Quasigroups and Related Systems **24** (2016), 205 – 218

On the fine structure of quadratical quasigroups

Wieslaw A. Dudek and Robert A. R. Monzo

Abstract. We prove that quadratical quasigroups form a variety $\mathcal{Q}$ of right and left simple groupoids and that the spectrum of $\mathcal{Q}$ is contained in the set of integers equal to 1 plus a multiple of 4. Properties of quadratical quasigroups are described and their inter-relationships are explored. Every element of a quadratical quasigroup is proved to belong to a 4-cycle. These results are applied to find conditions under which the group of additive integers, modulo n, induces quadratical quasigroups.

1. Introduction

This paper builds on the work of Polonijo [3], Volenec [5] and Dudek [1] on quadratical quasigroups. Polonijo [3] and Volenec [5] proved that a quadratical groupoid is a quasigroup. Volenec [5, 6] gave a motivation for studying quadratical quasigroups, in terms of a geometrical representation of the complex numbers C as points of the Euclidean plane. He defined a product $*$ on C that defines a quadratical quasigroup and in which the product of distinct elements x and y is the third vertex of a positively oriented, isosceles right triangle, at which the right angle occurs. Other geometrical motivations for the study of quadratical quasigroups one can find in [7, 8].

Volenec proved in [5] a number of properties of quadratical quasigroups, which are listed in Theorem 2.2 below. These properties tell us a great deal and, indeed, we apply them to prove that quadratical quasigroups form a variety $\mathcal{Q}$ (Theorem 2.30). Inter-relationships amongst the properties of quadratical quasigroups are explored in Section 2.

We begin to amplify our understanding of the fine structure of quadratical quasigroups in Section 3. In so doing, we give further meaning to the *quad* in the word quadratical, in terms of 4-*cycles*. We apply this to prove that the order of a finite quadratical quasigroup is $m = 4t + 1$ for some $t \in \{0, 1, 2, \ldots\}$ (Propositions 3.1 – 3.4), fine tuning Dudek's result that the order of a finite quadratical quasigroup is odd [1, Corollary 1].

In Section 4 we prove results about conditions under which the group of additive integers, modulo n, induces quadratical quasigroups. Results in this section rely heavily on Dudek's Theorem (cf. Theorem 4.1) that proves that every quadratical quasigroup is induced by a commutative group.

2010 Mathematics Subject Classification: 20M15, 20N02
Keywords: quadratical quasigroup, variety, dual groupoid, cycle.

This paper is the first of two by the authors on quadratical quasigroups. The second paper will examine the fine structure of quadratical quasigroups in detail and introduce the concept of a *translatable* quadratical quasigroup. Quadratical quasigroups of many new orders will also be given, along with ideas about possible directions of future research in this area.

2. Properties of quadratical groupoids

Definition 2.1. A groupoid $(Q, \cdot)$ has *property* A if it satisfies the identity

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

It is called *right solvable* (*left solvable*) if for any $\{a, b\} \subseteq Q$ there exists a unique $x \in G$ such that $ax = b$ ($xa = b$). It is *left* (*right*) *cancellative* if $xy = xz$ implies $y = z$ ($yx = zx$ implies $y = z$). It is a *quasigroup* if it is left and right solvable.

Note that a right solvable groupoid is left cancellative and a left solvable groupoid is right cancellative.

Volenec [5] defined a *quadratical groupoid* as a right solvable groupoid satisfying property A. He proved that a quadratical groupoid is left solvable and satisfies the following identities:

Theorem 2.2. *A quadratical groupoid satisfies the following identities:*

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

Corollary 2.3. [2 and 3, Theorem 5] *A quadratical groupoid is a quasigroup.*

Note that throughout the remainder of this paper we will use the fact that quadratical groupoids are quasigroups and satisfy properties (1) through (10), often without mention. Note also that property (3) allows us to write the term xyx without ambivalence in any quadratical quasigroup.

Definition 2.4. We define $\mathcal{Q}$ to be the collection of quadratical quasigroups.

Theorem 2.5. *A groupoid Q is a quadratical quasigroup if and only if it satisfies* (A), (3), (4) *and* (7).

Proof. ($\Rightarrow$) This follows from Theorem 2.2 and the definition of a quadratical quasigroup.
($\Leftarrow$) First we prove that Q is left cancellative. Suppose that $ax = ay$. Then,

$$x \overset{(4)}{=} ax \cdot xa \overset{ax=ay}{=} ay \cdot xa \overset{(A)}{=} yx \cdot y \overset{(3)}{=} xy \cdot x \overset{(A)}{=} ax \cdot ya \overset{ax=ay}{=} ay \cdot ya \overset{(4)}{=} y.$$

So $x = y$ and Q is left cancellative.

Property A implies $x^2 \cdot x = x^2x^2$ and so left cancellativity implies $x = x^2$. Hence, Q is idempotent. Since Q is medial and idempotent it is therefore (left and right) distributive.

Using left and right distributivity, mediality, idempotency and strong elasticity we have

$$a(b \cdot ba) = ab \cdot (a \cdot ba) = ab \cdot (ba \cdot b) = (a \cdot ba)b = (ab \cdot a)b.$$

Hence,

$$a(b \cdot ba) = (ab \cdot a)b. \tag{11}$$

We now prove that $ax = b$ has a unique solution $x = (b \cdot ba) \cdot (b \cdot ba)(ba \cdot a)$. Indeed,

$$\begin{aligned} ax &\overset{(5)}{=} a(b \cdot ba) \cdot (a(b \cdot ba) \cdot a(ba \cdot a)) \overset{(11),(5),(3)}{=} (aba \cdot b) \cdot (aba \cdot b)(aba \cdot a) \\ &\overset{(5)}{=} (aba)(b \cdot ba) \overset{(7),(1)}{=} ab \cdot ba \overset{(4)}{=} b. \end{aligned}$$

The solution x is unique because Q is left cancellative. We have proved that Q is right solvable and so by definition, Q is a quadratical quasigroup. □

Corollary 2.6. *Q is a quadratical quasigroup if and only if it a medial, idempotent groupoid that satisfies property A.*

Proof. ($\Rightarrow$) This follows from the definition of a quadratical quasigroup and from Theorem 2.2.
($\Leftarrow$) Let Q be a medial, idempotent groupoid that satisfies property A. By Theorem 2.5 we need only show that Q satisfies (3) and (4).

Since Q is idempotent and satisfies property A, for all $\{x, y\} \subseteq Q$,

$$x = x^2 \overset{(7)}{=} x^2x \overset{(A)}{=} yx \cdot xy,$$

so Q satisfies (4). Also, idempotency and mediality imply (5) and so

$$xy \cdot x \overset{(1)}{=} xy \cdot x^2 \overset{(7)}{=} x^2 \cdot yx \overset{(1)}{=} x \cdot yx \overset{(A)}{=} yx \cdot yy \overset{(1)}{=} yx \cdot y,$$

which proves (3). □

Theorem 2.7. *A groupoid satisfying* (4) *and either* (5) *or* (6) *is idempotent*

Proof. From (4) we obtain $x^2x^2 = x$ for any $x \in G$. If Q also satisfies (5), then

$$x^2x = x^2(x^2x^2) \overset{(5)}{=} (x^2x^2)(x^2x^2) = x^2.$$

Also,

$$x = x^2x^2 = (x^2x)(x^2x) \overset{(5)}{=} ((x^2x)x^2)((x^2x)x) = (x^2x^2)(x^2x) = xx^2.$$

Then

$$x^2 = x^2x = (x^2x)(xx^2) \overset{(4)}{=} x.$$

Similarly, in a groupoid satisfying (4) and (6), $x = x^2x$, $x^2 = xx^2$ and $x^2 = xx^2 = (x^2x)(xx^2) = x$, by (4). □

Example 2.8. A groupoid Q of order greater than or equal to 2 and satisfying the identity $xy = zw$ is distributive but not idempotent.

Example 2.9. The following groupoid Q satisfies (4) but not (1), (2), (7), (5), (10). Moreover, it is not left solvable or right solvable.

$\cdot$	x	y	z	w
x	y	z	w	y
y	w	x	w	x
z	y	x	w	y
w	z	z	x	z

Theorem 2.10. *A groupoid Q satisfying* (4), (5), (6) *and* (7) *is cancellative.*

Proof. Suppose that $ax = ay$ for any $\{a, x, y\} \subseteq Q$. By Theorem 2.7, $ax = (ax)^2$. Then, $ax = ax \cdot ax = ax \cdot ay = ay \cdot ax = a \cdot yx = a \cdot xy$. Consequently, $yx \overset{(4)}{=} (a{\cdot}yx)(yx{\cdot}a) = ax{\cdot}(yx{\cdot}a) \overset{(5)}{=} (ax{\cdot}yx)(ax{\cdot}a) \overset{(6)}{=} (ay{\cdot}x)(ay{\cdot}a) \overset{(5)}{=} ay{\cdot}xa = ax{\cdot}xa \overset{(4)}{=} x$. Similarly, $xy = y$. So $y = xy \cdot yx = yx = x$.

Analogously, $xa = ya$ implies $x = y$, so Q is cancellative. □

Theorem 2.11. *A groupoid satisfying* (4), (5), (6) *and* (7) *also satisfies* (3).

Proof. Theorems 2.7 and 2.10 imply that Q is idempotent and cancellative. So $xy{\cdot}x = xy{\cdot}xx = x{\cdot}yx$. Hence, $(xy{\cdot}x)y = (x{\cdot}yx)y \overset{(6)}{=} xy{\cdot}(yx{\cdot}y) \overset{(5)}{=} (xy{\cdot}yx)(xy{\cdot}y) \overset{(4)}{=} y(xy \cdot y) \overset{(5)}{=} (y \cdot xy)y^2 = (y \cdot xy)y$ and, by cancellation, $xy \cdot x = y \cdot xy \overset{(5)}{=} yx \cdot y$. Therefore, Q is strongly elastic, i.e., it satisfies (3). □

Corollary 2.12. *An idempotent medial groupoid satisfying* (4) *is cancellative and strongly elastic.*

Proof. Medial idempotent groupoids are distributive. The corollary follows from Theorems 2.10 and 2.11. □

Theorem 2.13. *A left (or right) cancellative, medial, idempotent groupoid satisfying* (3) *satisfies* (4).

Proof. Mediality and idempotency imply distributivity. Then, $(ca \cdot ac)^2 = ca \cdot ac = (ca \cdot a)(ca \cdot c)$. Thus, by (3) we obtain

$$(ca \cdot ac)^2 = ca \cdot ac = (ca \cdot a)(c \cdot ac) = (ca \cdot a)(ca \cdot c) = (ca \cdot a)(ac \cdot a) = (ca \cdot ac)a$$

and so left cancellativity implies $ca \cdot ac = a$. Also, using right cancellativity,

$$(ca \cdot ac)^2 = ca \cdot ac = ca \cdot (ac)^2 = (c \cdot ac)(a \cdot ac) = (a \cdot ca)(a \cdot ac) = a(ca \cdot ac)$$

implies $a = ca \cdot ac$. □

Theorem 2.14. *A groupoid Q is a quadratical quasigroup if and only if it is idempotent, medial and satisfies* (4).

Proof. ($\Rightarrow$) This follows from Theorem 2.2.
($\Leftarrow$) By Corollary 2.6, we need only show that $xy \cdot x = zx \cdot yz$. But, since mediality and idempotency imply left distributivity, $zx \cdot yz = (zx \cdot y)(zx \cdot z)$ and, by Corollary 2.12, $zx \cdot yz = (zx \cdot y)(xz \cdot x) = (zx \cdot xz)(yx) = x \cdot yx = xy \cdot x$. □

Definition 2.15. The *dual* of a groupoid $(Q, \cdot)$ is the groupoid $Q^* = (Q, *)$, where $x * y = y \cdot x$.

Corollary 2.16. *The dual of a quadratical quasigroup is a quadratical quasigroup.*

Corollary 2.17. *Any subgroupoid of a quadratical quasigroup is a quadratical quasigroup.*

Note that an idempotent semigroup satisfies (4) if and only if it satisfies the identity $x = xyx$; that is, if and only if it is a rectangular band. A semigroup with property A is cancellative if and only if it is trivial.

Theorem 2.18. *An idempotent groupoid satisfying* (4) *and* (10) *is elastic.*

Proof. Indeed, $x = x^2 = yx \cdot xy$ implies $x \cdot yx = xy \cdot x$. □

Theorem 2.19. *An elastic groupoid satisfying* (4) *is idempotent.*

Proof. $x^2 = xx^2 \cdot x^2x = x^2x \cdot xx^2 = x$. □

Theorem 2.20. *A groupoid Q is a quadratical quasigroup if and only if it satisfies* (2), (4) *and* (7).

Proof. ($\Rightarrow$) This follows from Theorem 2.2.
($\Leftarrow$) Assume that Q satisfies (2), (4) and (7). By Theorem 2.19, Q is idempotent. By Theorem 2.14 then, Q is quadratical. □

Theorem 2.21. *An idempotent groupoid satisfying* (2) *and* (10) *satisfies* (4).

Proof. $x \cdot yx = xy \cdot x$ implies $yx \cdot xy = x^2 = x$. □

Corollary 2.22. *An idempotent groupoid satisfying* (10) *satisfies* (2) *if and only if it satisfies* (4).

Proof. This follows from Theorems 2.18 and 2.21. □

Theorem 2.23. *A medial groupoid satisfying* (4) *satisfies* (10).

Proof. Suppose that $xy = zw$. Then $zw \cdot yx = xy \cdot yx = y$ and $wz \cdot xy = wz \cdot zw = z$. Therefore, $yz = (zw \cdot yx)(wz \cdot xy) = (zw \cdot wz)(yx \cdot xy) = wx$. □

Theorem 2.24. *A groupoid Q is a quadratical quasigroup if and only if it satisfies* (1), (2), (7) *and* (10).

Proof. ($\Rightarrow$) This follows from Theorem 2.2.
($\Leftarrow$) Suppose that Q satisfies (1), (2), (7) and (10). By Theorem 2.21, it satisfies (4). By Theorem 2.20 it is a quadratical quasigroup. □

Theorem 2.25. *A left* (*or right*) *distributive groupoid satisfying* (3) *and* (10) *has the property A.*

Proof. Since in a left distributive groupoid $y \cdot zx = yz \cdot yx$, $zx \cdot yz = yx \cdot y = xy \cdot x$. Similarly, in a right distributive groupoid. □

Theorem 2.26. *In a quadratical quasigroup $x \cdot yz = xy \cdot z$ if and only if $x = z$.*

Proof. ($\Rightarrow$) Using Theorem 2.2, $x \cdot yz = xy \cdot z$ implies $xy \cdot xz = xz \cdot yz$ implies $yz \cdot xy = (xz)^2 = xz = zx \cdot z$ implies $xz = zx \cdot z$ implies $x = zx$ implies $x = z$.
($\Leftarrow$) By Theorem 2.2, a quadratical quasigroup is elastic and so $x \cdot yx = xy \cdot x$. □

Definition 2.27. A groupoid is *nowhere commutative* if $xy = yx$ implies $x = y$.

Theorem 2.28. *Quadratical quasigroups are nowhere commutative.*

Proof. Since by Theorem 2.2, quadratical quasigroups are alterable and idempotent, $xy = yx$ implies $y^2 = x^2$ implies $y = x$. □

Theorem 2.29. *A groupoid Q is a quadratical quasigroup if and only if it satisfies* (4), (5) *and* (10).

Proof. ($\Rightarrow$) This follows from Theorem 2.2.
($\Leftarrow$) By Theorem 2.7, Q is idempotent. Therefore, by Theorem 2.14 we need only show that Q is medial. Observe that by Theorems 2.11 and 2.25, this groupoid has the property A. Hence, $wx \cdot w = zw \cdot xz = yw \cdot xy$ and, using (10), $xz \cdot yw = xy \cdot zw$. So it is medial. □

As a consequence of the above results we obtain

Theorem 2.30. *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).

Definition 2.31. A subset I of a groupoid Q is a *right* (*left*) *ideal* of Q if $ig \in I$ ($gi \in I$) for all $i \in I$ and all $g \in Q$. The subset I is called an *ideal* if it is a right ideal and a left ideal. A groupoid Q is *simple* (*right simple; left simple*) if for every ideal (right ideal; left ideal) I of Q, $I = Q$.

Theorem 2.32. *Groupoids satisfying* (4) *are right simple and left simple groupoids.*

Proof. Suppose that I is a right or left ideal of a groupoid Q satisfying (4). Let $i \in I$ and $g \in Q$. Then, $g = ig \cdot gi \in I$ and so $I = Q$. □

Corollary 2.33. *Quadratical quasigroups are right and left simple.*

3. Cycles in quadratical quasigroups

Let Q be a quadratical quasigroup with $a, b \in Q$ and $a \neq b$. 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 $C_i = \{x_i, x_{(i+1) \bmod n}, x_{(i+2) \bmod n}, \ldots, x_{(i+n-1) \bmod n}\}$.

Proposition 3.1. *If* n*-cycles exist in a quadratical quasigroup then* $n = 4$.

Proof. Since $aba = x_nx_1 = x_1x_2 = x_2x_3$, by (10) $x_1 = x_2x_n$ and $x_2 = x_3x_1$. Now $x_3 \cdot x_2x_4 = x_3x_2 \cdot x_3x_4 = x_3x_2 \cdot aba = (x_3 \cdot aba)(x_2 \cdot aba)$. But by (10), $aba \cdot x_2 = x_3 \cdot aba$ and so $x_3 \cdot x_2x_4 = (x_3 \cdot aba)(x_2 \cdot aba) = (aba \cdot x_2)(x_2 \cdot aba) = x_2 = x_3x_1$. Hence, by cancellation, $x_1 = x_2x_4 = x_2x_n$ and so $x_4 = x_n$. □

Proposition 3.2. *Let* Q *be a quadratical quasigroup with* $a, b \in Q$ *and* $a \neq b$. *Then every element* $x_1 \neq aba$ *of* Q *is a member of a* 4*-cycle based on* aba.

Proof. Let $a, b \in Q$ and $a \neq b$. Suppose that $x_1 \neq aba$ for some $x_1 \in Q$. Using right solvability, we can solve the equations $aba = x_1x$, $aba = xy$, $aba = yz$ and $aba = zw$. If we define $x_2 = x$, $x_3 = y$, $x_4 = z$ and $x_5 = w$, then $aba = x_1x_2 = x_2x_3 = x_3x_4 = x_4x_5$. Using (10), $x_4 = x_5x_3$ and $x_5x_1 = x_2x_4 = x_2 \cdot x_5x_3 = x_2x_5 \cdot x_2x_3 = x_2x_5 \cdot aba$. Therefore, by (10), $aba \cdot x_5 = x_1 \cdot x_2x_5 = x_1x_2 \cdot x_1x_5 = aba \cdot x_1x_5$. Hence $x_5 = x_1x_5$ and $x_1 = x_5$. So we have proved that $\{x_1, x_2, x_3, x_4\}$ is a 4-cycle based on aba. □

Proposition 3.3. *Let C and D be two 4-cycles based on aba ($a \neq b$) in a quadratical quasigroup. Then either $C = D$ or $C \cap D = \emptyset$.*

Proof. Suppose that $C = \{x_1, x_2, x_3, x_4\}$ and $D = \{y_1, y_2, y_3, y_4\}$. If $x_1 = y_1$, then $aba = x_1x_2 = y_1y_2 = x_1y_2$ and so $x_2 = y_2$. Then, $aba = x_2x_3 = y_2x_3 = y_2y_3$ and so $x_3 = y_3$. Finally, $aba = x_3x_4 = y_3x_4 = y_3y_4$ and $x_4 = y_4$. Hence, $C = D$. Similarly, if $x_1 = y_2$, then we can prove that $x_2 = y_3$, $x_3 = y_4$ and $x_4 = y_1$ and $C = D$. Similarly, if $x_1 \in \{y_3, y_4\}$ it is straightforward to prove that $C = D$.

The proofs that $C = D$ if $x_2 \in D$ or $x_3 \in D$ or $x_4 \in D$ are similar. □

Proposition 3.4. *Any finite quadratical quasigroup has order $m = 4t + 1$ for some $t \in \{0, 1, 2, \ldots\}$.*

Proof. A finite quadratical quasigroup consists of the element aba and the union of its disjoint 4-cycles based on aba. By definition, no cycle contains the element aba. The proposition is therefore valid. □

So, later we will assume that $m = 4t + 1$ for some natural t.

4. Existence of quadratical quasigroups

We start with the following theorem proved in [1].

Theorem 4.1. *A groupoid $(G, \cdot)$ is a quadratical quasigroup if and only if there exists a commutative group $(G, +)$ in which for every $a \in G$ the equation $z + z = a$ has a unique solution $z = \frac{1}{2}a \in G$, and two its automorphisms φ, ψ such that for all $x, y \in G$ we have*

$$x \cdot y = \varphi(x) + \psi(y), \tag{12}$$

$$\varphi(x) + \psi(x) = x, \tag{13}$$

$$2\psi\varphi(x) = x. \tag{14}$$

From the proof of this theorem it follows that $\varphi\psi = \psi\varphi$. So, if $\varphi \neq \psi$, then $(G, +)$ induces two quadratical quasigroups: $G = (G, \cdot)$ and its dual $G^* = (G, \circ)$, where $x \circ y = y \cdot x$. Clearly, in any case $G \neq G^*$ since $x \circ y = x \cdot y$ means that $(G, \cdot)$ is commutative which together with the basic identity (A) gives $xy \cdot x = zx \cdot yz = xz \cdot yz = xy \cdot z$. This implies $x = z$, a contradiction. Since, G and G^*, by (12), are isotopic to the same group, they are isotopic too. Moreover, from Theorem 3.3 in [2] it follows that *all parastrophes of a quadratical quasigroup are isotopic.*

Corollary 4.2. *There are no quadratical quasigroups with left (right) neutral element.*

Proof. If e is a left neutral element then $x = e \cdot x = \varphi(e) + \psi(x)$. Since $\psi(x) = x - \varphi(e)$ is an automorphism of a group $(Q, +)$, we have $(x + y) - \varphi(e) = \psi(x + y) = \psi(x) + \psi(y) = (x + y) - 2\varphi(e)$, which implies $\varphi(e) = 0$. Thus $\psi(x) = x$, consequently, by (13), $\varphi(x) = 0$ for every $x \in Q$, a contradiction.

Analogously for quasigroups with a right neutral element. □

Corollary 4.3. *There are no quadratical quasigroups that are loops or groups.*

Corollary 4.4. *If a quadratical quasigroup Q is induced by groups $(Q,+)$ and $(Q,\circ)$, then these groups are isomorphic.*

Proof. Indeed, $x\cdot y=\varphi(x)+\psi(y)=\alpha(x)\circ\beta(y)$. Thus, $\varphi\alpha^{-1}(x)+\psi\beta^{-1}(y)=x\circ y$. So, groups $(Q,+)$ and $(Q,\circ)$ are isotopic. Thus, by Albert's theorem, they are isomorphic. □

Corollary 4.5. *Quadratical quasigroups are isotopic if and only if they are induced by isomorphic groups.*

Proof. Let quadratical quasigroups Q_1 and Q_2 be induced by groups $(Q_1,*_1)$ and $(Q_2,*_2)$, respectivety. If quasigroups Q_1 and Q_2 are isotopic, then groups $(Q_1,*_1)$ and $(Q_2,*_2)$ also are isotopic, and consequently, they are isomorphic. □

Corollary 4.6. *Quadratical quasigroups induced by the same group are isotopic.*

Corollary 4.7. *Quadratical quasigroups of the same prime order are isotopic.*

Theorem 4.8. *A quadratical groupoid induced by the additive group $\mathbb{Z}_m$ has the form*

$$x\cdot y=ax+(1-a)y\,, \tag{15}$$

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

$$2a^2-2a+1=0. \tag{16}$$

Proof. First observe that in the additive group $\mathbb{Z}_m$, where $m=4t+1$, for every $b\in\mathbb{Z}_m$ there exists $z\in\mathbb{Z}_m$ such that $z+z=b$. Indeed, if b is even, then obviously $z=\frac{1}{2}b\in\mathbb{Z}_m$. If b is odd, then $1+b$ is even and $z+z=b+4t+1$ for $z=2t+\frac{1+b}{2}\in\mathbb{Z}_m$.

In $\mathbb{Z}_m$ the equation (16) has the form $2a(a-1)+1=0=km$. Let d be a positive common divisor of a and m. Since m is odd, d also is odd and $d|(2a(a-1)+1)$. Consequently, $d|1$. Hence $(a,m)=1$. Analogously we can see that $(a-1,m)=1$. So, for any a satisfying (16) we have $(a,m)=(1-a,m)=1$. Thus the maps $\varphi(x)=ax$ and $\psi(x)=(1-a)x$, where $a\in\mathbb{Z}_m$ satisfies (16), are automorphisms of the additive group $\mathbb{Z}_m$ and satisfy (13), which in this case is equivalent to (15). Since (14) is equivalent to (16), a quasigroup defined by (15) is quadratical. □

Corollary 4.9. *A groupoid induced by $\mathbb{Z}_m$ by (15) is quadratical if and only if its dual groupoid with the operation*

$$x\cdot y=(1-a)x+ay \tag{17}$$

is quadratical.

Proof. Indeed, as it is not difficult to see a satisfies (16) if and only if (16) is satisfied by $1-a$. So, a and $1-a$ are roots of the polynomial $w(x) = 2x^2 - 2x + 1$. If $a = 1-a$, then $w(x) = 2(x-a)^2 = 2x^2 - 4ax + 2a^2$. Hence $2a = 1$ and $2a^2 = 1$. Thus, $1 = 4a^2 = 2$. Obtained contradiction shows that $a \neq 1-a$. Thus, (15) and (17) define two different quadratical quasigroups. □

Theorem 4.10. *If $m = 4t+1$ is prime, then the additive group $\mathbb{Z}_m$ induces exactly two quadratical groupoids. They have form*

$$x \circ_1 y = a_1 x + a_2 y \qquad \text{and} \qquad x \circ_2 y = a_2 x + a_1 y,$$

where $a_1 = 2t + 1 + s$, $a_2 = 2t + 1 - s$ and $s^2 \equiv t (\mathrm{mod}\, m)$.

Proof. By the Lagrange theorem (cf. [4]), the equation $2a^2 - 2a + 1 \equiv 0 (\mathrm{mod}\, m)$ has no more than two solutions in $\mathbb{Z}_m$. $(\mathbb{Z}_m, +, \cdot)$ is a field, so these solutions have the form $a_1 = \frac{1}{2} + \sqrt{t}$ and $a_1 = \frac{1}{2} - \sqrt{t}$. Since in this field $\frac{1}{2}$ is equal to $2t+1$ and $\sqrt{t} \in \mathbb{Z}_m$ for each $t \in \mathbb{Z}_m$, we have $a_1 = 2t + 1 + s$ and $a_2 = 2t + 1 - s$, where $s^2 \equiv t (\mathrm{mod}\, m)$. Obviously $a_1 \neq a_2$ and $(a_1, m) = (a_2, m) = 1$. Theorem 4.8 completes the proof. □

Theorem 4.11. *There are no quadratical quasigroups of order $m = p_1 p_2 \cdots p_k$, where p_i are different odd primes such that at least one $p_j \equiv 3 (\mathrm{mod}\, 4)$.*

Proof. Indeed, all groups of such order are isomorphic to the additive group $\mathbb{Z}_m$. Since any automorphism of the group $\mathbb{Z}_m$ has the form $\varphi(x) = ax$, by Theorem 4.8, a quadratical quasigroup induced by this group has the form (15), where a satisfies (16).

The equation (16) is equivalent to the equation $4a^2 - 4a + 2 = 0 (\mathrm{mod}\, m)$, i.e., to the equation $(2a-1)^2 + 1 = 0 (\mathrm{mod}\, m)$. In the ring $\mathbb{Z}_m$ the last equation can be written in the form $x^2 \equiv (-1) (\mathrm{mod}\, m)$, where $x = 2a - 1$. The equation $x^2 \equiv (-1) (\mathrm{mod}\, m)$ has a solution only in the case when each prime divisor p of m has the property $p \equiv 1 (\mathrm{mod}\, 4)$ (cf. [4]). So, if some prime $p_j | m$ and $p_j \equiv 3 (\mathrm{mod}\, 4)$, then this group cannot induce quadratical quasigroups. □

Corollary 4.12. *There are no quadratical quasigroups of order* $21, 33, 57, 69, 77, 93, 105, 129, \ldots$

Theorem 4.13. *A commutative group of order $m = p_1 p_2 \cdots p_n$, where $p_1, \ldots, p_n$ are different primes such that $p_i \equiv 1 (\mathrm{mod}\ 4)$, induces 2^n different quadratical quasigroups.*

Proof. Such groups are isomorphic to the additive group $\mathbb{Z}_m$. Quadratical quasigroups defined on this group have the form (15), where a satisfies (16). The number of solutions of the equation $f(x) \equiv 0 (\mathrm{mod}\ m)$ is equal to $T_1 T_2 \cdots T_n$, where T_i denotes of the number of solutions of the equation $f(x) \equiv 0 (\mathrm{mod}\ p_i)$ (cf. [4]). But for $f(x) = 2x^2 - 2x + 1$ the last equation has exactly two solutions (Theorem 4.10). Thus, $f(x) \equiv 0 (\mathrm{mod}\, m)$ has exactly 2^n solutions. Consequently, it defines 2^n quadratical quasigroups. □

Each finite commutative group is isomorphic to a direct product of cyclic groups. For simplicity consider the case when a commutative group G of order $m = 4t + 1$ is a direct product of two groups $\mathbb{Z}_{m_1}$ and $\mathbb{Z}_{m_2}$. If $m_1 \neq m_2$, then each automorphism φ of G has the form $\varphi(x, y) = (\varphi_1(x), \varphi(x_2))$, where φ_i is an automorphism of the group $\mathbb{Z}_{m_i}$ because any automorphism saves the order of each element, so $\varphi(\mathbb{Z}_{m_1} \times \{0\}) = \mathbb{Z}_{m_1} \times \{0\}$. Thus, in this case, quadratical quasigroups induced by G are direct products of quadratical quasigroups induced by groups $\mathbb{Z}_{m_i}$.

Theorem 4.14. *The group $\mathbb{Z}_m$ induces a quadratical quasigroup if and only if $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, where p_i are different primes such that $p_i \equiv 1 (\mathrm{mod}\, 4)$ for all $i = 1, 2, \ldots, n$.*

Proof. Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, where p_i are different primes. Then obviously $\mathbb{Z}_m = \mathbb{Z}_{p_1^{\alpha}} \times \mathbb{Z}_{p_1^{\alpha_2}} \times \ldots \times \mathbb{Z}_{p_n^{\alpha_n}}$. Any automorphism of this group has the form $\varphi(x_1, x_2, \ldots, x_n) = a(x_1, x_2, \ldots, x_n) = (ax_1, ax_2, \ldots, ax_n)$. So, the equation (16), i.e., $2a^2 - 2a + 1 \equiv 0 (\mathrm{mod}\, m)$ has a solution if and only if each of equations $2a^2 - 2a + 1 \equiv 0 (\mathrm{mod}\, p_i^{\alpha_i})$ has a solution. The last equation is solved only in the case when $2a^2 - 2a + 1 \equiv 0 (\mathrm{mod}\, p_i)$ is solved (cf. [4]), but it is possible if and only if $p_i \equiv 1 (\mathrm{mod}\, 4)$. □

Corollary 4.15. *If there exists a prime $p|m$ such that $p \equiv 3 (\mathrm{mod}\, 4)$, then there are no quadratical quasigroups induced by the group $\mathbb{Z}_m$.*

Below are listed all quadratical quasigroups of the form $x \cdot y = ax + by (\mathrm{mod}\, m)$, where $a < b$, defined on the group $\mathbb{Z}_m$ for $m < 400$. Dual quasigroups $x \circ y = bx + ay (\mathrm{mod}\, m)$ are omitted.

m	a	b
5	2	4
13	3	11
17	7	11
25	4	22
29	9	21
37	16	22
41	5	37
53	12	42
61	6	56
65	24	42
	29	37
73	14	60
85	7	79
	24	62
89	28	62
97	38	60

m	a	b
101	46	56
109	17	93
113	8	106
125	29	97
137	19	119
145	9	137
	67	79
149	53	97
157	65	93
169	50	120
173	47	127
181	10	172
185	22	164
	59	127
193	41	153
197	92	106

m	a	b
205	37	169
	87	119
221	11	211
	24	198
229	54	176
233	45	189
241	89	153
257	121	137
265	12	254
	42	224
269	94	176
277	109	169
281	27	255
289	126	164
293	78	216

m	a	b
305	67	239
	117	189
313	13	301
317	102	216
325	29	297
	154	172
337	95	243
349	107	243
353	156	198
365	14	352
	87	279
373	135	239
377	50	328
	154	224
389	58	332
397	32	366

The case when finite commutative group is isomorphic to a direct product of cyclic groups of the same order is more complicated. Suppose for simplicity that $G = \mathbb{Z}_n \times \mathbb{Z}_n$ for some natural $n > 1$. Then G can be considered as a module or a vector space $\mathbb{Z}_n \times \mathbb{Z}_n$ over $\mathbb{Z}_n$. So, automorphisms of this group can be calculated as linear maps of $\mathbb{Z}_n \times \mathbb{Z}_n$. From Theorem 4.1 it follows that the matrices of these maps satisfy the equation $2A(A - I) + I = \theta$, where I and θ are the identity and zero matrices. Obviously, if A satisfies this equation then $B = A - I$ also satisfies this equation and $A + B = I$. Hence $(x, y) * (z, u) = A(x, y) + B(z, u)$ and $(x, y) \circ (z, u) = B(x, y) + A(z, u)$ are dual quasigroups.

Case $m = 9$.
Direct computations shows that for $\mathbb{Z}_3 \times \mathbb{Z}_3$ we have six such quasigroups (cf. [1]). These quasigroups are defined by maps with the following matrices:

$$A_1 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, A_2 = \begin{bmatrix} 0 & 2 \\ 2 & 1 \end{bmatrix}, A_3 = \begin{bmatrix} 2 & 1 \\ 2 & 2 \end{bmatrix} \text{ and } B_i = A_i - I.$$

Case $m = 25$.
Using a similar argument we can see that the group $G = \mathbb{Z}_5 \times \mathbb{Z}_5$ induces 16 quadratical quasigroups $(G, *_i)$ with the operation

$$(x, y) *_i (z, u) = A_i(x, y) + B_i(z, u) \tag{18}$$

and 16 quasigroups dual to the above. These quasigroups are determined by matrices A_i:

$$\begin{bmatrix} 0 & a \\ b & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & c \\ d & 4 \end{bmatrix}, \begin{bmatrix} 3 & 1 \\ 1 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 3 \\ 2 & 3 \end{bmatrix},$$

where $ab = 2 (\mathrm{mod}\, 5)$ and $cd = 0 (\mathrm{mod}\, 5)$.

Case $m = 45$.
Commutative groups of order $m = 45$ are isomorphic to $\mathbb{Z}_{45}$, $\mathbb{Z}_3 \times \mathbb{Z}_{15}$, $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ or $\mathbb{Z}_9 \times \mathbb{Z}_5$. Groups $\mathbb{Z}_3$, $\mathbb{Z}_9$ and $\mathbb{Z}_{45}$ do not induce quadratical quasigroups. Therefore, from the above groups only $\mathbb{Z}_\times \mathbb{Z}_3 \times \mathbb{Z}_5$ induces such quasigroups. These quasigroups are a direct product of quadratical quasigroups induced by $\mathbb{Z}_3 \times \mathbb{Z}_3$ and $\mathbb{Z}_9$. So, they have the form

$$(x_1, y_1, z_1) *_i (x_2, y_2, z_2) = (A_i(x_1, y_1) + B_i(x_2, y_2), a_i z_1 + b_i z_2),$$

where A_i, B_i are as in the above and a_i is equal to 2 or to 4. We have 12 such quasigroups.

Case $m = 49$.
By Theorem 4.11 the group $\mathbb{Z}_{49}$ do not induce any quadratical quasigroups. The group $\mathbb{Z}_7 \times \mathbb{Z}_7$ induces 21 quadratical quasigroups defined by (18) and 21 duals. These quasigroups are determined by matrices A_i:

$$\begin{bmatrix} 0 & a \\ b & 1 \end{bmatrix}, \begin{bmatrix} 2 & c \\ d & 6 \end{bmatrix}, \begin{bmatrix} 3 & e \\ f & 5 \end{bmatrix}, \begin{bmatrix} 4 & 1 \\ 5 & 4 \end{bmatrix}, \begin{bmatrix} 4 & 2 \\ 6 & 4 \end{bmatrix}, \begin{bmatrix} 4 & 3 \\ 4 & 4 \end{bmatrix},$$

where $ab = 3(\mathrm{mod}\,7)$, $cd = 1(\mathrm{mod}\,7)$ and $ef = 4(\mathrm{mod}\,7)$.

Case $m = 65$.
Quadratical quasigroups induced by $\mathbb{Z}_{65} = \mathbb{Z}_5 \times \mathbb{Z}_{13}$ are direct products of quadratical quasigroups induced by $\mathbb{Z}_5$ an $\mathbb{Z}_{13}$. So, they have the form

$$(x, y) *_1 (z, u) = (2x + 4z, 3y + 11u),$$
$$(x, y) *_2 (z, u) = (4x + 2z, 11y + 3u),$$
$$(x, y) *_3 (z, u) = (2x + 4z, 11y + 3u),$$
$$(x, y) *_4 (z, u) = (4x + 2z, 3y + 11u).$$

Obviously $(G, *_1)$ and $(G, *_2)$, also $(G, *_3)$ and $(G, *_4)$, are dual and are isomorphic to quasigroups mentioned in the above table for $\mathbb{Z}_{65}$.

Case $m = 81$.
Commutative groups of order $m = 81$ are isomorphic to one of groups $\mathbb{Z}_{81}$, $\mathbb{Z}_9 \times \mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_{27}$, $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9$ or $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. By Corollary 4.15 groups $\mathbb{Z}_3$, $\mathbb{Z}_9$, $\mathbb{Z}_{27}$, $\mathbb{Z}_{81}$ do not induce quadratical quasigroups. Thus quadratical quasigroups of order 81 can be induced by groups $\mathbb{Z}_9 \times \mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ only. The group $\mathbb{Z}_9 \times \mathbb{Z}_9$ induces 27 quadratical quasigroups defined by (18) and 27 duals. These quasigroups are determined by matrices A_i:

$$\begin{bmatrix} 0 & a \\ b & 1 \end{bmatrix}, \begin{bmatrix} 2 & c \\ d & 8 \end{bmatrix}, \begin{bmatrix} 3 & e \\ f & 7 \end{bmatrix}, \begin{bmatrix} 4 & g \\ h & 6 \end{bmatrix}, \begin{bmatrix} 5 & 1 \\ 2 & 5 \end{bmatrix}, \begin{bmatrix} 5 & 2 \\ 1 & 5 \end{bmatrix}, \begin{bmatrix} 5 & 4 \\ 5 & 5 \end{bmatrix},$$

where $ab = 4(\mathrm{mod}\,9)$, $cd = 2(\mathrm{mod}\,9)$, $ef = 7(\mathrm{mod}\,9)$ and $gh = 1(\mathrm{mod}\,9)$.

Using a computer we can see that the group $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ induces 2106 quadratical quasigroups defined by (18) and 2106 duals. So, this group defines 4212 quadratical quasigroups.

Case $m = 125$.
Commutative groups of order $m = 125$ are isomorphic to one of the groups $\mathbb{Z}_{125}$, $\mathbb{Z}_5 \times \mathbb{Z}_{25}$ or $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$. The first group induces only two quadratical quasigroups, the second induces 64. Using a computer we can see that the last group induces 1552 quadratical quasigroups. So in the case $m = 125$ we have 1618 such quasigroups.

It is not difficult to observe that if p is prime and $p \equiv 1(\mathrm{mod}\ 4)$ then the group $(\mathbb{Z}_p)^k$ induces quadratical quasigroups for every k, but for $p \equiv 3(\mathrm{mod}\ 4)$ it induces quadratical quasigroups only for even k.

Theorem 4.16. *There are no quadratical quasigroups induced by the additive groups $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.*

Proof. In $\mathbb{Z}$ there are no x such that $x + x = 1$, so, by Theorem 4.1 such a group cannot induce quadratical quasigroups. Automorphisms of the group $(\mathbb{Q}, +)$ have the form $\varphi(x) = ax$ for some $0 \neq a \in \mathbb{Q}$. Obviously $\psi(x) = (1 - a)x$ for $a \neq 1$, also is an automorphism and φ, ψ satisfy (13). Then (14) gives (16), which is

equivalent to $(2a-1)^2+1=0$. So, $a=\frac{1}{2}(1+i)$ or $a=\frac{1}{2}(1-i)$. These elements are not in $\mathbb{Q}$. Since for each automorphism φ of $(\mathbb{R},+)$ there is $a\in\mathbb{R}-\{0\}$ such that $\varphi(x)=ax$ for $x\in\mathbb{Q}$, each automorphism of $(\mathbb{R},+)$ defining a quadratical quasigroup satisfies (14), i.e., a satisfies (16). But in this case $a\notin\mathbb{R}$. □

Corollary 4.17. *The smallest quadratical quasigroup of infinite order is defined on the additive group* $\mathbb{Q}[i]=\{u+vi\,|\,u,v\in\mathbb{Q}\}$ *and has the form* $xy=ax+(1-a)y$, *where* $a=\frac{1}{2}(1+i)$ *or* $a=\frac{1}{2}(1-i)$.

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] **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.

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

[5] **V. Volenec**, *Quadratical groupoids*, Note di Matematica **13** (1993), no. 1, 107 – 115.

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

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

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

Received February 23, 2016
Revised September 20, 2016

W.A. Dudek
Faculty of Pure and Applied Mathematics, Wroclaw University of Science and Technology
50-370 Wroclaw, Poland
Email: 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