	b	d
f	a	f	a	c	a	f
1	a	b	c	d	f	1

The quasi-ideal of S is $\{\{a\},\{a,b\},\{a,c\},\{a,d\},\{a,f\},\{a,b,d\},\ \{a,c,d\},$ $\{a,b,f\},\{a,c,f\},\{a,b,c,d,f\},S\}$. We have $\sqrt{\{a,c,d\}}=\{a,c,d,f\}$ which is not a subsemigroup of S.

Theorem 2.2. *Let S be a semigroup with identity. Then the radical of every right ideal of S is a quasi-ideal of S if and only if*

$$\forall a,b,c\in S\ [a\mid_r c\wedge b\mid_l c\Longrightarrow \forall i,j\in\mathbb{N}\ [a^i\xrightarrow{r}c\vee b^j\xrightarrow{r}c]].$$

Proof. Assume that the radical of every right ideal of S is a quasi-ideal of S. Let $a,b,c\in S$ such that $a\mid_r c$ and $b\mid_l c$. Then $c=au$ and $c=vb$ for some $u,v\in S$. Let $i,j\in\mathbb{N}$. Put $R=\{a^i,b^j\}S$; then R is a right ideal of S and $a,b\in\sqrt{R}$. By assumption, $\sqrt{R}$ is a quasi-ideal of S. Since $c=au$ and $c=vb$,

$$c\in\sqrt{R}S\cap S\sqrt{R}\subseteq\sqrt{R}.$$

Thus $c^n\in R$ for some $n\in\mathbb{N}$, whence $a^i\xrightarrow{r}c$ or $b^j\xrightarrow{r}c$.

Conversely, assume that for all a,b,c in S,

$$a\mid_r c\wedge b\mid_l c\Longrightarrow\forall i,j\in\mathbb{N}\ [a^i\xrightarrow{r}c\vee b^j\xrightarrow{r}c].$$

Let R be a right ideal of S. To show that $\sqrt{R}S\cap S\sqrt{R}\subseteq\sqrt{R}$, let $x\in\sqrt{R}S\cap S\sqrt{R}$. Then $x=au$ and $x=vb$ for some $u,v\in S$ and $a,b\in\sqrt{R}$. Since $a,b\in\sqrt{R}$, there exist $i,j\in\mathbb{N}$ such that $a^i,b^j\in R$. By assumption, there exists $n\in\mathbb{N}$ such that $x^n\in\{a^i,b^j\}S$. Since

$$\{a^i,b^j\}S\subseteq RS\subseteq R,$$

then $x\in\sqrt{R}$. Hence $\sqrt{R}$ is a quasi-ideal of S. □

As Theorem 2.2, we obtain the following.

Theorem 2.3. *Let S be a semigroup with identity. Then the radical of every left ideal of a semigroup S is a quasi-ideal of S if and only if*

$$\forall a,b,c \in S\ [a \mid_r c \wedge b \mid_l c \Longrightarrow \forall i,j \in \mathbb{N}\ [a^i \xrightarrow{l} c \vee b^j \xrightarrow{l} c]].$$

Theorem 2.4. *Let S be a semigroup with identity. Then the radical of every quasi-ideal of S is a quasi-ideal of S if and only if*

$$\forall a,b,c \in S\ [a \mid_r c \wedge b \mid_l c \Longrightarrow \forall i,j \in \mathbb{N}\ \exists n \in \mathbb{N}\ [c^n \in \{a^i,b^j\}S \cap S\{a^i,b^j\}]].$$

Proof. Assume that the radical of every quasi-ideal of S is a quasi-ideal of S. Let $a,b,c \in S$ such that $a \mid_r c$ and $b \mid_l c$. Then $c = au$ and $c = vb$ for some $u,v \in S$. Let $i,j \in \mathbb{N}$. Put

$$Q = \{a^i,b^j\}S \cap S\{a^i,b^j\}.$$

Then Q is a quasi-ideal of S and $a,b \in \sqrt{Q}$. By assumption, $\sqrt{Q}$ is a quasi-ideal of S. Since $c = au$ and $c = vb$,

$$c \in \sqrt{Q}S \cap S\sqrt{Q} \subseteq \sqrt{Q}.$$

Hence $c^n \in \{a^i,b^j\}S \cap S\{a^i,b^j\}$ for some $n \in \mathbb{N}$.

Conversely, assume that for all $a,b,c \in S$,

$$a \mid_r c \wedge b \mid_l c \Longrightarrow \forall i,j \in \mathbb{N}\ \exists n \in \mathbb{N}\ [c^n \in \{a^i,b^j\}S \cap S\{a^i,b^j\}].$$

Let Q be a quasi-ideal of S. We need show that $\sqrt{Q}S \cap S\sqrt{Q} \subseteq \sqrt{Q}$. Let $x \in \sqrt{Q}S \cap S\sqrt{Q}$. Then $x = au$ and $x = vb$ for some $a,b \in \sqrt{Q}$ and $u,v \in S$. Since $a,b \in \sqrt{Q}$, there exist $i,j \in \mathbb{N}$ such that $a^i,b^j \in Q$. By assumption, there exists $n \in \mathbb{N}$ such that $x^n \in \{a^i,b^j\}S \cap S\{a^i,b^j\}$. Since

$$\{a^i,b^j\}S \cap S\{a^i,b^j\} \subseteq QS \cap SQ \subseteq Q,$$

then $x \in \sqrt{Q}$, whence $\sqrt{Q}$ is a quasi-ideal of S. □

Theorem 2.5. *Let S be a semigroup with identity. The radical of every ideal of S is a quasi-ideal of S if and only if*

$$\forall a,b,c \in S\ [a \mid_r c \wedge b \mid_l c \Longrightarrow \forall i,j \in \mathbb{N}\ [a^i \to c \vee b^j \to c]].$$

Proof. Assume that the radical of every ideal of S is a quasi-ideal of S. Let $a,b,c \in S$ such that $a \mid_r c$ and $b \mid_l c$. Then $c = au$ and $c = vb$ for some $u,v \in S$. Let $i,j \in \mathbb{N}$. Put $A = S\{a^i,b^j\}S$, then A is an ideal of S and $a,b \in \sqrt{A}$. By assumption, $\sqrt{A}$ is a quasi-ideal of S. Since $c = au$ and $c = vb$,

$$c \in \sqrt{A}S \cap S\sqrt{A} \subseteq \sqrt{A}.$$

Then there exists $n \in \mathbb{N}$ such that $c^n \in A$. Hence $a^i \to c$ or $b^j \to c$. The opposite direction can be proved similarly to the converse of Theorem 2.2. □

Theorem 2.6. *Let S be a semigroup with identity. The radical of every quasi-ideal of S is a bi-ideal of S if and only if*

$$\forall a, b, c \in S\ \forall i, j \in \mathbb{N}\ \exists n \in \mathbb{N}\ [(abc)^n \in \{a^i, c^j\}S \cap S\{a^i, c^j\}].$$

Proof. Assume that the radical of every quasi-ideal of S is a bi-ideal of S. Let $a, b, c \in S$, and let $i, j \in \mathbb{N}$. Put $Q = \{a^i, c^j\}S \cap S\{a^i, c^j\}$. Observe firstly that Q is a quasi-ideal of S and $a, c \in \sqrt{Q}$. By assumption, $\sqrt{Q}$ is a bi-ideal of S. Then

$$abc \in \sqrt{Q}S\sqrt{Q} \subseteq \sqrt{Q}.$$

Hence $(abc)^n \in \{a^i, c^j\}S \cap S\{a^i, c^j\}$ for some $n \in \mathbb{N}$.

Conversely, assume that for any $a, b, c \in S$, and $i, j \in \mathbb{N}$,

$$(abc)^n \in \{a^i, c^j\}S \cap S\{a^i, c^j\} \text{ for some } n \in \mathbb{N}.$$

Let Q be a quasi-ideal of S. Let $a, c \in \sqrt{Q}$, and let $b \in S$. Then $a^i, c^j \in Q$ for some $i, j \in \mathbb{N}$. By assumption, $(abc)^n \in \{a^i, c^j\}S \cap S\{a^i, c^j\}$ for some $n \in \mathbb{N}$. Consider

$$(abc)^n \in \{a^i, c^j\}S \cap S\{a^i, c^j\} \subseteq QS \cap SQ \subseteq Q.$$

Thus $abc \in \sqrt{Q}$, and $\sqrt{Q}$ is a bi-ideal of S. □

Theorem 2.7. *Let S be a semigroup with identity. The radical of every quasi-ideal of a semigroup S is a right ideal of S if and only if*

$$a^k \xrightarrow{t} ab \text{ for all } a, b \in S \text{ and } k \in \mathbb{N}.$$

Proof. Assume that the radical of every quasi-ideal of S is a right ideal of S. Let $a, b \in S$ and $k \in \mathbb{N}$. Put $Q = a^kS \cap Sa^k$. Then Q is a quasi-ideal of S and $a \in \sqrt{Q}$. By assumption, $\sqrt{Q}$ is a right ideal of S. Thus $ab \in \sqrt{Q}S \subseteq \sqrt{Q}$. We then have that there exists $n \in \mathbb{N}$ such that $(ab)^n \in Q$. Hence $a^k \xrightarrow{t} ab$.

Conversely, assume that $a^k \xrightarrow{t} ab$ for all $a, b \in S$ and $k \in \mathbb{N}$. Let Q be a quasi-ideal of S, and let $a \in \sqrt{Q}$ and $b \in S$. Then $a^k \in Q$ for some $k \in \mathbb{N}$. Since

$$a^kS \cap Sa^k \subseteq QS \cap SQ \subseteq Q,$$

$(ab)^n \in Q$ for some $n \in \mathbb{N}$. This implies $ab \in \sqrt{Q}$, and hence $\sqrt{Q}$ is a right ideal of S. □

As Theorem 2.7, we obtain the following theorem.

Theorem 2.8. *Let S be a semigroup with identity. The radical of every quasi-ideal of S is a left ideal of S if and only if $a^k \xrightarrow{t} ba$ for all $a, b \in S$ and $k \in \mathbb{N}$.*

Theorem 2.9. *Let S be a semigroup with identity. Then the following conditions are equivalent:*

(1) *the radical of every quasi-ideal of S is an ideal of S;*

(2) *$a^k \xrightarrow{t} ab$ and $a^k \xrightarrow{t} ba$ for all $a, b \in S$ and $k \in \mathbb{N}$.*

Proof. (1) $\Rightarrow$ (2): Assume (1). Let $a, b \in S$, and let $k \in \mathbb{N}$. Put $A = a^kS \cap Sa^k$. Clearly, A is a quasi-ideal of S and $a \in \sqrt{A}$. By assumption, $\sqrt{A}$ is an ideal of S. Thus $ab \in \sqrt{A}S \subseteq \sqrt{A}$ and $ba \in S\sqrt{A} \subseteq \sqrt{A}$. This implies $(ab)^m, (ba)^n \in A$ for some $m, n \in \mathbb{N}$. Hence $a^k \xrightarrow{t} ab$ and $a^k \xrightarrow{t} ba$.

(2) $\Rightarrow$ (1): Assume (2). Let Q be a quasi-ideal of S. To show that $\sqrt{Q}$ is an ideal of S, let $a \in \sqrt{Q}$ and $b \in S$. Since $a \in \sqrt{Q}$, $a^k \in Q$ for some $k \in \mathbb{N}$. By assumption, there exist $m, n \in \mathbb{N}$ such that $(ab)^m, (ba)^n \in a^kS \cap Sa^k$. Hence $(ab)^m, (ba)^n \in Q$, because

$$a^kS \cap Sa^k \subseteq QS \cap SQ \subseteq Q.$$

This implies $ab, ba \in \sqrt{Q}$, and thus $\sqrt{Q}$ is an ideal of S. □

Theorem 2.10. *Let S be a semigroup with identity. Then the following conditions are equivalent:*

(1) *the radical of every bi-ideal of S is a quasi-ideal of S;*

(2) $\forall a, b, c \in S\ [a \mid_r c \wedge b \mid_l c \Longrightarrow \forall i, j \in \mathbb{N}\ \exists n \in \mathbb{N}\ [c^n \in \{a^i, b^j\}S\{a^i, b^j\}]]$.

Proof. (1) $\Rightarrow$ (2): Assume (1). Let $a, b, c \in S$ such that $c = au$ and $c = vb$ for some $u, v \in S$. Let $i, j \in \mathbb{N}$. It is observed that

$$B = \{a^i, b^j\}S\{a^i, b^j\}$$

is a bi-ideal of S and $a, b \in \sqrt{B}$. By assumption, $\sqrt{B}$ is a quasi-ideal of S. Therefore, $c \in \sqrt{B}S \cap S\sqrt{B} \subseteq \sqrt{B}$. Hence $c^n \in \{a^i, b^j\}S\{a^i, b^j\}$ for some $n \in \mathbb{N}$.

(2) $\Rightarrow$ (1): Assume (2). Let B be a bi-ideal of S. Let $x \in \sqrt{B}S \cap S\sqrt{B}$. Then $x = au$ and $x = vb$ for some $a, b \in \sqrt{B}$ and $u, v \in S$. Hence, there exist $i, j \in \mathbb{N}$ such that $a^i, b^j \in B$. By assumption,

$$x^n \in \{a^i, b^j\}S\{a^i, b^j\} \subseteq BSB \subseteq B.$$

Thus $x \in \sqrt{B}$. Hence $\sqrt{B}$ is a quasi-ideal of S. □

Theorem 2.11. *Let S be a semigroup with identity. Then the following conditions are equivalent:*

(1) *the radical of every subsemigroup of S is a quasi-ideal of S;*

(2) $\forall a, b, c \in S\ [a \mid_r c \wedge b \mid_l c \Longrightarrow \forall i, j \in \mathbb{N}\ \exists n \in \mathbb{N}\ [c^n \in \langle a^i, b^j \rangle]]$.

Proof. (1) $\Rightarrow$ (2): Assume (1), and let $a, b, c \in S$, such that $a \mid_r c$ and $b \mid_l c$. Then $c = au$ and $c = vb$ for some $u, v \in S$. Let $i, j \in \mathbb{N}$. Put $A = \langle a^i, b^j \rangle$. By (1), $\sqrt{A}$ is a quasi-ideal of S. Since $c = au$ and $c = vb$, $c \in \sqrt{A}S \cap S\sqrt{A}$. Then

$$c \in \sqrt{A}S \cap S\sqrt{A} \subseteq \sqrt{A}.$$

Hence $c^n \in \langle a^i, b^j \rangle$ for some $n \in \mathbb{N}$.

(2) $\Rightarrow$ (1): Assume (2), and let A be a subsemigroup of S. Let $x \in \sqrt{A}S \cap S\sqrt{A}$; then $x = au$ and $x = vb$ for some $a, b \in \sqrt{A}$ and $u, v \in S$. We then have that $a^i, b^j \in A$ for some $i, j \in \mathbb{N}$. By assumption, $x^n \in \langle a^i, b^j \rangle$. Since $\langle a^i, b^j \rangle \subseteq A$, $x \in \sqrt{A}$. Thus $\sqrt{A}$ is a quasi-ideal of S. □

Finally, we have the following result.

Theorem 2.12. *Let S be a semigroup with identity. Then the following conditions are equivalent:*

(1) *the radical of every quasi-ideal of S is a quasi-ideal of S;*

(2) $\forall a, b \in S$ [$\sqrt{\{a,b\}S \cap S\{a,b\}}$ *is a quasi-ideal of* S];

(3) $\forall a, b, c \in S$ $[a \mid_r c \wedge b \mid_l c \Longrightarrow \exists n \in \mathbb{N}$ $[c^n \in \{a^2, b^2\}S \cap S\{a^2, b^2\}]]$;

(4) $\forall a, b, c \in S$ $[a \mid_r c \wedge b \mid_l c \Longrightarrow \forall k \in \mathbb{N}\ \exists n \in \mathbb{N}$ $[c^n \in \{a^k, b^k\}S \cap S\{a^k, b^k\}]]$.

Proof. (1) $\Rightarrow$ (2): Assume (1), and let $a, b \in S$. Since $\{a,b\}S \cap S\{a,b\}$ is a quasi-ideal of S and (1), $\sqrt{\{a,b\}S \cap S\{a,b\}}$ is a quasi-ideal of S.

(2) $\Rightarrow$ (3): Assume (2), and let $a, b, c \in S$ such that $a \mid_r c$ and $b \mid_l c$. Then $c = au$ and $c = vb$ for some $u, v \in S$. Clearly, $a, b \in \sqrt{\{a^2, b^2\}S \cap S\{a^2, b^2\}}$. By (2), $\sqrt{\{a^2, b^2\}S \cap S\{a^2, b^2\}}$ is a quasi-ideal of S. From $c = au$ and $c = vb$, it follows that

$$\begin{aligned} c &\in \sqrt{\{a^2, b^2\}S \cap S\{a^2, b^2\}}S \cap S\sqrt{\{a^2, b^2\}S \cap S\{a^2, b^2\}} \\ &\subseteq \sqrt{\{a^2, b^2\}S \cap S\{a^2, b^2\}}. \end{aligned}$$

Thus $c^n \in \{a^2, b^2\}S \cap S\{a^2, b^2\}$ for some $n \in \mathbb{N}$.

(3) $\Rightarrow$ (4): Assume (3), and let $a, b, c \in S$ such that $a \mid_r c$ and $b \mid_l c$. Then $c = au$ and $c = vb$ for some $u, v \in S$. By (3), $c^n \in \{a^2, b^2\}S \cap S\{a^2, b^2\}$ for some $n \in \mathbb{N}$. It is observed that

$$\{a^2, b^2\}S \cap S\{a^2, b^2\} \subseteq \{a,b\}S \cap S\{a,b\}.$$

Then

$$c^n \in \{a,b\}S \cap S\{a,b\}.$$

Suppose that there exists $m \in \mathbb{N}$ where $k \in \mathbb{N}$ such that

$$c^m \in \{a^k, b^k\}S \cap S\{a^k, b^k\}.$$

By (3), there exists $l \in \mathbb{N}$ such that

$$(c^m)^l \in \{a^{2k}, b^{2k}\}S \cap S\{a^{2k}, b^{2k}\}.$$

Consider

$$\begin{aligned}(c^m)^l &\in \{a^{2k}, b^{2k}\}S \cap S\{a^{2k}, b^{2k}\}\\ &= \{a^{k+1}a^{k-1}, b^{k+1}b^{k-1}\}S \cap S\{a^{k-1}a^{k+1}, b^{k-1}b^{k+1}\}\\ &\subseteq \{a^{k+1}, b^{k+1}\}S \cap S\{a^{k+1}, b^{k+1}\}.\end{aligned}$$

Hence

$$c^{ml} = (c^m)^l \in \{a^{k+1}, b^{k+1}\}S \cap S\{a^{k+1}, b^{k+1}\}.$$

Therefore (4) holds.

(4) $\Rightarrow$ (1): Assume (4), and let Q be a quasi-ideal of S. Let $x \in \sqrt{Q}S \cap S\sqrt{Q}$. Then $x = au$ and $x = vb$ for some $u, v \in S$ and $a, b \in \sqrt{Q}$. Then $a^i, b^j \in Q$ for some $i, j \in \mathbb{N}$. By (4), there exists $n \in \mathbb{N}$ such that

$$x^n \in \{a^{i+j}, b^{i+j}\}S \cap S\{a^{i+j}, b^{i+j}\}.$$

Consider

$$x^n \in \{a^{i+j}, b^{i+j}\}S \cap S\{a^{i+j}, b^{i+j}\} \subseteq \{a^i, b^j\}S \cap S\{a^i, b^j\} \subseteq QS \cap SQ \subseteq Q.$$

Thus $x \in \sqrt{Q}$, and Q is a quasi-ideal of S. □

References

[1] **M. Ćirić and S. Bogdanović**, *Semigroups in which the radical of every ideal is a subsemigroup*, Zbornik rad. Fil. fak. Niš. Ser. Mat., **6** (1992), 129–135.

[2] **J.M. Howei**, *An Introduction to Semigroup Theory*, Academic Press, London, 1976.

[3] **O. Steinfeld**, *Quasi-ideals in Rings and Semigroups*, Akadémiai Kiadó, Budapest, 1978.

Received November 2, 2019

J. Sanborisoot
Department of Mathematics, Faculty of Science, Khon Kaen University, Khon Kaen 40002, Thailand
E-mail: sanborisoot@hotmail.com, thacha@kku.ac.th

Th. Changphas
Centre of Excellence in Mathematics, CHE, Si Ayuttaya Rd., Bangkok 10400, Thailand
E-mail: thacha@kku.ac.th

Quasigroups and Related Systems **28** (2020), 309 – 318

On ordered semigroups satisfying certain regularity conditions

Jatuporn Sanborisoot and Thawhat Changphas

Abstract. In terms of ideals, this paper investigates ordered semigroups satisfying certain regularity conditions. In particular we study regularity, complete regularity, quasi-regularity, intra-regularity as well as left (right) regularity, left (right) quasi-regularity, and left (right) reproduce.

1. Preliminaries

Regular rings and semigroups have been introduced and studied by Neumann [10]. These lead to study other types of regularity, for example, completely regularity, intra-regularity and quasi-regularity ([9], [12]). Using the so-called *linear words*, Bogdanovíc et al. classified all the types of regularity of semigroups [2]; based on the results obtained the authors then described semigroups satisfying certain regularity conditions [1]. In [11], Phochai and Changphas determined all the types of regularity conditions for ordered semigroups. This paper then examines ordered semigroups satisfying each of the types of regularity conditions. Some types of regularity of ordered semigroups have been studied ([3], [4]).

An *ordered semigroup* $(S, \cdot, \leqslant)$ consists of a semigroup $(S, \cdot)$ together with a relation $\leqslant$ that is *compatible* with the semigroup operation (cf. [7]), meaning that, for any $a, b, c \in S$, $a \leqslant b$ implies $ac \leqslant bc$ and $ca \leqslant cb$. For $\emptyset \neq A, B \subseteq S$, $AB := \{ab \in S \mid a \in A, b \in B\}$ and $(A] := \{x \in S \mid \exists a \in A, x \leqslant a\}$. It is observed that (1) $A \subseteq (A]$; (2) $(A](B] \subseteq (AB]$; (3) $((A](B]] = (AB]$.

A non-empty subset A of an ordered semigroup $(S, \cdot, \leqslant)$ is called a *left* (resp. *right*) *ideal* of S if (i) $SA \subseteq A$ (resp. $AS \subseteq A$); (ii) $(A] = A$. We say that A is a (*two-sided*) *ideal* of S if A is both a left and a right ideal of S. S is said to be *simple* if S contains no proper ideals. If $a \in S$ then $L(a) = (a \cup Sa]$ (resp. $R(a) = (a \cup aS]$, $J(a) = (a \cup aS \cup Sa \cup SaS]$) is a left (resp. right, two-sided) ideal containing a. An ordered semigroup S is simple if and only if $S = (SaS]$ for all $a \in S$ [8]. A subsemigroup B of S (that is, $BB \subseteq B$) is called a *bi-ideal* of S if (i)

2000 Mathematics Subject Classification: 06F05
Keywords: ordered semigroup, ideal, simple, semilattice, linear word, regularity conditions
The first author is supported by grant number 6200056 of the National Research Council of Thailand: NRCT. The second author is supported by Research Fund for Supporting Lecturer to Admit High Potential Student to Study and Research on His Expert Program Year 2018

$BSB \subseteq B$; (ii) $(B] = B$ ([5], p. 242). If $a \in S$ then $(a \cup a^2 \cup aSa]$ is a bi-ideal containing a .

Let X be a countable alphabet whose elements are called *variables*. Let c be a symbol such that $c \notin X$, called a *constant*. Consider $(X \cup \{c\})^+$, free semigroup generated by $X \cup \{c\}$, let L be the set of all words $u \in (X \cup \{c\})^+$ satisfying the following conditions:

(i) The constant c appears at least once in u.
(ii) There is at least one occurrence of a variable in u.
(iii) Any variable appears at most once in u.

A word $u \in L$ is called *linear*, and we shall write $u(c, x_1, \ldots, x_n)$ instead of u to emphasize that $\{x_1, \ldots, x_n\}$ is the set of all variables appearing in u. For $u(c, x_1, \ldots, x_n) \in L$, an expression of the form $c \leqslant u(c, x_1, \ldots, x_n)$ is called a *regularity condition*. For an ordered semigroup $(S, \cdot, \leqslant)$ and $a \in S$, an expression of the form $a \leqslant u(a, x_1, \ldots, x_n)$ is *solvable* in S if there exist $a_1, \ldots, a_n \in S$ such that $a \leqslant u(a, a_1, \ldots, a_n)$. Two regularity conditions $c \leqslant u(c, x_1, \ldots, x_n)$ and $c \leqslant v(c, y_1, \ldots, y_m)$ are *equivalent* if for every ordered semigroup $(S, \cdot, \leqslant)$, and for every $a \in S$,

$$a \leqslant u(a, x_1, \ldots, x_n) \text{ is solvable in } S \iff a \leqslant v(a, y_1, \ldots, y_m) \text{ is solvable in } S.$$

We denote by $\mathbb{N}$ the set of all positive integers. It was proved in [11] that an arbitrary regularity condition $c \leqslant u(c, x_1, \ldots, x_n)$ is equivalent to one of the regularity conditions (C1)–(C16):

Number	Condition	Name
C1	$c \leqslant xcy$	
C2	$c \leqslant xc$	Left Reproduce
C3	$c \leqslant cx$	Right Reproduce
C4	$c \leqslant xcycz$	Intra-quasi-regular
C5	$c \leqslant xcyc$	Left Quasi-regular
C6	$c \leqslant cxcy$	Right Quasi-regular
C7	$c \leqslant cxc$	Regular
C8	$c \leqslant xc^k y$, for some $k \in \mathbb{N}$	Intra-regular ($k = 2$)
C9	$c \leqslant xc^k yc$, for some $k \in \mathbb{N}$	Left Regular
C10	$c \leqslant cxc^k y$, for some $k \in \mathbb{N}$	Right Regular
C11	$c \leqslant xc^2$	
C12	$c \leqslant xc^2$	
C13	$c \leqslant c^2 x$	
C14	$c \leqslant c^2 xc^2$	
C15	$c \leqslant cxc^2$	
C16	$c \leqslant c^2 xc$	

Let $(S, \cdot, \leqslant)$ be an ordered semigroup. S is said to satisfy a regularity condition $c \leqslant u(c, x_1, ..., x_n)$, if for every $a \in S$, the expression $a \leqslant u(a, x_1, ..., x_n)$ is solvable

in S. It is observed that an ordered semigroup $(S, \cdot, \leqslant)$ is intra-quasi-regular (resp. left quasi-regular) if $a \in (SaSaS]$ (resp. $a \in (SaSa]$) for all $a \in S$. Any other types of regularity can be observed similarly. Finally, we call an element a of S a *left* (resp. *right*) *reproduce element* if $a \leqslant xa$ (resp. $a \leqslant ax$) is solvable. Any other types of elements can be defined similarly.

The main results can be described shortly as the following: Theorem 1 shows that every ordered semigroup in a semilattice satisfies the same regularity condition of such semilattice. In Theorem 2, we consider relationships of ordered semigroups containing intra-quasi-regular elements, intra-regular elements, left [resp. right] quasi-regular elements, left [resp. right] regular elements. In Theorem 3, we characterize several regularities of elements by its principal ideal, principal left ideal and principal right ideal. The rest of this paper shows characterizations of regularities of semigroups and regularity conditions of semigroups as well.

2. Main Results

Let Y be a semilattice. An ordered semigroup $(S, \cdot, \leqslant)$ is a *semilattice* Y of ordered semigroups $(S_\alpha, \cdot_\alpha, \leq_\alpha)$, $\alpha \in Y$ if (i) $S_\alpha \cap S_\beta = \emptyset$ for all different $\alpha, \beta \in Y$; (ii) $S = \bigcup_{\alpha \in Y} S_\alpha$; (iii) $S_\alpha S_\beta \subseteq S_{\alpha\beta}$ for all $\alpha, \beta \in Y$.

Theorem 1. *Assume an ordered semigroup $(S, \cdot, \leqslant)$ is a semilattice Y of ordered semigroups $(S_\alpha, \cdot_\alpha, \leq_\alpha)$, $\alpha \in Y$. If $(S, \cdot, \leqslant)$ satisfies one of the regularity conditions $(C4)$–$(C14)$ then $(S_\alpha, \cdot_\alpha, \leq_\alpha)$ satisfies the same regularity condition for all $\alpha \in Y$.*

Proof. Assume that S satisfies (C4); that is S is left intra-quasi-regular. Let $\alpha \in Y$. To show that $(S_\alpha, \cdot_\alpha, \leq_\alpha)$ satisfies (C4), let $a \in S_\alpha$. By assumption, $a \leqslant xayaz$ for some $x, y, z \in S$. Since $S = \bigcup_{\nu \in Y} S_\nu$, there exist $\beta, \gamma, \delta \in Y$ such that $x \in S_\beta, y \in S_\gamma, z \in S_\delta$. We have $\alpha\beta = \alpha\gamma = \alpha\delta = \alpha$ because $a \in S_\alpha$ and $a \leqslant axayaz$, so

$$\begin{aligned} a &\leqslant xayaz \leqslant x(xayaz)y(xayaz)z = (xxay)a(zyx)a(yazz) \\ &\leqslant (xxay)(xayaz)(zyx)a(yazz) = (xxayx)a(yazzyx)a(yazz) \in S_\alpha a S_\alpha a S_\alpha. \end{aligned}$$

Then $a \in (S_\alpha a S_\alpha a S_\alpha]$. So S_α satisfies (C4). The rest of the assertions can be proved similarly. □

Theorem 2. *The following statements hold for an ordered semigroup $(S, \cdot, \leqslant)$:*

(1) *S has an intra-quasi-regular element if and only if S has an intra-regular element.*

(2) *S has a left quasi-regular element if and only if S has a left regular element.*

(3) *S has a right quasi-regular element if and only if S has a right regular element.*

Proof. (1) Assume that S has an intra-quasi-regular element a; then $a \leqslant xayaz$ for some $x, y, z \in S$. We have

$$\begin{aligned} yaz &\leqslant y(xayaz)z = (yx)a(yazz) \leqslant (yx)(xayaz)(yazz) \\ &= (yxxa)(yaz)(yaz)z \in S(yaz)^2S. \end{aligned}$$

Then $yaz \in (S(yaz)^2S]$, and S has an intra-regular element yaz.

Conversely, assume that S has an intra-regular element a. That is, $a \leqslant xa^2y$ for some $x, y \in S$. We have

$$a \leqslant xa^2y \leqslant xa(xa^2y)y = xaxa(ayy) \in SaSaS.$$

Then $a \in (SaSaS]$, and S has an intra-quasi-regular element a.

(2) Assume that S has a left quasi-regular element a; then $a \leqslant xaya$ for some $x, y \in S$. Thus,

$$\begin{aligned} ya &\leqslant y(xaya) = (yx)a(ya) \leqslant (yx)(xaya)(ya) \\ &= (yxxa)(ya)(ya) \in S(ya)^2. \end{aligned}$$

So $ya \in (S(ya)^2]$, and S has a left regular element ya.

Conversely, assume that S has a left regular element a. Then $a \leqslant xa^2$ for some $x \in S$. Since

$$a \leqslant xa^2 \leqslant xaxa^2 = xa(xa)a \in SaSa$$

then $a \in (SaSa]$, and a is a left quasi-regular element. That (3) holds can be proved analogously. □

Theorem 3. *For an element a of an ordered semigroup $(S, \cdot, \leqslant)$, the following statements hold:*

(1) *a is intra-quasi-regular if and only if the principal two-sided ideal $J(a)$ of S has an intra-regular generator.*
(2) *a is left quasi-regular if and only if the principal left ideal $L(a)$ of S has a left regular generator.*
(3) *a is right quasi-regular if and only if the principal right ideal $R(a)$ of S has a right regular generator.*

Proof. (1) Assume that $a \in S$ is intra-quasi-regular; then $a \leqslant xayaz$ for some $x, y, z \in S$. Since $a \in J(a)$, $J(yaz) \subseteq J(a)$. By $a \leqslant xayaz$, $J(a) \subseteq J(yaz)$. Then $J(a) = J(yaz)$. As the proof of Theorem 2 we have yaz is intra-regular, and then $J(a)$ has an intra-regular generator.

Conversely, assume that the principal ideal $J(a)$ has an intra-regular generator b. Then $J(a) = J(b)$ and $b \leqslant pb^2q$ for some $p, q \in S$. We have

$$a \in J(b) = J(pb^2q) = (pb^2q \cup S(pb^2q) \cup (pb^2q)S \cup S(pb^2q)S] \subseteq (Sb^2S].$$

Since $b \in J(a)$, then $b^2 \in J(a)J(a) \subseteq (SaSaS]$. Hence, a is intra-quasi-regular. That (2) and (3) hold can be proved similarly. □

Next, we deal with ordered semigroups satisfying $c \leqslant xc^2yc$, and satisfying both of $c \leqslant xc^2yc$ and $c \leqslant cxc^2y$.

Theorem 4. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. The following are equivalent:*

(1) $a \in (SbSa]$ *for all* $a, b \in S$;
(2) S *is simple and left quasi-regular;*
(3) S *is simple and left reproduce;*
(4) *every left ideal of* S *is simple;*
(5) S *is simple and every left ideal of* S *is intra-regular.*

Proof. (1) $\Longleftrightarrow$ (2): Assume that $a \in (SbSa]$ for all $a, b \in S$. Since $a \in (SaSa]$ for any $a \in S$, S is left quasi-regular. To show that S is simple, let $a \in S$. Clearly, $(SaS] \subseteq S$. By assumption, $a \in (SaSa] \subseteq (SaS]$, and so $S \subseteq (SaS]$. Then $S = (SaS]$.

Conversely, assume that S is simple and left quasi-regular. Let $a, b \in S$. Since S is simple, $S = (SaS]$ and $S = (SbS]$. Since S is left quasi-regular, $a \in (SaSa]$, and so $S = (SaSa]$. Thus

$$a \in S = (SbS] \subseteq (Sb(SaSa]] \subseteq ((S](b](SaSa]] = (SbSaSa] \subseteq (SbSa],$$

as required.

(1) $\Longleftrightarrow$ (3): If $a \in (SbSa]$ for all $a, b \in S$, then $a \in (SaSa]$ for all $a \in S$; hence $a \in (Sa]$ for all $a \in S$. We have S is left reproduce. As in the proof of (1) $\Longleftrightarrow$ (2), S is simple.

Conversely, assume that S is simple and left reproduce. Let $a, b \in S$. Since S is simple, $S = (SaS]$ and $S = (SbS]$. Since S is left reproduce, $a \in (Sa]$, so $S = (Sa]$. Thus

$$a \in S = (SbS] \subseteq (Sb(Sa]] \subseteq ((S](b](Sa]] = (SbSa],$$

as required.

(1) $\Longleftrightarrow$ (4): Assume that $a \in (SbSa]$ for all $a, b \in S$. Let L be a left ideal of S, and let $a \in L$. Clearly, $(LaL] \subseteq (LLL] \subseteq (L] = L$. If $b \in L$, then $b \in (SaaSb]$ by assumption. Since

$$(SaaSb] \subseteq (SLaSL] \subseteq (LaL]$$

it follows that $b \in (LaL]$, and $(LaL] = L$. Hence, L is simple.

Conversely, assume that every left ideal of S is simple. Let $a, b \in S$. Since $(a \cup Sa]$ is a left ideal of S, it follows by assumption that

$$\begin{aligned}(a \cup Sa] &= ((a \cup Sa](ba)(a \cup Sa]] \subseteq ((a \cup Sa](ba](a \cup Sa]] \\ &= ((a \cup Sa)(ba)(a \cup Sa)] = (abaa \cup abaSa \cup Sabaa \cup SabaaSa] \\ &\subseteq (SbSa].\end{aligned}$$

Hence, (1) holds.

(1) $\Longleftrightarrow$ (5): Assume that $a \in (SbSa]$ for all $a, b \in S$. As in the proof of (1) $\Longleftrightarrow$ (2) we have S is simple. Let L be a left ideal of S, and let $a \in L$. By assumption,

$$a \in (SaaaSa] \subseteq (SLaaSL] \subseteq (La^2L].$$

Then L is intra-regular.

Conversely, assume that S is simple and every left ideal of S is intra-regular. Let $a, b \in S$. Since S is simple, $(SaS] = (SbS]$. Since $(a \cup Sa]$ is a left ideal of S, we have $(a \cup Sa]$ is intra-regular, and so $a \in ((a \cup Sa]aa(a \cup Sa]]$. Consider:

$$\begin{aligned} a \in ((a \cup Sa]aa(a \cup Sa]] &\subseteq ((a \cup Sa](aa](a \cup Sa]] = ((a \cup Sa)(aa)(a \cup Sa)] \\ &= (aaaa \cup aaaSa \cup Saaaa \cup SaaaSa] \subseteq (SaSa] \subseteq ((SaS]a] = ((SbS]a] \\ &\subseteq ((SbS](a]] = (SbSa]. \end{aligned}$$

Hence, (1) holds. □

An ordered semigroup $(S, \cdot, \leqslant)$ is called *completely quasi-regular* (resp. *completely reproduce*) if S is left and right quasi-regular (resp. left and right reproduce). Using Theorem 4 and its dual, we have:

Corollary 1. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. The following are equivalent:*

(1) $a \in (SbSa] \cap (bSaS]$ *for all* $a, b \in S$;
(2) S *is simple and completely quasi-regular;*
(3) S *is simple and completely reproduce;*
(4) *every one-sided ideal of* S *is simple;*
(5) S *is simple and every one-sided ideal of* S *is intra-regular.*

Theorem 5. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. The following are equivalent:*

(1) S *satisfies the regularity condition* $c \leqslant xc^2yc$;
(2) S *is intra-regular and left quasi-regular;*
(3) *every left ideal of* S *is intra-regular;*
(4) *every left ideal of* S *is intra-quasi-regular.*

Proof. (1) $\Longleftrightarrow$ (2): That (1) $\Longrightarrow$ (2) is clear. To prove (2) $\Longrightarrow$ (1), assume that S is intra-regular and left quasi-regular. Let $a \in S$. Since S is intra-regular, $a \leqslant xa^2y$ for some $x, y \in S$. Since S is left quasi-regular, $a \leqslant uava$ for some $u, v \in S$. Then

$$a \leqslant uava \leqslant uxa^2yva.$$

Hence S satisfies the regularity condition $c \leqslant xc^2yc$.

(1) $\Longrightarrow$ (3): Assume that S satisfies the regularity condition $c \leqslant xc^2yc$. Let L be a left ideal of S. If $a \in L$, then by assumption we have $a \leqslant xa^2ya$ for some $x, y \in S$, and $a^2 \leqslant ua^4va^2$ for some $u, v \in S$. Thus,

$$a \leqslant xa^2ya \leqslant x(ua^4va^2)ya = (xua^2)a^2(va^2ya) \in La^2L$$

it follows that $a \in (La^2L]$, and L is intra-regular.

(3) $\Longrightarrow$ (4): This is easy to see.

(4) $\Longrightarrow$ (1): Assume that every left ideal of S is intra-quasi-regular. Let $a \in S$. Since $(a \cup Sa]$ is a left ideal of S, $(a \cup Sa]$ is intra-quasi-regular. Then

$$\begin{aligned} a &\in ((a \cup Sa]a(a \cup Sa]a(a \cup Sa]] \subseteq ((a \cup Sa](a](a \cup Sa](a](a \cup Sa]] \\ &= ((a \cup Sa)a(a \cup Sa)a(a \cup Sa)] \subseteq (Sa^2Sa]. \end{aligned}$$

Hence S satisfies the condition $c \leqslant xc^2yc$. □

Using Theorem 5 and its dual, we have the following.

Corollary 2. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. The following are equivalent:*

(1) *S satisfies the regularity conditions $c \leqslant xc^2yc$ and $c \leqslant cxc^2y$;*
(2) *S is intra-regular and completely quasi-regular;*
(3) *every one-sided ideal of S is intra-regular;*
(4) *every one-sided ideal of S is intra-quasi-regular.*

We next consider ordered semigroups satisfying the regularity $c \leqslant cxc^2yc$.

Theorem 6. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. The following are equivalent:*

(1) *$a \in (aSbSa]$ for all $a, b \in S$;*
(2) *S is simple and regular;*
(3) *every bi-ideal of S is simple.*

Proof. (1) $\Longrightarrow$ (2): Assume that $a \in (aSbSa]$ for all $a, b \in S$. Then, for any $a \in S$, we have $a \in (aSaSa] \subseteq (aSa]$. Hence, S is regular. Since $(aSaS] \subseteq (SaS]$, $S \subseteq (SaS]$, and so S is simple.

(2) $\Longrightarrow$ (1): Assume that S is simple and regular. Let $a, b \in S$. Since S is simple, $S = (SbS]$. Since S is regular, $a \in (aSa]$. Then

$$a \in (a(SbS]a] \subseteq ((a](SbS](a]] = (aSbSa]$$

as required.

(1) $\Longrightarrow$ (3): Assume that $a \in (aSbSa]$ for all $a, b \in S$. Let B be a bi-ideal of S. Then $(BSB] \subseteq B$. If $b \in B$, then $b \in (bSbSb] \subseteq (BSBSB] \subseteq (BSB]$. Thus $B \subseteq (BSB]$, and B is simple.

(3) $\Longrightarrow$ (1): Assume that every bi-ideal of S is simple. Let $a, b \in S$. Since $(a \cup a^2 \cup aSa]$ is a bi-ideal of S, it follows by assumption that

$$\begin{aligned} a \in (a \cup a^2 \cup aSa] &= ((a \cup a^2 \cup aSa]aba(a \cup a^2 \cup aSa]] \\ &\subseteq ((a \cup a^2 \cup aSa](aba](a \cup a^2 \cup aSa]] \\ &= ((a \cup a^2 \cup aSa)aba(a \cup a^2 \cup aSa)] \subseteq (aSbSa]. \end{aligned}$$

Thus (1) holds. □

Theorem 7. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. The following are equivalent:*

(1) *S satisfies the regularity condition $c \leqslant cxc^2yc$;*
(2) *S is intra-regular and regular;*
(3) *every left ideal of S is right quasi-regular;*
(4) *every right ideal of S is left quasi-regular;*
(5) *every bi-ideal of S is intra-regular;*
(6) *every bi-ideal of S is intra-quasi-regular.*

Proof. (1) $\Longleftrightarrow$ (2): That (1) $\Longrightarrow$ (2) is clear. To show that (2) $\Longrightarrow$ (1), assume that S is intra-regular and regular. Let $a \in S$. Since S is regular, $a \leqslant axa$ for some $x \in S$. Since S is intra-regular, $a \leqslant ya^2z$ for some $y, z \in S$. We have

$$a \leqslant (ax)a \leqslant (ax)a(xa) \leqslant (ax)ya^2z(xa).$$

Then (1) holds.

(1) $\Longrightarrow$ (3): Assume that S satisfies the regularity condition $c \leqslant cxc^2yc$. Let L be a left ideal of S, and let $a \in L$. By assumption, $a \leqslant axa^2ya$ for some $x, y \in S$. By $xa, ya \in L$, it follows that

$$a \leqslant axa^2ya = a(xa)a(ya) \in aLaL.$$

Thus $a \in (aLaL]$. Hence, L is right quasi-regular.

(3) $\Longrightarrow$ (1): Assume that every left ideal of S is right quasi-regular. Let $a \in S$. Since $(a \cup Sa]$ is a left ideal of S, $(a \cup Sa]$ is right quasi-regular. Then

$$a \in (a(a \cup Sa]a(a \cup Sa]] \subseteq ((a](a \cup Sa](a](a \cup Sa]] = (a(a \cup Sa)a(a \cup Sa)].$$

This implies that $a \in (aSa^2Sa]$, and S satisfies the regularity condition $c \leqslant cxc^2yc$.

(1) $\Longrightarrow$ (4): Assume that S satisfies the regularity condition $c \leqslant cxc^2yc$. Let R be a right ideal of S, and let $a \in R$. By assumption, $a \leqslant axa^2ya$ for some x, y in S. By $ax, ay \in R$, it follows that

$$a \leqslant axa^2ya = (ax)a(ay)a \in RaRa.$$

Thus $a \in (RaRa]$, whence R is left quasi-regular.

(4) $\Longrightarrow$ (1): Assume that every right ideal of S is left quasi-regular. Let $a \in S$. Since $(a \cup aS]$ is a right ideal of S, $(a \cup aS]$ is left quasi-regular. Then

$$a \in ((a \cup aS]a(a \cup aS]a] \subseteq ((a \cup aS](a](a \cup aS](a]] = ((a \cup aS)a(a \cup aS)a].$$

This implies that $a \in (aSa^2Sa]$, and S satisfies the regularity condition $c \leqslant cxc^2yc$.

(1) $\Longrightarrow$ (5): Assume that S satisfies the regularity condition $c \leqslant cxc^2yc$. Let B be a bi-ideal of S, and let $a \in B$. Then $a \leqslant axa^2ya$ for some $x, y \in S$ and $a^2 \leqslant a^2ua^4va^2$ for some $u, v \in S$. We have

$$a \leqslant axa^2ya \leqslant ax(a^2ua^4va^2)ya = (axa^2ua)a^2(ava^2ya) \in (BSB)a^2(BSB) \subseteq Ba^2B$$

Then $a \in (Ba^2B]$, and B is intra-regular.

(5) $\Longrightarrow$ (6): This is easy to see.

(6) $\Longrightarrow$ (1): Assume that every bi-ideal of S is intra-quasi-regular. Let $a \in S$. Since $(a \cup a^2 \cup aSa]$ is a bi-ideal of S, $(a \cup a^2 \cup aSa]$ is intra-quasi-regular. Consider:

$$\begin{aligned} a &\in ((a \cup a^2 \cup aSa]a(a \cup a^2 \cup aSa]a(a \cup a^2 \cup aSa]] \\ &\subseteq ((a \cup a^2 \cup aSa](a](a \cup a^2 \cup aSa](a](a \cup a^2 \cup aSa]] \\ &= ((a \cup a^2 \cup aSa)a(a \cup a^2 \cup aSa)a(a \cup a^2 \cup aSa)] \\ &\subseteq (aSa^2Sa] \end{aligned}$$

Thus, S satisfies the regularity condition $c \leqslant cxc^2yc$. □

Finally, ordered semigroups satisfying left regularity and complete regularity conditions will be characterized.

Theorem 8. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. The following are equivalent:*

(1) *S is left regular;*
(2) *every left ideal of S is left quasi-regular;*
(3) *every left ideal of S is left reproduce.*

Proof. (1) $\Longrightarrow$ (2): Assume that S is left regular. Let L be a left ideal of S, and let $a \in L$. By assumption, $a \leqslant xa^2$ for some $x \in S$. We have

$$a \leqslant xaa \leqslant x(xaa)a \leqslant x(x(xaa)a)a = (xxxa)a(aa) \in LaLa.$$

That is: $a \in (LaLa]$. Hence L is left quasi-regular.

(2) $\Longrightarrow$ (3): This is easy to see.

(3) $\Longrightarrow$ (1): Assume that every left ideal of S is left reproduce. Let $a \in S$. By assumption, $(a \cup Sa]$ is left reproduce. Then

$$a \in ((a \cup Sa]a] \subseteq ((a \cup Sa](a]] = ((a \cup Sa)a] = (a^2 \cup Sa^2].$$

This implies $a \in (Sa^2]$, and S is left regular. □

An ordered semigroup $(S, \cdot, \leqslant)$ is called *completely regular* if S satisfies both of the regularity conditions $c \leqslant c^2x$ and $c \leqslant xc^2$, equivalently, if S satisfies the regularity condition $c \leqslant c^2xc^2$. The proof of the following assertion will be omitted.

Theorem 9. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. The following are equivalent:*

(1) *S is completely regular;*
(2) *S is left regular, right regular, left quasi-regular, and right quasi-regular;*
(3) *every left ideal of S is left regular, and every right ideal is right regular;*
(4) *every left and right ideal of S is completely quasi-regular;*
(5) *every bi-ideal of S is left and right quasi-regular.*

References

[1] **S. Bogdanović, M. Ćirić and M. Mitrović**, *Semigroups satisfying certain regularity conditions*, Advances in Algebra, Proc. ICM Satellite Confer. Algebra and Related Topics, Hong Kong, 2002, World Scientific, 2003, 46 – 59.

[2] **S. Bogdanovíc, M. Ćiríc and M. Mitrovíc**, *Linear equations and regularity conditions on semigroups*, Semigroup Forum, **69** (2004), 63 – 74.

[3] **L. Bussaban and T. Changphas**, *A note on (m,n)-ideals in regular duo ordered semigroups*, Quasigroups and Related Systems, **23** (2015), 211 – 216.

[4] **L. Bussaban and T. Changphas**, *On (m,n)-ideals and (m,n)-regular ordered semigroups*, Songklanakarin J. Sci. Technol., **38** (2016), 199 – 206.

[5] **Y. Cao**, *Characterizations of regular ordered semigroups by quasi-ideals*, Vietnam J. Math., **30** (2002), 239 – 250.

[6] **T. Changphas, P. Summaprab**, *On ordered semigroups containing covered one-sided ideals*, Quasigroups and Related Systems, **25** (2017), 201 – 210.

[7] **L. Fuchs**, *Partially Ordered Algebraic Systems*, Addison-Wesley Publishing Co., Pergamon Press, 1963.

[8] **N. Kehayopulu**, *Note on Green's relations in ordered semigroups*, Math. Japon., **37** (1991), 211 – 214.

[9] **S. Lajos and G. Szász**, *Generalized regularity in semigroups*, Dept. Math. K. Marx Univ. of Economics, Budapest, **75** (1975), 1 – 23.

[10] **J. von Neumann**, *On regular rings*, Proc. Nat. Acad. Sci., USA, **22** (1936), 707 – 713.

[11] **T. Phochai and T. Changphas**, *Linear inequations and regularity conditions on ordered semigroups*, An. Stiint. Univ. Al. I. Cuza Iasi. Mat. (N.S.), **63** (2017), 627 – 636.

[12] **G. Szász**, *On semigroups in which $a \in Sa^kS$ for any element*, Math. Japon., **20** (1976), 283 – 284.

Received March 02, 2020
Revised June 14, 2020

Department of Mathematics, Faculty of Science, Khon Kaen University, Khon Kaen 40002, Thailand
Centre of Excellence in Mathematics, CHE, Si Ayuttaya Rd., Bangkok 10400, Thailand
E-mails: sanborisoot@hotmail.com, thacha@kku.ac.th

Quasigroups and Related Systems **28** (2020), 319 – 338

Families of semi-automata in finite quasigroups and iterated hash functions

Volodymyr G. Skobelev and Volodymyr V. Skobelev

Abstract. Families of semi-automata defined by a recurrence relation in a finite quasigroup are investigated. Initially, these families are defined in an abstract finite quasigroup, and their structure is studied. It is shown that from a probabilistic point of view these semi-automata are the best mathematical models for computationally secure families of iterated hash functions. Then families of semi-automata in T-quasigroups determined by a finite Abelian group are defined, and their structure is studied. Representation of these semi-automata by the parallel composition of the ones defined in T-quasigroups determined by cyclic groups of prime power order is considered. This decomposition results in speed up the functioning and reducing space complexity of a semi-automaton. In addition, families of semi-automata in the Abelian group of an elliptic curve over a finite field are investigated.

1. Introduction

Over the past two decades, intensive research of quasigroups has been largely caused by their successful applications in various fields, including cryptography. The significance of the latter is as follows.

Currently, the main approach to solving cryptography problems relies on algebraic models. Most of them are built in finite associative algebraic systems. However, for algebraic systems without the requirements "to be associative", "to be commutative", and "to be with unit", high complexity of solving identification problems is typical. Such algebraic systems include quasigroups [2, 18], i.e. magma with both left and right division. It seems promising to apply quasigroups to solving cryptography problems due to the following two circumstances, at least. Firstly, they have been applied successfully in the design of basic cryptography primitives including block and stream ciphers, public key crypto-schemes, signature schemes, codes, and hash functions [7, 10, 13, 14]. Secondly, a hardware implementation of encryption based on a finite quasigroup has been designed [15]. Some applications of quasigroups to solving cryptography problems have also been considered in [3, 4, 17].

Among the above pointed cryptography primitives, hash functions should be noted, since they are widely used for information protection. We remind, that any

2010 Mathematics Subject Classification: 20N05, 20K01, 68Q70, 94A60
Keywords: finite quasigroups, finite T-quasigroups, semi-automata, hash functions, computational security, elliptic curves

hash function is a mapping that transforms any binary string (a message) into a binary string of some fixed length (this string is the hash value or, simply, the hash). Informally, a cryptographic hash function (see [16], for example) satisfies the following four conditions:

1. The hash of any message can be computed sufficiently easy.
2. It is infeasible to reconstruct the original message via its hash.
3. It is infeasible to find two different messages with the same hash.
4. Small changes in a message lead to uncorrelated changes in its hash.

Numerous attempts for the design and implementation of cryptographic hash functions have led to the notion of an iterated hash function [16]. It can be characterized as follows. The original message is divided into the blocks of the equal length. If necessary, the last block is extended to the required length by its concatenation with some fixed string. Some fixed block is added as the initial fragment. Firstly, this block is hashed in accordance with a certain rule. Then the iterative process starts: the next hash is computed from the current hash and the current block of the message. The final hash is the hash of the original message.

It is evident that a mathematical model for iterated hash function is a semi-automaton, i.e. an automaton without output mapping. Hence, investigation of families of semi-automata defined by recurrence relations in a finite quasigroup due to their possible applications as mathematical models of iterated hash function is actual from both theoretic and applied point of view. Some attempts to solve this problem have been done in [19-21]. The main aim of the given paper is to generalize and to unify these results. By time and space complexity we mean asymptotic the worst-case complexity under logarithmic weight [1].

The rest of the paper is organized as follows. Section 2 contains mathematical notions and structures sufficient to present the results. In Section 3 basic families of semi-automata defined by a recurrence relation in a finite abstract quasigroup are investigated. In Section 4 these families of semi-automata are detailed for finite T-quasigroups. Section 5 is devoted to semi-automata defined by a recurrence relation in the Abelian group of an elliptic curve over a finite field. Section 6 is some discussion of obtained results. Section 7 contains concluding remarks.

2. Mathematical backgrounds

2.1. Abstract quaigroups and iterated hash functions

A semi-automaton (SA) is a triple $M = (Q, X, \delta)$, where Q ($|Q| \geqslant 2$) is a finite set of states, X is a finite input alphabet, and $\delta : Q \times X \to Q$ is the transition mapping. This mapping can be extended onto the set $Q \times X^+$ by the equality $\delta(q, wx) = \delta(\delta(q, w), x)$ $(w \in X^+, x \in X)$.

An initial SA is a pair (M, q) $(q \in Q)$, where q is the initial state. Any initial SA (M, q) implements the mapping $H_{(M,q)} : X^+ \to Q$ defined by the equality $H_{(M,q)}(w) = \delta(q, w)$ $(w \in X^+)$. This mapping can be interpreted as an iterated

hash function. Hence, any SA $M = (Q, X, \delta)$ implements the family of iterated hash functions $\mathfrak{H}_M = \{H_{(M,q)}\}_{q \in Q}$.

Let $\mathfrak{Q}_Q$ be the set of all quasigroups with the finite carrier Q ($|Q| \geqslant 2$).

Based on the Cayley table, we get for any quasigroup $\mathcal{Q} = (Q, \circ) \in \mathfrak{Q}_Q$ that the upper bounds of time and space complexity for computation the element $a \circ b$ ($a, b \in Q$) are equal, correspondingly, to:

$$T_\circ = O(|Q| \log |Q|) \quad (|Q| \to \infty), \tag{1}$$

$$V_\circ = O(|Q|^2 \log |Q|) \quad (|Q| \to \infty). \tag{2}$$

Besides, for any mapping $\chi : Q \to Q$ the upper bounds of time and space complexity for computation the value $\chi(a)$ ($a \in Q$) are equal, correspondingly, to:

$$T_\chi = O(|Q| \log |Q|) \quad (|Q| \to \infty), \tag{3}$$

$$V_\chi = O(|Q| \log |Q|) \quad (|Q| \to \infty). \tag{4}$$

Any quasigroup $\mathcal{Q} = (Q, \circ) \in \mathfrak{Q}_Q$ can be presented by the labeled directed graph $\Gamma_\mathcal{Q}$ with the set of vertices Q such that for any $q_1, q_2, q \in Q$ there is an arc started in the vertex q_1, terminated in the vertex q_2, and labeled by the element q if and only if $q_1 \circ q = q_2$. It is evident that $\Gamma_\mathcal{Q}$ is completed labeled directed graph with a single loop in each vertex. Besides, for any vertex $q \in Q$, all $|Q|$ arcs started in q terminate in pair-wise different vertices, and exactly $|Q|$ arcs are terminated in q and labels of these arcs are pair-wise different. We can interpret $\Gamma_\mathcal{Q}$ as the SA $\Gamma_\mathcal{Q} = (Q, Q, \circ)$, where Q is both the set of the states and the input alphabet, and $\circ$ is the transition mapping. This SA implements the family of iterated hash functions $\mathfrak{H}_{\Gamma_\mathcal{Q}} = \{H_{(\Gamma_\mathcal{Q},q)}\}_{q \in Q}$. Since elements of the family $\mathfrak{H}_{\Gamma_\mathcal{Q}}$ are pair-wise different hash functions, this family can be identified with the set $\mathfrak{H}_{\Gamma_\mathcal{Q}} = \{H_{(\Gamma_\mathcal{Q},q)} | q \in Q\}$.

Remark 1. It is known, that the set of string transformations [8, 9, 11, 12] of any quasigroup $\mathcal{Q} = (Q, \circ) \in \mathfrak{Q}_Q$ contains the set of bijections $e_{q,\circ} : Q^+ \to Q^+$ ($q \in Q$), where $e_{q,\circ}(q_1 q_2 \dots q_m) = q'_1 q'_2 \dots q'_m$ ($q_1 q_2 \dots q_m \in Q^+$; $m = 1, 2, \dots$) if and only if $q'_1 = q \circ q_1$ and $q'_i = q'_{i-1} \circ q_i$ ($i = 2, \dots m$). Relationship between the sets of mappings $\{e_{q,\circ} | q \in Q\}$ and $\mathfrak{H}_{\Gamma_\mathcal{Q}} = \{H_{(\Gamma_\mathcal{Q},q)} | q \in Q\}$ is that the equality $e_{q,\circ}(q_1 q_2 \dots q_m) = q'_1 q'_2 \dots q'_m$ implies the equality $H_{(\Gamma_\mathcal{Q},q)}(q_1 q_2 \dots q_m) = q'_m$.

Proposition 1. *Let $\mathcal{Q} = (Q, \circ) \in \mathfrak{Q}_Q$ be any quasigroup. Then:*

1. *For any elements $q, q' \in Q$ holds the equality*

$$|\{x \in Q^m | H_{(\Gamma_\mathcal{Q},q)}(x) = q'\}| = |Q|^{m-1} \quad (m = 1, 2, \dots). \tag{5}$$

2. *For any elements $q, q', q'' \in Q$ ($q \neq q'$) holds the equality*

$$\{x \in Q^+ | H_{(\Gamma_\mathcal{Q},q)}(x) = q''\} \cap \{x \in Q^+ | H_{(\Gamma_\mathcal{Q},q')}(x) = q''\} = \emptyset. \tag{6}$$

Proof. By induction on the length of an input string. □

Since $H^{-1}_{(\Gamma_{\mathcal{Q}},q)}(q') = \{x \in Q^+ | H_{(\Gamma_{\mathcal{Q}},q)}(x) = q'\}$ $(q, q' \in Q)$, we can present (5) and (6) as follows:

$$|H^{-1}_{(\Gamma_{\mathcal{Q}},q)}(q') \cap Q^m| = |Q|^{m-1} \quad (q, q' \in Q;\ m = 1, 2, \dots), \tag{7}$$

$$H^{-1}_{(\Gamma_{\mathcal{Q}},q)}(q'') \cap H^{-1}_{(\Gamma_{\mathcal{Q}},q')}(q'') = \emptyset \quad (q, q', q'' \in Q;\ q \neq q'). \tag{8}$$

Let $\mathsf{P}^{(1)}_{\Gamma_{\mathcal{Q}},q,m}(q')$ $(q, q' \in Q;\ m = 1, 2, \dots)$ be the probability that uniformly randomly chosen input string $x \in Q^m$ is a solution of equation $H_{(\Gamma_{\mathcal{Q}},q)}(x) = q'$, and $\mathsf{P}^{(2)}_{\Gamma_{\mathcal{Q}},q,m}$ $(q \in Q;\ m = 1, 2, \dots)$ be the probability that for two uniformly randomly chosen input strings $x, x' \in Q^m$ $(x \neq x')$ the equality $H_{(\Gamma_{\mathcal{Q}},q)}(x) = H_{(\Gamma_{\mathcal{Q}},q)}(x')$ holds. Applying (7) and (8), it is not difficult to prove the following theorem.

Theorem 1. *Let $\mathcal{Q} = (Q, \circ) \in \mathfrak{Q}_Q$ be any quasigroup. Then:*

$$P^{(1)}_{\Gamma_{\mathcal{Q}},q,m}(q') = |Q|^{-1} \quad (q, q' \in Q;\ m = 1, 2, \dots), \tag{9}$$

$$P^{(2)}_{\Gamma_{\mathcal{Q}},q,m} = |Q|^{-1}(1 - (|Q| - 1)(|Q|^m - 1)^{-1}) \quad (q \in Q;\ m = 1, 2, \dots). \tag{10}$$

It follows directly from (9) and (10) that $\lim\limits_{|Q|\to\infty} \mathsf{P}^{(1)}_{\Gamma_{\mathcal{Q}},q,m}(q') = 0$ $(q, q' \in Q)$ and $\lim\limits_{m\to\infty} \mathsf{P}^{(2)}_{\Gamma_{\mathcal{Q}},q,m} = |Q|^{-1}$. This is a significant argument to use finite quasigroups in mathematical models of cryptographic iterated hash functions.

2.2. T-quaigroups

A quasigroup $\mathcal{Q} = (Q, \circ) \in \mathfrak{Q}_Q$ is a T-quasigroup [6] if there exist an Abelian group $\mathcal{G} = (Q, +)$, some ordered pair $(\xi, \zeta) \in \mathrm{Aut}(\mathcal{G}) \times \mathrm{Aut}(\mathcal{G})$, and an element $c \in Q$ such that holds the equality

$$a \circ b = \xi(a) + \zeta(b) + c \quad (a, b \in Q). \tag{11}$$

It follows from this definition that any finite Abelian group $\mathcal{G} = (Q, +)$ $(|Q| \geqslant 2)$ determines the family of T-quasigroups $\mathfrak{F}_{\mathcal{G}} = \{(Q, +, \xi, \zeta, c)\}_{\xi,\zeta\in\mathrm{Aut}(\mathcal{G});c\in Q}$, where $(Q, +, \xi, \zeta, c)$ is the T-quasigroup $\mathcal{Q} = (Q, \circ) \in \mathfrak{Q}_Q$ such that the operation $\circ$ is defined by the equality (11). Since elements of the family $\mathfrak{F}_{\mathcal{G}}$ are pair-wise different T-quasigroups (see Theorem 1 in [20]), this family can be identified with the set $\mathfrak{F}_{\mathcal{G}} = \{(Q, +, \xi, \zeta, c) | \xi, \zeta \in \mathrm{Aut}(\mathcal{G}); c \in Q\}$.

Let $\varepsilon_Q : Q \to Q$ be the identity mapping. It is not difficult to prove that for any finite Abelian group $\mathcal{G} = (Q, +)$ $(|Q| \geqslant 2)$:

1. There exists the left unit e_l in a T-quasigroup $(Q, +, \xi, \zeta, c) \in \mathfrak{F}_{\mathcal{G}}$ if and only if $\zeta = \varepsilon_Q$. In this case, $e_l = -\xi^{-1}(c)$.

2. There exists the right unit e_r in a T-quasigroup $(Q, +, \xi, \zeta, c) \in \mathfrak{F}_{\mathcal{G}}$ if and only if $\xi = \varepsilon_Q$. In this case, $e_l = -\zeta^{-1}(c)$.

3. $(Q, +, \xi, \zeta, c) \in \mathfrak{F}_{\mathcal{G}}$ is a loop if and only if $\xi = \zeta = \varepsilon_Q$. In this case, $e = -c$.

4. $(Q,+,\xi,\zeta,c)\in\mathfrak{F}_{\mathcal{G}}$ is a commutative T-quasigroup if and only if $\xi=\zeta$ (see Theorem 2 in [20]).

5. $(Q,+,\xi,\zeta,c)\in\mathfrak{F}_{\mathcal{G}}$ is an associative T-quasigroup if and only if $\xi=\zeta=\varepsilon_Q$ (see Theorem 3 in [20]).

Remark 2. Therefore, for T-quasigroups the statements "a loop", "to be associative", and "to be associative-commutative" are the same.

Due to Fundamental Theorem, any Abelian group can be presented uniquely as a direct product of cyclic groups of prime-power order. More precisely, let $\mathcal{G}=(Q,+)$ ($|Q|\geqslant 2$) be any Abelian group, such that $|Q|=p_1^{r_1}\dots p_m^{r_m}$ ($m\geqslant 1$), where $r_i\geqslant 1$ ($i=1,\dots,m$) and p_i ($i=1,\dots,m$) are pair-wise different prime integers. Then

$$\mathcal{G}\cong\bigotimes_{i=1}^{m}\bigotimes_{j=1}^{k_i}(\mathbb{Z}_{p_j^{d_{ij}}},+_{ij}), \tag{12}$$

where $\cong$ is the isomorphism relation, d_{ij} ($i=1,\dots,m;j=1,\dots,k_i$) are fixed positive integers such that $1\leqslant d_{i1}\leqslant\dots\leqslant d_{ik_i}$ ($i=1,\dots,m$), $r_i=\sum\limits_{j=1}^{k_i}d_{ij}$ ($i=1,\dots,m$), $\mathbb{Z}_{p_j^{d_{ij}}}=\{0,1,\dots,p_j^{d_{ij}}-1\}$ ($i=1,\dots,m;j=1,\dots,k_i$), and $+_{ij}$ ($i=1,\dots,m;j=1,\dots,k_i$) is the module $p_j^{d_{ij}}$ addition. Due to (12), any element $z\in Q$ can be identified with a vector $z=(z_{11},\dots,z_{1k_1},\dots,z_{m1},\dots,z_{mk_m})$, where $z_{ij}\in\mathbb{Z}_{p_j^{d_{ij}}}$ ($i=1,\dots,m;j=1,\dots,k_i$). Hence, computation the sum $x+y$ ($x,y\in Q$) can be reduced to independent additions of corresponding components of vectors x and y. From here it follows that for any Abelian group $\mathcal{G}=(Q,+)$ ($|Q|\geqslant 2$) that satisfies to (12), time and space complexity for computation the element $x+y$ ($x,y\in Q$) are equal, correspondingly, to:

$$T_+=O(\sum_{i=1}^{m}\sum_{j=1}^{k_i}d_{ij}\log p_i)\quad(|Q|\to\infty), \tag{13}$$

$$V_+=O(\sum_{i=1}^{m}\sum_{j=1}^{k_i}d_{ij}\log p_i)\quad(|Q|\to\infty). \tag{14}$$

Remark 3. If additions of the corresponding components of vectors x and y can be implemented in parallel then time complexity for computation the element $x+y$ can be reduced to

$$T_+=O(\max_{i=1,\dots m}\max_{j=1,\dots k_i}d_{ij}\log p_i)\quad(|Q|\to\infty). \tag{15}$$

If an Abelian group $\mathcal{G}=(Q,+)$ ($|Q|\geqslant 2$) satisfies to (12) then

$$\mathrm{Aut}(\mathcal{G})\cong\bigotimes_{i=1}^{m}\mathrm{Aut}(\bigotimes_{j=1}^{k_i}(\mathbb{Z}_{p_j^{d_{ij}}},+_{ij})). \tag{16}$$

Besides, for any $i = 1, \dots, m$ (see Theorem 4.1 in [5]) holds the equality

$$|\mathrm{Aut}(\bigotimes_{j=1}^{k_i}(\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}))| = \prod_{j=1}^{k_i}(p_i^{\alpha_{ij}} - p_i^{j-1}) \prod_{j=1}^{k_i}(p_i^{d_{ij}})^{k_i-\alpha_{ij}} \prod_{j=1}^{k_i}(p_i^{d_{ij}})^{k_i-\beta_{ij}+1}, \quad (17)$$

where $\alpha_{ij} = \max\{h | d_{ih} = d_{ij}\}$ and $\beta_{ij} = \min\{h | d_{ih} = d_{ij}\}$ for all $i = 1, \dots, m$ and $j = 1, \dots k_i$. Due to (16) and (17), for any Abelian group $\mathcal{G} = (Q, +)$ ($|Q| \geqslant 2$) that satisfies to (12) holds the equality

$$|\mathrm{Aut}(\mathcal{G})| = \prod_{i=1}^{m}\prod_{j=1}^{k_i}(p_i^{\alpha_{ij}} - p_i^{j-1}) \prod_{j=1}^{k_i}(p_i^{d_{ij}})^{k_i-\alpha_{ij}} \prod_{j=1}^{k_i}(p_i^{d_{ij}})^{k_i-\beta_{ij}+1}. \quad (18)$$

Since $\bigotimes\limits_{j=1}^{k_i} \mathrm{Aut}((\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}))$ is a subgroup of the group $\mathrm{Aut}(\bigotimes\limits_{j=1}^{k_i}(\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}))$, then $\bigotimes\limits_{i=1}^{m}\bigotimes\limits_{j=1}^{k_i} \mathrm{Aut}((\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}))$ is a subgroup of the group $\bigotimes\limits_{i=1}^{m} \mathrm{Aut}(\bigotimes\limits_{j=1}^{k_i}(\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}))$. Besides, $|\mathrm{Aut}((\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}))| = p_i^{d_{ij}}(1 - p_i^{-1})$ $(i = 1, \dots, m;\ \ j = 1, \dots, k_i)$. Hence

$$|\bigotimes_{i=1}^{m}\bigotimes_{j=1}^{k_i} \mathrm{Aut}((\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}))| = |Q| \prod_{i=1}^{m}(1 - p_i^{-1}). \quad (19)$$

By comparing (18) and (19), we conclude that $\bigotimes\limits_{i=1}^{m}\bigotimes\limits_{j=1}^{k_i} \mathrm{Aut}((\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}))$ is a non-trivial subset of the set $\mathrm{Aut}(\mathcal{G})$.

For any $\chi = (\chi_{11}, \dots, \chi_{1k_1}, \dots, \chi_{m1}, \dots, \chi_{mk_m}) \in \bigotimes\limits_{i=1}^{m}\bigotimes\limits_{j=1}^{k_i} \mathrm{Aut}((\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}))$ and $z = (z_{11}, \dots, z_{1k_1}, \dots, z_{m1}, \dots, z_{mk_m}) \in \bigotimes\limits_{i=1}^{m}\bigotimes\limits_{j=1}^{k_i}(\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij})$ we get

$$\chi(z) = (\chi_{11}(z_{11}), \dots, \chi_{1k_1}(z_{1k_1}), \dots, \chi_{m1}(z_{m1}), \dots, \chi_{mk_m}(z_{mk_m})),$$

i.e. computation the vector $\chi(z)$ can be reduced to independent computations of its components. From here it follows that for any Abelian group $\mathcal{G} = (Q, +)$ ($|Q| \geqslant 2$) that satisfies to (12), time and space complexity for computation the element $\chi(z)$ ($z \in \bigotimes\limits_{i=1}^{m}\bigotimes\limits_{j=1}^{k_i}(\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}), \chi \in \bigotimes\limits_{i=1}^{m}\bigotimes\limits_{j=1}^{k_i} \mathrm{Aut}((\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij}))$) are equal, correspondingly, to

$$T_\chi = O(\sum_{i=1}^{m}\sum_{j=1}^{k_i} d_{ij} \log p_i) \quad (|Q| \to \infty), \quad (20)$$

$$V_\chi = O(\sum_{i=1}^{m}\sum_{j=1}^{k_i} d_{ij} \log p_i) \quad (|Q| \to \infty). \quad (21)$$

Remark 4. If computations of components can be implemented in parallel then time complexity for computation the element $\chi(z)$ can be reduced to

$$T_\chi = O(\max_{i=1,\dots m} \max_{j=1,\dots k_i} d_{ij} \log p_i) \quad (|Q| \to \infty). \tag{22}$$

Comparing (13), (14) with (1), (2), and (20), (21) with (3), (4), we conclude that for any Abelian group $\mathcal{G} = (Q, +)$ ($|Q| \geqslant 2$) that satisfies to (12) it is reasonable to consider the set of T-quasigroups

$$\widetilde{\mathfrak{F}}_{\mathcal{G}} = \{(Q, +, \xi, \zeta, c) | \xi, \zeta \in \bigotimes_{i=1}^{m} \bigotimes_{j=1}^{k_i} \mathrm{Aut}((\mathbb{Z}_{p_j^{d_{ij}}}, +_{ij})); c \in Q\}.$$

Due to (18) and (19), $\widetilde{\mathfrak{F}}_{\mathcal{G}}$ is a non-trivial subset of the set $\mathfrak{F}_{\mathcal{G}}$ for any Abelian group $\mathcal{G} = (Q, +)$ ($|Q| \geqslant 2$) that satisfies to (12).

2.3. Elliptic curves over finite fields

At present, Abelian groups associated with elliptic curves over finite fields are widely used for solving information protection problems. This is due to the high complexity of identification the elements of these groups. So, it is it is reasonable to consider the sets of T-quasigroups defined by Abelian groups associated with elliptic curves over finite fields.

We remind, that an elliptic curve γ over any field $\mathbb{F} = (F, +, \cdot)$ can be defined as the set of all solutions of an equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad (a_1, a_2, a_3, a_4, a_6 \in F),$$

such that $\Delta = d_2^2 - 8d_4^3 - 27d_6^2 + 9d_2 d_4 d_6 \neq 0$, where $d_2 = a_1^2 + 4a_2$, $d_4 = 2a_4 + a_1 a_3$, $d_6 = a_3^2 + 4a_6$, and $d_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$. With this elliptic curve can be associated the Abelian group $\mathcal{G}_\gamma = (\gamma \cup \{\mathbf{0}\}, +_{\mathcal{G}_\gamma})$, where $\mathbf{0} +_{\mathcal{G}_\gamma} \mathbf{0} = \mathbf{0}$, $\mathbf{0} +_{\mathcal{G}_\gamma} P = P +_{\mathcal{G}_\gamma} \mathbf{0} = P$ ($P \in \gamma$), and $P = (x, y) \in \gamma \Rightarrow -_{\mathcal{G}_\gamma} P = (x, -y - a_1 x - a_3)$. For any two points $P_i = (x_i, y_i) \in \gamma$ ($i = 1, 2$), such that $P_1 \neq -_{\mathcal{G}_\gamma} P_2$, the point $P_3 = P_1 +_{\mathcal{G}_\gamma} P_2$ can be computed as follows

$$\begin{cases} x_3 = -x_1 - x_2 + \alpha^2 + \alpha a_1 - a_2 \\ y_3 = -y_1 + \alpha(x_1 - x_3) + a_1 x_3 - a_3 \end{cases},$$

where

$$\alpha = \begin{cases} (3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1)(2y_1 + a_1 x_1 + a_3)^{-1}, & if \;\; x_1 = x_2 \\ (y_1 - y_2)(x_1 - x_2)^{-1}, & if \;\; x_1 \neq x_2 \end{cases}.$$

For any non-negative integer m and any element $P \in \gamma \cup \{\mathbf{0}\}$ we set

$$mP = \begin{cases} \mathbf{0}, & if \;\; m = 0 \\ \underbrace{P +_{\mathcal{G}_\gamma} \cdots +_{\mathcal{G}_\gamma} P}_{m \;\; times}, & if \;\; m = 1, 2, \dots \end{cases}.$$

Let γ be an elliptic curve over any finite field $\mathbb{F} = (F, +, \cdot)$.

We define the mappings $\chi_m : \gamma \cup \{\mathbf{0}\} \to \gamma \cup \{\mathbf{0}\}$ $(m = 0, 1, \ldots, |\gamma|)$ by the equality $\chi_m(P) = mP$ $(P \in \gamma \cup \{\mathbf{0}\})$.

It is evident that $\chi_m \in \mathrm{Aut}(\mathcal{G}_\gamma)$ $(m = 1, \ldots, |\gamma|)$ if and only if the integer m is not a multiple of the order of any element $P \in \gamma$. Hence, we can define the set of T-quasigroups $\mathfrak{F}_{\mathcal{G}_\gamma} = \{(\gamma \cup \{\mathbf{0}\}, +_{\mathcal{G}_\gamma}, \xi, \zeta, P) | \xi, \zeta \in \mathrm{Aut}(\mathcal{G}_\gamma), P \in \gamma \cup \{\mathbf{0}\}\}$, and apply to it all results obtained in Subsection 2.2.

3. Families of SA in finite abstract quasigroups

For any abstract finite quasigroup $\mathcal{Q} = (Q, \circ) \in \mathfrak{Q}_Q$ the following families of SA $\mathfrak{A}_\mathcal{Q}^{(i)}$ $(i = 1, \ldots, 22)$ can be defined, at least:

$$\mathfrak{A}_\mathcal{Q}^{(1)} = \{M_{a,b}^{(1)} = (Q, Q, \delta_{a,b}^{(1)}) | \delta_{a,b}^{(1)}(q, x) = (a \circ q) \circ (b \circ x) \ \ (q, x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(2)} = \{M_{a,b}^{(2)} = (Q, Q, \delta_{a,b}^{(2)}) | \delta_{a,b}^{(2)}(q, x) = (b \circ x) \circ (a \circ q) \ \ (q, x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(3)} = \{M_{a,b}^{(3)} = (Q, Q, \delta_{a,b}^{(3)}) | \delta_{a,b}^{(3)}(q, x) = (q \circ a) \circ (b \circ x) \ \ (q, x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(4)} = \{M_{a,b}^{(4)} = (Q, Q, \delta_{a,b}^{(4)}) | \delta_{a,b}^{(4)}(q, x) = (b \circ x) \circ (q \circ a) \ \ (q, x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(5)} = \{M_{a,b}^{(5)} = (Q, Q, \delta_{a,b}^{(5)}) | \delta_{a,b}^{(5)}(q, x) = (a \circ q) \circ (x \circ b) \ \ (q, x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(6)} = \{M_{a,b}^{(6)} = (Q, Q, \delta_{a,b}^{(6)}) | \delta_{a,b}^{(6)}(q, x) = (x \circ b) \circ (a \circ q) \ \ (q, x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(7)} = \{M_{a,b}^{(7)} = (Q, Q, \delta_{a,b}^{(7)}) | \delta_{a,b}^{(7)}(q, x) = (q \circ a) \circ (x \circ b) \ \ (q, x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(8)} = \{M_{a,b}^{(8)} = (Q, Q, \delta_{a,b}^{(8)}) | \delta_{a,b}^{(8)}(q, x) = (x \circ b) \circ (q \circ a) \ \ (q, x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(9)} = \{M_{a}^{(9)} = (Q, Q, \delta_{a}^{(9)}) | \delta_{a}^{(9)}(q, x) = (a \circ q) \circ x \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(10)} = \{M_{a}^{(10)} = (Q, Q, \delta_{a}^{(10)}) | \delta_{a}^{(10)}(q, x) = x \circ (a \circ q) \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(11)} = \{M_{a}^{(11)} = (Q, Q, \delta_{a}^{(11)}) | \delta_{a}^{(11)}(q, x) = (q \circ a) \circ x \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(12)} = \{M_{a}^{(12)} = (Q, Q, \delta_{a}^{(12)}) | \delta_{a}^{(12)}(q, x) = x \circ (q \circ a) \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(13)} = \{M_{a}^{(13)} = (Q, Q, \delta_{a}^{(13)}) | \delta_{a}^{(13)}(q, x) = q \circ (a \circ x) \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(14)} = \{M_{a,b}^{(14)} = (Q, Q, \delta_{a,b}^{(14)}) | \delta_{a}^{(14)}(q, x) = (a \circ x) \circ q \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(15)} = \{M_{a}^{(15)} = (Q, Q, \delta_{a}^{(15)}) | \delta_{a}^{(15)}(q, x) = q \circ (x \circ a) \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(16)} = \{M_{a}^{(16)} = (Q, Q, \delta_{a}^{(16)}) | \delta_{a}^{(15)}(q, x) = (x \circ a) \circ q \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_\mathcal{Q}^{(17)} = \{M_{a}^{(17)} = (Q, Q, \delta_{a}^{(17)}) | \delta_{a}^{(17)}(q, x) = a \circ (q \circ x) \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_{\mathcal{Q}}^{(18)} = \{M_a^{(18)} = (Q, Q, \delta_a^{(17)}) | \delta_a^{(18)}(q, x) = (q \circ x) \circ a \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_{\mathcal{Q}}^{(19)} = \{M_a^{(19)} = (Q, Q, \delta_a^{(19)}) | \delta_a^{(19)}(q, x) = a \circ (x \circ q) \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_{\mathcal{Q}}^{(20)} = \{M_a^{(20)} = (Q, Q, \delta_a^{(20)}) | \delta_a^{(20)}(q, x) = (x \circ q) \circ a \ \ (q, x \in Q)\}_{a \in Q},$$

$$\mathfrak{A}_{\mathcal{Q}}^{(21)} = \{M_a^{(21)} = (Q, Q, \delta_a^{(21)}) | \delta_a^{(21)}(q, x) = q \circ x \ \ (q, x \in Q)\},$$

$$\mathfrak{A}_{\mathcal{Q}}^{(22)} = \{M_a^{(22)} = (Q, Q, \delta_a^{(22)}) | \delta_a^{(22)}(q, x) = x \circ q \ \ (q, x \in Q)\}.$$

It is evident that any family $\mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \ldots, 8)$ consists of $|Q|^2$ elements, any family $\mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 9, \ldots, 20)$ consists of $|Q|$ elements, and any family $\mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 21, 22)$ consists of a single element.

Let $Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})$ $(i = 1, \ldots, 22)$ be the set of all SA that are elements of the family $\mathfrak{A}_{\mathcal{Q}}^{(i)}$. Then $|Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})| = 1$ $(i = 21, 22)$. Besides, since $\mathcal{Q} \in \mathfrak{Q}_Q$ is a cancellative magma, it is not difficult to prove that $|Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})| \geqslant |Q|$ $(i = 1, \ldots, 8)$, and $|Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})| = |Q|$ $(i = 9, \ldots, 20)$, i.e. elements of the family $\mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 9, \ldots, 20)$ are pair-wise different SA.

It follows from definition of the families $\mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \ldots, 22)$ that the following proposition is true.

Proposition 2. *Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any abstract finite quasigroup. Then any SA $M \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \ldots, 8)$ is functioning by 1.5 times more slowly than any SA $M' \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 9, \ldots, 20)$, and three times more slowly than the SA $M'' \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 21, 22)$. Besides, any SA $M' \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 9, \ldots, 20)$ is functioning twice more slowly than the SA $M'' \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 21, 22)$.*

Applying (1) and (2) it is not difficult to prove the following theorem.

Theorem 2. *Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any abstract finite quasigroup. Then for any SA $M \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \ldots, 22)$ time and space complexity for computing the value of the transition mapping are equal, correspondingly, to*

$$T_M = O(|Q| \log |Q|) \ \ (|Q| \to \infty), \tag{23}$$

$$V_M = O(|Q|^2 \log |Q|) \ \ (|Q| \to \infty). \tag{24}$$

Any abstract finite quasigroup $\mathcal{Q} \in \mathfrak{Q}_Q$ is a cancellative magma. Hence, the diagram of any SA $M \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \ldots, 22)$ is completed labeled directed graph with a single loop in each vertex, such that for any vertex $q \in Q$, all $|Q|$ arcs started in q terminate in pair-wise different vertices, and exactly $|Q|$ arcs are terminated in q and labels of these arcs are pair-wise different. From here we get that Theorem 1 is true for any SA $M \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \ldots, 22)$, and it can be reformulated as follows.

Theorem 3. *Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any be any abstract finite quasigroup. Then for any SA $M \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \dots, 22)$ hold equalities:*

$$P_{M,q,m}^{(1)}(q') = |Q|^{-1} \quad (q, q' \in Q;\ m = 1, 2, \dots), \tag{25}$$

$$P_{M,q,m}^{(2)} = |Q|^{-1}(1 - (|Q| - 1)(|Q|^m - 1)^{-1}) \quad (q \in Q;\ m = 1, 2, \dots). \tag{26}$$

Due to Theorems 2 and 3, we can consider $\mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \dots, 22)$ as basic families of SA defined by a recurrence relation in an abstract finite quasigroup $\mathcal{Q} \in \mathfrak{Q}_Q$.

Let us characterize the structure of the families $\mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \dots, 22)$ with additional restrictions on the operation in an abstract finite quasigroup $\mathcal{Q} \in \mathfrak{Q}_Q$.

Based on the definition of the left unit, the right unit and the unit in a quasigroup, it is not difficult to prove the following three propositions.

Proposition 3. *Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any abstract finite quasigroup with the left unit. Then the following inclusions hold:*

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(1)})\ (i = 9, 13, 21), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(2)})\ (i = 10, 14, 22),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(11)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(3)}), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(12)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(4)}), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(15)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(5)}),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(16)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(6)}), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(21)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})\ (i = 9, 13, 17),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(22)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})\ (i = 10, 14, 19).$$

Proposition 4. *Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any abstract finite quasigroup with the right unit. Then the following inclusions hold:*

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(7)})\ (i = 11, 15, 21), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(8)})\ (i = 12, 16, 22),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(13)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(3)}), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(14)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(4)}), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(9)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(5)}),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(10)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(6)}), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(21)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})\ (i = 11, 15, 18),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(22)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})\ (i = 12, 16, 20).$$

Proposition 5. *Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any abstract finite loop. Then the following inclusions hold:*

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(1)})\ (i = 9, 13, 21), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(2)})\ (i = 10, 14, 22),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(3)})\ (i = 11, 13, 21), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(4)})\ (i = 12, 14, 22),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(5)})\ (i = 9, 15, 21), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(6)})\ (i = 12, 14, 22),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(7)})\ (i = 11, 15, 21), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(8)})\ (i = 12, 16, 22),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(21)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})\ (i = 9, 11, 13, 15, 17, 18),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(22)}) \subseteq Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})\ (i = 10, 12, 14, 16, 19, 20).$$

Proceeding from definitions of associative and/or commutative magma, it is not difficult to prove the following three propositions.

Proposition 6. *Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any finite associative quasigroup. Then the following equalities hold:*

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(9)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(17)}), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(10)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(16)}), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(11)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(13)}),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(12)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(20)}), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(14)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(19)}), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(15)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(18)}).$$

Proposition 7. *Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any finite commutative quasigroup. Then the following equalities hold:*

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(j)}) \ (i,j = 1,\dots,8), \qquad Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(j)}) \ (i,j = 9,\dots,12),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(j)}) \ (i,j = 13,\dots,16), \ Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(j)}) \ (i,j = 17,\dots,20),$$

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(j)}) \ (i,j = 21,22).$$

Proposition 8. *Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any finite associative-commutative quasigroup. Then the following equalities hold:*

$$Set(\mathfrak{A}_{\mathcal{Q}}^{(i)}) = Set(\mathfrak{A}_{\mathcal{Q}}^{(17)}) \ (i = 1,\dots,16,18,19,20).$$

It should be noted, that if $\mathcal{Q} \in \mathfrak{Q}_Q$ is a finite associative-commutative quasigroup, then for all elements $a,b \in Q$ any SA $M_{a,b}^{(i)} \in Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})$ $(i = 1,\dots,8)$ appears as an element of the family $Set(\mathfrak{A}_{\mathcal{Q}}^{(i)})$ $(i = 9,\dots,20)$ exactly $|Q|$ times.

4. Families of SA in finite T-quasigroups

Let $\mathcal{G} = (Q,+)$ $(|Q| \geqslant 2)$ be given Abelian group.

For any T-quasigroup $\mathcal{Q} = (Q,\circ) = (Q,+,\xi,\zeta,c) \in \mathfrak{F}_{\mathcal{G}}$, applying (11), we can redefine the families of SA $\mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1,\dots,22)$ as follows:

$$\mathfrak{A}_{(Q,+,\xi,\zeta,c)}^{(1)} = \{M_{a,b,c,\xi,\zeta}^{(1)} = (Q,Q,\delta_{a,b,c,\xi,\zeta}^{(1)}) | \delta_{a,b,c,\xi,\zeta}^{(1)}(q,x) =$$

$$= \xi\zeta(q) + \zeta^2(x) + \xi^2(a) + \zeta\xi(b) + \xi(c) + \zeta(c) + c \ \ (q,x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}_{(Q,+,\xi,\zeta,c)}^{(2)} = \{M_{a,b,c,\xi,\zeta}^{(2)} = (Q,Q,\delta_{a,b,c,\xi,\zeta}^{(2)}) | \delta_{a,b,c,\xi,\zeta}^{(2)}(q,x) =$$

$$= \zeta^2(q) + \xi\zeta(x) + \zeta\xi(a) + \xi^2(b) + \xi(c) + \zeta(c) + c \ \ (q,x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}_{(Q,+,\xi,\zeta,c)}^{(3)} = \{M_{a,b,c,\xi,\zeta}^{(3)} = (Q,Q,\delta_{a,b,c,\xi,\zeta}^{(3)}) | \delta_{a,b,c,\xi,\zeta}^{(3)}(q,x) =$$

$$= \xi^2(q) + \zeta^2(x) + \xi\zeta(a) + \zeta\xi(b) + \xi(c) + \zeta(c) + c \ \ (q,x \in Q)\}_{a,b \in Q},$$

$$\mathfrak{A}^{(4)}_{(Q,+,\xi,\zeta,c)} = \{M^{(4)}_{a,b,c,\xi,\zeta} = (Q,Q,\delta^{(4)}_{a,b,c,\xi,\zeta})|\delta^{(4)}_{a,b,c,\xi,\zeta}(q,x) =$$
$$= \zeta\xi(q) + \xi\zeta(x) + \zeta^2(a) + \xi^2(b) + \xi(c) + \zeta(c) + c \ \ (q,x \in Q)\}_{a,b\in Q},$$
$$\mathfrak{A}^{(5)}_{(Q,+,\xi,\zeta,c)} = \{M^{(5)}_{a,b,c,\xi,\zeta} = (Q,Q,\delta^{(5)}_{a,b,c,\xi,\zeta})|\delta^{(5)}_{a,b,c,\xi,\zeta}(q,x) =$$
$$= \xi\zeta(q) + \zeta\xi(x) + \xi^2(a) + \zeta^2(b) + \xi(c) + \zeta(c) + c \ \ (q,x \in Q)\}_{a,b\in Q},$$
$$\mathfrak{A}^{(6)}_{(Q,+,\xi,\zeta,c)} = \{M^{(6)}_{a,b,c,\xi,\zeta} = (Q,Q,\delta^{(6)}_{a,b,c,\xi,\zeta})|\delta^{(6)}_{a,b,c,\xi,\zeta}(q,x) =$$
$$= \zeta^2(q) + \xi^2(x) + \zeta\xi(a) + \xi\zeta(b) + \xi(c) + \zeta(c) + c \ \ (q,x \in Q)\}_{a,b\in Q},$$
$$\mathfrak{A}^{(7)}_{(Q,+,\xi,\zeta,c)} = \{M^{(7)}_{a,b,c,\xi,\zeta} = (Q,Q,\delta^{(7)}_{a,b,c,\xi,\zeta})|\delta^{(7)}_{a,b,c,\xi,\zeta}(q,x) =$$
$$= \xi^2(q) + \zeta\xi(x) + \xi\zeta(a) + \zeta^2(b) + \xi(c) + \zeta(c) + c \ \ (q,x \in Q)\}_{a,b\in Q},$$
$$\mathfrak{A}^{(8)}_{(Q,+,\xi,\zeta,c)} = \{M^{(8)}_{a,b,c,\xi,\zeta} = (Q,Q,\delta^{(8)}_{a,b,c,\xi,\zeta})|\delta^{(8)}_{a,b,c,\xi,\zeta}(q,x) =$$
$$= \zeta\xi(q) + \xi^2(x) + \zeta^2(a) + \xi\zeta(b) + \xi(c) + \zeta(c) + c \ \ (q,x \in Q)\}_{a,b\in Q},$$
$$\mathfrak{A}^{(9)}_{(Q,+,\xi,\zeta,c)} = \{M^{(9)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(9)}_{a,c,\xi,\zeta})|\delta^{(9)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \xi\zeta(q) + \zeta(x) + \xi^2(a) + \xi(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(10)}_{(Q,+,\xi,\zeta,c)} = \{M^{(10)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(10)}_{a,c,\xi,\zeta})|\delta^{(10)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \zeta^2(q) + \xi(x) + \zeta\xi(a) + \zeta(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(11)}_{(Q,+,\xi,\zeta,c)} = \{M^{(11)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(11)}_{a,c,\xi,\zeta})|\delta^{(11)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \xi^2(q) + \zeta(x) + \xi\zeta(a) + \xi(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(12)}_{(Q,+,\xi,\zeta,c)} = \{M^{(12)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(12)}_{a,c,\xi,\zeta})|\delta^{(12)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \zeta\xi(q) + \xi(x) + \zeta^2(a) + \zeta(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(13)}_{(Q,+,\xi,\zeta,c)} = \{M^{(13)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(13)}_{a,c,\xi,\zeta})|\delta^{(13)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \xi(q) + \zeta^2(x) + \zeta\xi(a) + \zeta(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(14)}_{(Q,+,\xi,\zeta,c)} = \{M^{(14)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(14)}_{a,c,\xi,\zeta})|\delta^{(14)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \zeta(q) + \xi\zeta(x) + \xi^2(a) + \xi(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(15)}_{(Q,+,\xi,\zeta,c)} = \{M^{(15)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(15)}_{a,c,\xi,\zeta})|\delta^{(15)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \xi(q) + \zeta\xi(x) + \zeta^2(a) + \zeta(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(16)}_{(Q,+,\xi,\zeta,c)} = \{M^{(16)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(16)}_{a,c,\xi,\zeta})|\delta^{(16)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \zeta(q) + \xi^2(x) + \xi\zeta(a) + \xi(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$

$$\mathfrak{A}^{(17)}_{(Q,+,\xi,\zeta,c)} = \{M^{(17)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(17)}_{a,c,\xi,\zeta}) | \delta^{(17)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \zeta\xi(q) + \zeta^2(x) + \xi(a) + \zeta(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(18)}_{(Q,+,\xi,\zeta,c)} = \{M^{(18)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(18)}_{a,c,\xi,\zeta}) | \delta^{(18)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \xi^2(q) + \xi\zeta(x) + \zeta(a) + \xi(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(19)}_{(Q,+,\xi,\zeta,c)} = \{M^{(19)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(19)}_{a,c,\xi,\zeta}) | \delta^{(19)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \zeta^2(q) + \zeta\xi(x) + \xi(a) + \zeta(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(20)}_{(Q,+,\xi,\zeta,c)} = \{M^{(20)}_{a,c,\xi,\zeta} = (Q,Q,\delta^{(20)}_{a,c,\xi,\zeta}) | \delta^{(20)}_{a,c,\xi,\zeta}(q,x) =$$
$$= \xi\zeta(q) + \xi^2(x) + \zeta(a) + \xi(c) + c \ \ (q,x \in Q)\}_{a\in Q},$$
$$\mathfrak{A}^{(21)}_{(Q,+,\xi,\zeta,c)} = \{M^{(21)}_{c,\xi,\zeta} = (Q,Q,\delta^{(21)}_{c,\xi,\zeta}) | \delta^{(21)}_{c,\xi,\zeta}(q,x) = \xi(q) + \zeta(x) + c \ \ (q,x \in Q)\},$$
$$\mathfrak{A}^{(22)}_{(Q,+,\xi,\zeta,c)} = \{M^{(22)}_{c,\xi,\zeta} = (Q,Q,\delta^{(22)}_{c,\xi,\zeta}) | \delta^{(22)}_{c,\xi,\zeta}(q,x) = \zeta(q) + \xi(x) + c \ \ (q,x \in Q)\}.$$

It is evident that for any family of SA $\mathfrak{A}^{(i)}_{(Q,+,\xi,\zeta,c)}$ $(i = 1,\dots,22)$ all results obtained in Section 3 are true. Moreover, due to Remark 2, for T-quasigroups, Proposition 8 is the strongest one among Propositions 5, 6, and 8. Therefore, for a T-quasigroup $(Q,+,\xi,\zeta,c) \in \mathfrak{F}_{\mathcal{G}}$ with additional restrictions on the operation in it (see subsection 2.2), Propositions 3, 4, 7, and 8 can be reformulated as follows:

In Proposition 3, the phrase "Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any abstract finite quasigroup with the left unit" can be replaced by "Let $\mathcal{G} = (Q,+)$ $(|Q| \geqslant 2)$ be any finite Abelian group, and $(Q,+,\xi,\varepsilon_Q,c) \in \mathfrak{F}_{\mathcal{G}}$ be any T-quasigroup with the left unit". Besides, in all inclusions the symbol $\mathcal{Q}$ can be replaced by $(Q,+,\xi,\varepsilon_Q,c)$.

In Proposition 4, the phrase "Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any abstract finite quasigroup with the right unit" can be replaced by "Let $\mathcal{G} = (Q,+)$ $(|Q| \geqslant 2)$ be any finite Abelian group, and $(Q,+,\xi,\varepsilon_Q,c) \in \mathfrak{F}_{\mathcal{G}}$ be any T-quasigroup with the right unit". Besides, in all inclusions the symbol $\mathcal{Q}$ can be replaced by $(Q,+,\xi,\varepsilon_Q,c)$.

In Proposition 7, the phrase "Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any abstract finite commutative quasigroup" can be replaced by "Let $\mathcal{G} = (Q,+)$ $(|Q| \geqslant 2)$ be any finite Abelian group, and $(Q,+,\xi,\varepsilon_Q,c) \in \mathfrak{F}_{\mathcal{G}}$ be any commutative T-quasigroup". Besides, in all inclusions the symbol $\mathcal{Q}$ can be replaced by $(Q,+,\xi,\varepsilon_Q,c)$.

In Proposition 8, the phrase "Let $\mathcal{Q} \in \mathfrak{Q}_Q$ be any abstract finite loop" can be replaced by "Let $\mathcal{G} = (Q,+)$ $(|Q| \geqslant 2)$ be any finite Abelian group, and $(Q,+,\xi,\varepsilon_Q,c) \in \mathfrak{F}_{\mathcal{G}}$ be any loop". Besides, in all inclusions the symbol $\mathcal{Q}$ can be replaced by $(Q,+,\xi,\varepsilon_Q,c)$.

Fundamental theorem for finite Abelian groups (see Subsection 2.2) makes it possible to represent SA $M \in \mathfrak{A}^{(i)}_{(Q,+,\xi,\zeta,c)}$ $(i = 1,\dots,22)$ by the parallel composition of SA over T-quasigroups determined by cyclic groups of prime-power order.

Remark 5. The parallel composition of SA $M_i = (Q_i, X_i, \delta_i)$ $(i = 1, \ldots, n)$ is the SA $\bigotimes\limits_{i=1}^{n} M_i = (\bigotimes\limits_{i=1}^{n} Q_i, \bigotimes\limits_{i=1}^{n} X_i, \delta)$, where

$$\delta((q_1, \ldots, q_n), (x_1, \ldots, x_n)) = (\delta_1(q_1, x_1), \ldots, \delta_n(q_n, x_n))$$

for all $(q_1, \ldots, q_n) \in \bigotimes\limits_{i=1}^{n} Q_i$ and $(x_1, \ldots, x_n) \in \bigotimes\limits_{i=1}^{n} X_i$.

Indeed, let $\mathcal{G} = (Q, +)$ $(|Q| \geqslant 2)$ be an Abelian group that satisfies to (12), and $(Q, +, \xi, \zeta, c) \in \widetilde{\mathfrak{F}}_{\mathcal{G}}$. Setting

$$a = (a_{11}, \ldots, a_{1k_1}, \ldots, a_{m1}, \ldots, a_{mk_m}), \quad b = (b_{11}, \ldots, b_{1k_1}, \ldots, b_{m1}, \ldots, b_{mk_m}),$$

$$\xi = (\xi_{11}, \ldots, \xi_{1k_1}, \ldots, \xi_{m1}, \ldots, \xi_{mk_m}), \quad \zeta = (\zeta_{11}, \ldots, \zeta_{1k_1}, \ldots, \zeta_{m1}, \ldots, \zeta_{mk_m}),$$

$$c = (c_{11}, \ldots, c_{1k_1}, \ldots, c_{m1}, \ldots, c_{mk_m}),$$

we get the following representations of SA $M \in \mathfrak{A}^{(i)}_{(Q,+,\xi,\zeta,c)}$ $(i = 1, \ldots, 22)$ by the parallel composition of SA over cyclic groups of prime-power order:

1. If $M^{(i)}_{a,b,c,\xi,\zeta} \in \mathfrak{A}^{(i)}_{(Q,+,\xi,\zeta,c)}$ $(i = 1, \ldots, 8)$ then

$$M^{(i)}_{a,b,c,\xi,\zeta} \cong \bigotimes_{j=1}^{m} \bigotimes_{h=1}^{k_j} M^{(i)}_{a_{jh},b_{jh},c_{jh},\xi_{jh},\zeta_{jh}}. \tag{27}$$

2. If $M^{(i)}_{a,c,\xi,\zeta} \in \mathfrak{A}^{(i)}_{(Q,+,\xi,\zeta,c)}$ $(i = 9, \ldots, 20)$ then

$$M^{(i)}_{a,c,\xi,\zeta} \cong \bigotimes_{j=1}^{m} \bigotimes_{h=1}^{k_j} M^{(i)}_{a_{jh},c_{jh},\xi_{jh},\zeta_{jh}}. \tag{28}$$

3. If $M^{(i)}_{c,\xi,\zeta} \in \mathfrak{A}^{(i)}_{(Q,+,\xi,\zeta,c)}$ $(i = 21, 22)$ then

$$M^{(i)}_{c,\xi,\zeta} \cong \bigotimes_{j=1}^{m} \bigotimes_{h=1}^{k_j} M^{(i)}_{c_{jh},\xi_{jh},\zeta_{jh}}. \tag{29}$$

Applying (13), (14), (20) and (21) to the representations (27)-(29), the following theorem can be proved.

Theorem 4. *Let $\mathcal{G} = (Q, +)$ $(|Q| \geqslant 2)$ be an Abelian group that satisfies to (12), and $(Q, +, \xi, \zeta, c) \in \widetilde{\mathfrak{F}}_{\mathcal{G}}$. Then for any SA $M \in \mathfrak{A}^{(i)}_{(Q,+,\xi,\zeta,c)}$ $(i = 1, \ldots, 22)$ time and space complexity for computation the value of the transition mapping are equal, correspondingly, to*

$$T_M = O(\sum_{i=1}^{m} \sum_{j=1}^{k_i} d_{ij} \log p_i) \quad (|Q| \to \infty), \tag{30}$$

$$V_M = O(\sum_{i=1}^{m}\sum_{j=1}^{k_i} d_{ij}\log p_i) \quad (|Q|\to\infty). \tag{31}$$

Remark 6. If computations of transition mappings for components in the parallel composition of SA $M \in \mathfrak{A}^{(i)}_{(Q,+,\xi,\zeta,c)}$ $(i = 1,\dots,22)$ can be implemented in parallel, then, due to (15) and (22), for SA M time complexity for computation the value of the transition mapping can be reduced to

$$T_M = O(\max_{i=1,\dots m}\max_{j=1,\dots k_i} d_{ij}\log p_i) \quad (|Q|\to\infty). \tag{32}$$

By comparing (30), (31) with (23), (24), we conclude that for any T-quasigroup $(Q,+,\xi,\zeta,c) \in \widetilde{\mathfrak{F}}_{\mathcal{G}}$ it is reasonable to use SA $M \in \mathfrak{A}^{(i)}_{(Q,+,\xi,\zeta,c)}$ $(i = 1,\dots,22)$ as mathematical models for the families of fast iterated hash functions.

5. Families of SA in elliptic curves over finite fields

Let γ be any elliptic curve over a finite field, and $(\gamma\cup\{\mathbf{0}\}, +_{\mathcal{G}_\gamma}, \chi_{m_1}, \chi_{m_2}, P) \in \mathfrak{F}_{\mathcal{G}_\gamma}$ be any T-quasigroup. To transform the families $\mathfrak{A}^{(i)}_{(Q,+,\xi,\zeta,c)}$ $(i = 1,\dots,22)$ into the families $\mathfrak{A}^{(i)}_{(\gamma\cup\{\mathbf{0}\},+_{\mathcal{G}_\gamma},\chi_{m_1},\chi_{m_2},c)}$ it is sufficient to substitute:

1) $\gamma\cup\{\mathbf{0}\}$ instead of Q;
2) $P_1, P_2, P \in \gamma$, correspondingly, instead of $a, b, c \in Q$;
3) $\chi_{m_1}, \chi_{m_2} \in \mathrm{Aut}(\mathcal{G}_\gamma)$, correspondingly, instead of $\xi, \zeta \in \mathrm{Aut}(\mathcal{G})$;
4) $+_{\mathcal{G}_\gamma}$ instead of $+$.

It is evident that for the families of SA $\mathfrak{A}^{(i)}_{(\gamma\cup\{\mathbf{0}\},+_{\mathcal{G}_\gamma},\chi_{m_1},\chi_{m_2},c)}$ $(i = 1,\dots,22)$ all results obtained in Section 4 are true. Hence, $\mathfrak{A}^{(i)}_{(\gamma\cup\{\mathbf{0}\},+_{\mathcal{G}_\gamma},\chi_{m_1},\chi_{m_2},c)}$ $(i = 1,\dots,22)$ can be considered as basic families of SA defined by a recurrence relation in a T-quasigroup $(\gamma\cup\{\mathbf{0}\}, +_{\mathcal{G}_\gamma}, \chi_{m_1}, \chi_{m_2}, P) \in \mathfrak{F}_{\mathcal{G}_\gamma}$.

The following another approach to definition families of SA in an elliptic curve γ over a finite field has been proposed in [22].

Let $\mathcal{F}_\gamma = \{\chi_m | m = 1,\dots,|\gamma|\}$. For any fixed integer $l \in \{1,\dots,|\gamma|\}$ we can define the family of SA

$$\mathfrak{A}_{\gamma,l} = \{M_{\chi_m,P} = (\gamma\cup\{\mathbf{0}\}, \mathbb{Z}_{l+1}, \delta_{\chi_m,P})\}_{\chi_m\in\mathcal{F}_\gamma, P\in\gamma},$$

where

$$\delta_{\chi_m,P}(q,x) = \chi_m(q) +_{\mathcal{G}_\gamma} \chi_x(P) \quad (q \in \gamma\cup\{\mathbf{0}\}, x \in \mathbb{Z}_{l+1}). \tag{33}$$

Let $Ordr(P)$ be the order of the element P in the Abelian group $\mathcal{G}_\gamma$.

Theorem 5. *Let γ be any elliptic curve over a finite field, $l \in \{1,\dots,|\gamma|\}$ be any fixed integer, and $M_{\chi_m,P} = (\gamma\cup\{\boldsymbol{0}\}, \mathbb{Z}_{l+1}, \delta_{\chi_m,P}) \in \mathfrak{A}_{\gamma,l}$ be any SA. Then for any state $q \in \gamma\cup\{\boldsymbol{0}\}$ and any two different input symbols $x_1, x_2 \in \mathbb{Z}_{l+1}$ the inequality $\delta_{\chi_m,P}(q,x_1) \neq \delta_{\chi_m,P}(q,x_2)$ holds if and only if $Ordr(P) > l$.*

Proof. Suppose that there exists an SA $M_{\chi_m,P} = (\gamma \cup \{\mathbf{0}\}, \mathbb{Z}_{l+1}, \delta_{\chi_m,P}) \in \mathfrak{A}_{\gamma,l}$ such that $Ordr(P) > l$, and for some state $q \in \gamma \cup \{\mathbf{0}\}$ and some two different input symbols $x_1, x_2 \in \mathbb{Z}_{l+1}$ holds the equality $\delta_{\chi_m,P}(q, x_1) = \delta_{\chi_m,P}(q, x_2)$.

Due to (33), we get

$$(\exists q \in \gamma \cup \{\mathbf{0}\})(\exists x_1, x_2 \in \mathbb{Z}_{l+1})(x_1 \neq x_2 \& \delta_{\chi_m,P}(q, x_1) = \delta_{\chi_m,P}(q, x_2)) \Leftrightarrow$$

$$\Leftrightarrow (\exists q \in \gamma \cup \{\mathbf{0}\})(\exists x_1, x_2 \in \mathbb{Z}_{l+1})(x_1 \neq x_2 \& \chi_m(q) +_{\mathcal{G}_\gamma} \chi_{x_1}(P) =$$

$$= \chi_m(q) +_{\mathcal{G}_\gamma} \chi_{x_2}(P)) \Leftrightarrow (\exists x_1, x_2 \in \mathbb{Z}_{l+1})(x_1 \neq x_2 \& \chi_{x_1}(P) = \chi_{x_2}(P)) \Leftrightarrow$$

$$\Leftrightarrow (\exists x_1, x_2 \in \mathbb{Z}_{l+1})(x_1 \neq x_2 \& x_1 P = x_2 P) \Leftrightarrow$$

$$\Leftrightarrow (\exists x_1, x_2 \in \mathbb{Z}_{l+1})(x_1 \neq x_2 \& (\max\{x_1, x_2\} - \min\{x_1, x_2\})P = \mathbf{0}) \Leftrightarrow$$

$$\Leftrightarrow (\exists x \in \{1, \ldots, l\})(xP = \mathbf{0}) \Leftrightarrow Ordr(P) \leqslant l.$$

We get a contradiction, since, by supposition, $Ordr(P) > l$.

Therefore, $M_{\chi_m,P} = (\gamma \cup \{\mathbf{0}\}, \mathbb{Z}_{l+1}, \delta_{\chi_m,P}) \in \mathfrak{A}_{\gamma,l}$ is an SA such that for any state $q \in \gamma \cup \{\mathbf{0}\}$ and any two different input symbols $x_1, x_2 \in \mathbb{Z}_{l+1}$ the inequality $\delta_{\chi_m,P}(q, x_1) \neq \delta_{\chi_m,P}(q, x_2)$ holds if and only if $Ordr(P) > l$. □

From proof of Theorem 5 we get that the following corollary is true.

Corollary 1. *Let γ be any elliptic curve over a finite field, $l \in \{1, \ldots, |\gamma|\}$ be any fixed integer, and $M_{\chi_m,P} = (\gamma \cup \{\boldsymbol{0}\}, \mathbb{Z}_{l+1}, \delta_{\chi_m,P}) \in \mathfrak{A}_{\gamma,l}$ be any SA such that $Ordr(P) \leqslant l$. Then for any state $q \in \gamma \cup \{\boldsymbol{0}\}$ and for all two different input symbols $x_1, x_2 \in \mathbb{Z}_{l+1}$ such that the integer $\max\{x_1, x_2\} - \min\{x_1, x_2\}$ is some multiple of the integer $Ordr(P)$ holds the equality $\delta_{\chi_m,P}(q, x_1) = \delta_{\chi_m,P}(q, x_2)$.*

Theorem 6. *Let γ be any elliptic curve over a finite field, $l \in \{1, \ldots, |\gamma|\}$ be any fixed integer, and $M_{\chi_m,P} = (\gamma \cup \{\boldsymbol{0}\}, \mathbb{Z}_{l+1}, \delta_{\chi_m,P}) \in \mathfrak{A}_{\gamma,l}$ be any SA. Then for any two different states $q_1, q_2 \in \gamma \cup \{\boldsymbol{0}\}$ and any input symbol $x \in \mathbb{Z}_{l+1}$ the inequality $\delta_{\chi_m,P}(q_1, x) \neq \delta_{\chi_m,P}(q_2, x)$ holds if and only if $\chi_m \in Aut(\mathcal{G}_\gamma)$.*

Proof. Suppose that there exists an SA $M_{\chi_m,P} = (\gamma \cup \{\mathbf{0}\}, \mathbb{Z}_{l+1}, \delta_{\chi_m,P}) \in \mathfrak{A}_{\gamma,l}$ such that $\chi_m \in \mathrm{Aut}(\mathcal{G}_\gamma)$, and for some two different states $q_1, q_2 \in \gamma \cup \{\mathbf{0}\}$ and some input symbol $x \in \mathbb{Z}_{l+1}$ holds the equality $\delta_{\chi_m,P}(q_1, x) = \delta_{\chi_m,P}(q_2, x)$.

Due to (33), we get

$$(\exists q_1, q_2 \in \gamma \cup \{\mathbf{0}\})(\exists x \in \mathbb{Z}_{l+1})(q_1 \neq q_2 \& \delta_{\chi_m,P}(q_1, x) = \delta_{\chi_m,P}(q_2, x)) \Leftrightarrow$$

$$\Leftrightarrow (\exists q_1, q_2 \in \gamma \cup \{\mathbf{0}\})(\exists x \in \mathbb{Z}_{l+1})(q_1 \neq q_2 \& \chi_m(q_1) +_{\mathcal{G}_\gamma} \chi_x(P) =$$

$$= \chi_m(q_2) +_{\mathcal{G}_\gamma} \chi_x(P)) \Leftrightarrow (\exists q_1, q_2 \in \gamma \cup \{\mathbf{0}\})(q_1 \neq q_2 \& \chi_m(q_1) = \chi_m(q_2)) \Leftrightarrow$$

$$\Leftrightarrow (\exists q_1, q_2 \in \gamma \cup \{\mathbf{0}\})(q_1 \neq q_2 \& mq_1 = mq_2 P) \Leftrightarrow$$

$$\Leftrightarrow (\exists q_1, q_2 \in \gamma \cup \{\mathbf{0}\})(q_1 \neq q_2 \& m(q_1 -_{\mathcal{G}_\gamma} q_2) = \mathbf{0}) \Leftrightarrow$$

$$\Leftrightarrow (\exists q \in \gamma)(mq = \mathbf{0}) \Leftrightarrow (\exists q \in \gamma)(\chi_m(q) = \mathbf{0}) \Leftrightarrow \chi_m \notin \mathrm{Aut}(\mathcal{G}_\gamma).$$

We get a contradiction, since, by supposition, $\chi_m \in \mathrm{Aut}(\mathcal{G}_\gamma)$.

Therefore, $M_{\chi_m,P} = (\gamma \cup \{\mathbf{0}\}, \mathbb{Z}_{l+1}, \delta_{\chi_m,P}) \in \mathfrak{A}_{\gamma,l}$ is an SA such that for any two different states $q_1, q_2 \in \gamma \cup \{\mathbf{0}\}$ and any input symbol $x \in \mathbb{Z}_{l+1}$ the inequality $\delta_{\chi_m,P}(q_1, x) \neq \delta_{\chi_m,P}(q_2, x)$ holds if and only if $\chi_m \in \mathrm{Aut}(\mathcal{G}_\gamma)$. □

From proof of Theorem 6 we get that the following corollary is true.

Corollary 2. *Let γ be any elliptic curve over a finite field, $l \in \{1, \ldots, |\gamma|\}$ be any fixed integer, and $M_{\chi_m,P} = (\gamma \cup \{\boldsymbol{0}\}, \mathbb{Z}_{l+1}, \delta_{\chi_m,P}) \in \mathfrak{A}_{\gamma,l}$ be any SA such that $\chi_m \in \mathcal{F}_\gamma \backslash Aut(\mathcal{G}_\gamma)$. Then for all two different states $q_1, q_2 \in \gamma \cup \{\boldsymbol{0}\}$ such that the integer m is some multiple of the integer $Order(q_1 -_{\mathcal{G}_\gamma} q_2)$ any for any input symbol $x \in \mathbb{Z}_{l+1}$ holds the equality $\delta_{\chi_m,P}(q_1, x) = \delta_{\chi_m,P}(q_2, x)$.*

Due to Theorems 5 and 6, and Corollaries 1 and 2, it seems promising to use SA $M_{\chi_m,P} \in \mathfrak{A}_{\gamma,l}$ ($\chi_m \in \mathcal{F}_\gamma, P \in \gamma, Ordr(P) > l$) and SA $M_{\chi_m,P} \in \mathfrak{A}_{\gamma,l}$ ($\chi_m \in \mathrm{Aut}(\mathcal{G}_\gamma), P \in \gamma$) as mathematical models for the design and implementation of computationally secured families of iterated hash functions.

6. Discussion

The main aim of the given paper was to explore the feasibility to use SA defined by a reccurence relation in a finite quasigroup as mathematical models for computationally secure families of iterated hash functions.

Basic families of SA defined by a recurrence relation in an abstract finite quasigroup $\mathcal{Q} \in \mathfrak{Q}_Q$ have been introduced and examined in Section 3. The main results of these studies are presented in Theorem 1. Their significance is that from a probabilistic point of view SA $M \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ ($i = 1, \ldots, 22$) are the best in the class of SA mathematical models for computationally secure sets $\mathfrak{H}_M = \{H_{(M,q)} | q \in Q\}$ of iterated hash functions.

It is known that solving equations in a quasigroup $\mathcal{Q} \in \mathfrak{Q}_Q$ is a hard Problem when $|Q|$ is sufficiently large integer. Let the initial state $q \in Q$ of a SA $M \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ ($i = 1, \ldots, 22$) and the length l of the hashed input string $w \in Q^l$ be some part of the short-term secret key. Suppose that an intruder have intercepted the hash q', and his aim is to find the hashed input string $w \in Q^l$. Therefore, he is faced with the family of equations $H_{(M,q)}(w) = q'$ in a situation, when the integer l is unknown to him. In the absence of additional information this Problem cannot be solved at all. Even if the integer l is known to an intruder, then, due to Theorem 1, any searching based either on deterministic or probabilistic approach does not guarantee identification of the hashed input string w in the admissible time. Due to Theorem 1, the similar situation arises if an intruder tries to change the hashed message. The values of the parameters of SA $M \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ ($i = 1, \ldots, 20$) can be considered as some part of the medium-term secret key. In this case, when an intruder tries to find the hashed input string, he must additionally identify the

SA $M \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$. Besides, some algorithm that determines the selection of the family $\mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \ldots, 22)$ can be designed as the long-term secret key.

Any abstract quasigroup $\mathcal{Q} \in \mathfrak{Q}_Q$ is specified by the Cayley table, as a rule. Hence, any SA $M \in \mathfrak{A}_{\mathcal{Q}}^{(i)}$ $(i = 1, \ldots, 22)$ has a sufficiently high time and space complexity (see Theorem 2). It seems promising to define similar families of SA for some set of quasigroups that can be specified compactly and operations in which are fast. The set of all T-quasigroups defined by a given finite Abelian group $\mathcal{G} = (Q, +)$ meets these conditions. In Sections 4 the families of SA $\mathfrak{A}_{(Q,+,\xi,\zeta,c)}^{(i)}$ $(i = 1, \ldots, 22)$ defined in these T-quasigroups have been investigated. The representation of SA $M \in \mathfrak{A}_{(Q,+,\xi,\zeta,c)}^{(i)}$ $(i = 1, \ldots, 22)$ by the parallel composition of SA over T-quasigroups determined by cyclic groups of prime-power order reduces its time and space complexity (see Theorem 4 and Remark 6). Investigation of the families $\mathfrak{A}_{(Q,+,\xi,\zeta,c)}^{(i)}$ $(i = 1, \ldots, 22)$ for specific Abelian groups $\mathcal{G} = (Q, +)$ $(|Q| \geqslant 2)$ can help to find the most suitable families of SA for mathematical models of fast computationally secure families of iterated hash functions.

It is known, that elliptic curves over finite fields can be successfully used for solving information protection problems. In Section 5 it has been shown how the families $\mathfrak{A}_{(Q,+,\xi,\zeta,c)}^{(i)}$ $(i = 1, \ldots, 22)$ can be transformed into the families $\mathfrak{A}_{(\gamma\cup\{\mathbf{0}\},+_{\mathcal{G}_\gamma},\chi_{m_1},\chi_{m_2},c)}^{(i)}$, where γ is an elliptic curve over a finite field, and $\mathcal{G}_\gamma = (\gamma \cup \{\mathbf{0}\}, +_{\mathcal{G}_\gamma})$ is the Abelian group associated with it. Besides, the families of SA $\mathfrak{A}_{\gamma,l} = \{M_{\chi_m,P} = (\gamma \cup \{\mathbf{0}\}, \mathbb{Z}_{l+1}, \delta_{\chi_m,P})\}_{\chi_m \in \mathcal{F}_\gamma, P \in \gamma}$ $(l \in \{1, \ldots, |\gamma|\})$ have been analyzed. Obtained results justify that it is reasonable to use families of SA in elliptic curves over finite fields as mathematical models for computationally secure families of iterated hash functions.

7. Conclusion

In the given paper, some fragment of the Algebraic Theory of SA in finite quasigroups has been developed. The main aim of these studies was to elaborate some theoretic backgrounds for possible using these SA as mathematical models for the design and implementation of computationally secure families of iterated hash functions. To achieve this aim, basic families of SA in abstract finite quasigrops, in finite T-quasigroups, and in elliptic curves over finite fields have been defined and investigated. Obtained results form some base for developing similar fragment of the Algebraic Theory of Automata in finite quasigroups with the aim to use them as mathematical models for families of stream ciphers. This is the main area of our future research.

References

[1] **A.V. Aho, J.E. Hopcroft, J.D. Ullman**, *The design and analysis of computer*

algorithms, Boston, MA, USA, Addison-Wesley Longman Publishing Co., Inc. 1974.

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

[3] **D. Chauhan, I. Gupta, R. Verma**, *Quasigroups and their applications in cryptography*, Cryptologia, Taylor & Francis Online, Published online: 01 May 2020, 1 – 39, https://doi.org/10.1080/01611194.2020.1721615

[4] **M.M. Glukhov**, *Some applications of quasigroups in cryptography*, (Russian), Prikl. Diskr. Mat. **2** (2008), no. 2, 28 – 32.

[5] **C.D. Hillar, D.L. Rhea**, *Automorphisms of finite Abelian groups*, Amer. Math. Monthly, **115** (2007), no. 11, 17 – 23.

[6] **T. Kepka, P. Nemec**, *T-quasigroups. I*, Acta Univ. Carolin. Math. Phys. **12** (1971), no. 1, 39 – 49.

[7] **V.T. Markov, A.V. Michajlev, A.V. Gribov, P.A. Zolotykh, S.S. Skazenik**, *Quasigroups and rings in coding and design of cryptoschemes*, (Russian), Prikl. Diskr. Mat. **6** (2012), no. 4, 31 – 52.

[8] **S. Markovski, D. Gligoroski, V. Bakeva**, *Quasigrouop string processing: Part 1*, Contributions, Sec. Math. Tech. Sci., MANU, **20** (1999), no. 1 – 2, 13 – 28.

[9] **S. Markovski, V. Kusakatov**, *Quasigroup String Processing: Part 2*, Contributions, Sec. Math. Tech. Sci., MANU, **21** (2000), no. 1 – 2, 15 – 32.

[10] **S. Markovski, D. Gligoroski, V. Bakeva**, *Quasigroup and hash functions*, Proc. of the 6$^{\text{th}}$ ICDMA, Bansko, 2001, 43 – 50

[11] **S. Markovski, V. Kusakatov**, *Quasigroup String Processing: Part 3*, Contributions, Sec. Math. Tech.Sci., MANU, **23-24** (2002-2003), no. 1 – 2, 7 – 27.

[12] **S. Markovski, V. Bakeva**, *Quasigroup string processing: Part 4*, Contributions, Sec. Math. Tech. Sci., MANU, **27** (2006), no. 1 – 2, 41 – 53.

[13] **S. Markovski**, *Design of crypto primitives based on quasigroups*, Quasigroups and Related Systems, **23** (2015), 41 – 90.

[14] **A. Mileva, S. Markovski**, *Quasigroup string transformations and hash function design*, Proc. of Int. Conf. ICT Innovations 2009. Springer, Berlin, Heidelberg. 2010. 367 – 376.

[15] **N. A. Nikhil, D.S. Harish Ram**, *Hardware implementation of quasigroup based encryption*, Int. J. of Scientific & Engineering Research, **5** (2014), no. 5, 159 – 162.

[16] **B. Schneier**, *Applied cryptography, protocols, algorithms, and source code in C. Second Edition*, Wiley Computer Publishing, John Wiley & Sons, Inc., 1995.

[17] **V.A. Shcherbacov**, *Quasigroups in cryptology*, Comput. Sci. J. Moldova, **17** (2009), no. 2, 193 – 228.

[18] **V.A. Shcherbacov**, *Elements of Quasigroup Theory and Applications*, CRC Press, Boca Raton, London, New York. 2017.

[19] **V.V. Skobelev, V.G. Skobelev**, *Automata over abstract finite quasigroups*, Cybern. Syst. Anal., **53** (2017), no. 5, 669 – 674.

[20] **V.V. Skobelev, V.G. Skobelev**, *Automata over finite T-quasigroups*, Cybern. Syst. Anal., **54** (2018), no. 3, 345 – 356.

[21] **V.V. Skobelev, V.G. Skobelev**, *Finite automata over magmas: models and some applications in cryptography*, Comput. Sci. J. Moldova. **26** (2018), no. 1, 77 − 92.

[22] **V.V. Skobelev**, *Automata in algebraic structures. Models and methods of their analysis*, (Russian), Donetsk, Ukraine, IAMM of NAS of Ukraine. 2013.

Received June 20, 2020

V.M. Glushkov Institute of Cybernetics of NAS of Ukraine
Glushkova ave., 40
Kyiv, 03187
Ukraine
E-mails: skobelevvg@gmail.com, volodimirvskobelev@gmail.com