QUADRATICAL QUASIGROUPS AND MENDELSOHN DESIGNS

ALEŠ DRÁPAL, TERRY S. GRIGGS, AND ANDREW R. KOZLIK

Abstract. Let the product of points A and B be the vertex C of the right isosceles triangle for which AB is the base, and ABC is oriented anticlockwise. This yields a quasigroup that satisfies laws $(xu)(vy) = (xv)(uy)$, $(xy)(yx) = y$ and $xx = x$. Such quasigroups are called quadratical. Quasigroups that satisfy only the latter two laws are equivalent to perfect Mendelsohn designs of length four (PMD$(v, 4)$). This paper examines various algebraic identities induced by PMD$(v, 4)$, classifies finite quadratical quasigroups, and shows how the square structure of quadratical quasigroups is associated with toroidal grids.

Introduction

Define a binary operation upon the points of a Euclidean plane by setting $A \cdot A = A$, and $A \cdot B = C$ if $A \neq B$ and ABC is the anticlockwise oriented right isosceles triangle for which AB is the base. This operation satisfies the law $(xy)x = (zx)(yz)$, see Fig. 1. Volenec proved in 1994 [11] that any left quasigroup that satisfies this law is necessarily a (both sided) quasigroup, and that this quasigroup is idempotent ($xx = x$), medial ($(xu)(vy) = (xv)(uy)$), see Fig. 2, and fulfils the *Third Stein's law* $(xy)(yx) = y$, see Fig. 3. Quasigroups satisfying $(xy)x = (zx)(yz)$ are called *quadratical*.

The law $(xy)(yx) = y$ is essential for this paper. Its naming is due to Sade [7]. An alternative name is the *bookend law*. Another possible name for this law [8] is discussed at the end of Section 1. Here it will be called S3. An idempotent quasigroup that fulfils this law will be called an *S3-quasigroup*.

Perfect cyclic designs (now *perfect Mendelsohn designs*, PMD) were defined in 1977 by N. S. Mendelsohn [6]. The PMDs that are of concern here are of length four. A PMD$(v, 4)$ is a partition of an oriented complete graph on v elements into oriented 4-cycles (called *blocks*) such that diagonals of these 4-cycles partition the unoriented complete graph. A simple example over integers modulo 5 are the five 4-cycles $(i, i + 1, i + 3, i + 2)$.

There are two ways how to describe a PMD$(v, 4)$ algebraically as a quasigroup. One option [6] is to set $ab = c$ whenever (a, b, c, d) is a block. Proceeding along edges of the block yields the identity $(xy)(y(xy)) = x$. This law will be called M4, and an idempotent quasigroup satisfying this law will be called an *M4-quasigroup*. Each such quasigroup uniquely determines blocks of a PMD$(v, 4)$.

Another option [1] is to set $ac = b$, for any block (a, b, c, d). This yields an S3-quasigroup, and each S3-quasigroup also describes a PMD$(v, 4)$.

Dudek and Monzo [3] recently observed that any idempotent medial binary operation that satisfies the S3 law has to be a quadratical quasigroup. The present

2010 *Mathematics Subject Classification.* 05B05, 20N10.

Key words and phrases. Perfect Mendelsohn design; quadratical quasigroup; Third Stein's law; toroidal grid; Second Schoöder's law.

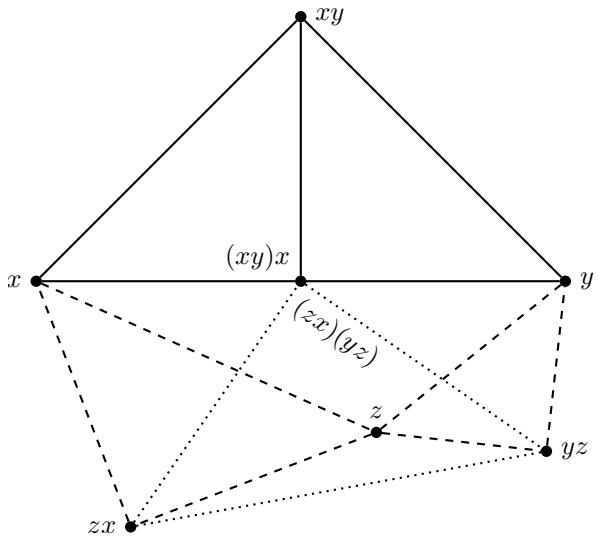

FIGURE 1. An illustration of the quadratical law $(xy)x = (zx)(yz)$ for the operation in the Euclidean plane.

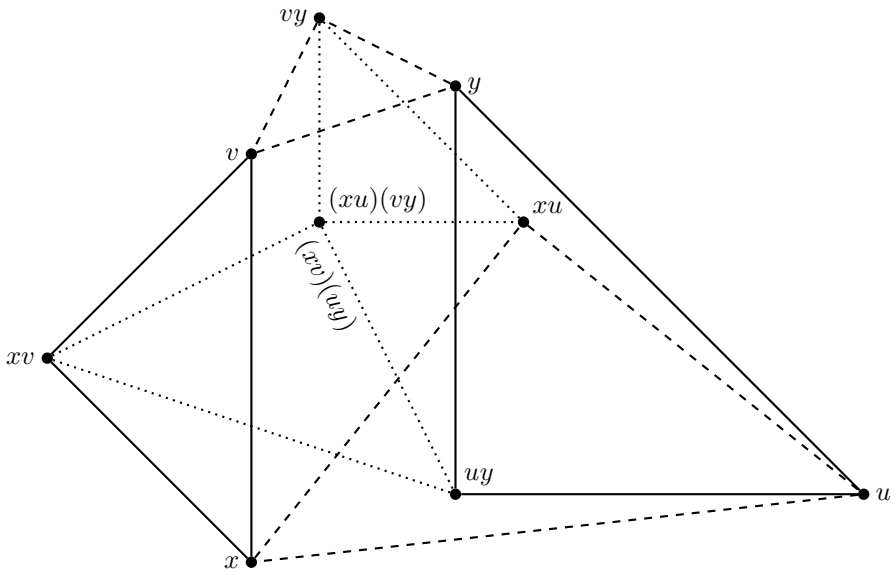

FIGURE 2. An illustration of the medial law $(xu)(vy) = (xv)(uy)$ for the operation in the Euclidean plane.

paper puts their results into a broader context of PMD$(v, 4)$s, shows how a certain class of PMD$(v, 4)$s is connected to toroidal grids, and uses this connection to answer some of the open questions posed by Dudek and Monzo [3, 4]. Main ingredients are the complete classification of finite quadratical quasigroups and concepts induced by the notion of *centred* PMD$(v, 4)$ that was defined in [5].

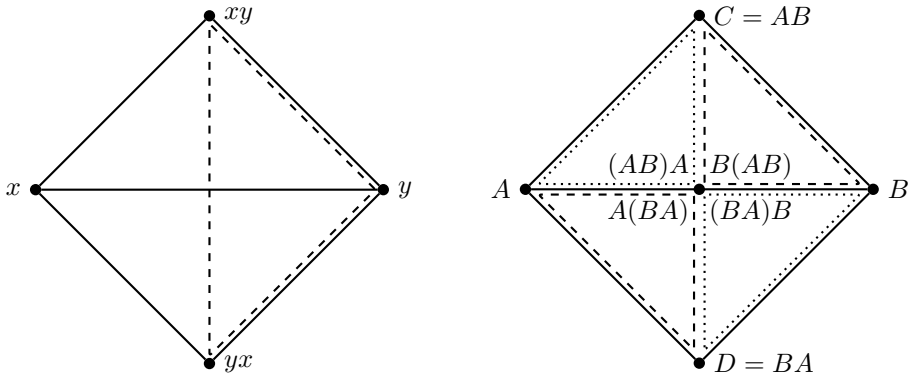

FIGURE 3. An illustration of the Third Stein's law $(xy)(yx) = y$ for the operation in the Euclidean plane (left) and an illustration of the geometrical center of the square (A, C, B, D) being equal to $(AB)A = A(BA) = B(AB) = (BA)B$ (right).

The operation of the initial example yields a quadratical quasigroup. Hence it is an S3-quasigroup, and so it induces a PMD$(v, 4)$. If $AB = C$ and $BA = D$, then (A, C, B, D) is a block. This block is a square in the euclidean plane. In fact, blocks of the PMD$(v, 4)$ are exactly all clockwise oriented squares of the plane. The geometrical centre of the square (A, C, B, D) is equal to $(AB)A = A(BA) = B(AB) = (BA)B$, see Fig. 3.

Volenec [12] defined a *square* as an oriented 4-cycle (a, ab, b, ba) for any $a, b \in Q$, $a \neq b$, Q a quadratical quasigroup. In this way he obtained the associated PMD$(v, 4)$ of Q without making an explicit reference to PMDs. He also noted [12] that the *centre* of (a, ab, b, ba) may be defined without introducing a geometrical context as $(ab)a$ since the quadratical law implies $(ab)a = a(ba) = b(ab) = (ba)b$. As we shall observe, this definition may be used for all S3-quasigroups that fulfil the *flexible law* $x(yx) = (xy)x$. (This identity is also known as the *elastic law*. Another ambiguity in nomenclature concerns the *medial law* $(xy)(uv) = (xu)(yv)$, which is often called *entropic*.)

Volenec and his collaborators have focused upon algebraic proofs of theorems from planar geometry [13, 14], and have not investigated finite models of quadratical quasigroups. That seems to be one of reasons why the connection to PMD$(v, 4)$s was not utilized earlier. This paper seems to be the first in which this connection is stated explicitly.

The investigation of finite models was initiated by Dudek [2], and continued in [3, 4]. Those papers show how finite quadratical quasigroups can be constructed, but fall short of complete classification. Such a classification appears in Section 3.

Section 1 describes how Law S3 interacts with Law M4, and with the Second Schröder's Law $xy \cdot yx = x$. Section 2 investigates properties of flexible S3 operations and connections between the medial and the quadratical law. Amongst others it shows that an idempotent quadratical operation is always a quasigroup. Section 3 classifies finite quadratical quasigroups and explains that some of the finite quadratical quasigroups discussed in [2] and [3] as separate examples are in fact isomorphic.

A quadratical quasigroup is isomorphic to its mirror image if and only if the associated PMD design is isomorphic to its converse. Section 3 finishes by describing finite quadratical quasigroups that possess this quality.

Section 4 establishes the notion of a k-regular PMD$(v, 4)$ and shows that the centred PMD$(v, 4)$s (those that can be obtained from a flexible S3-quasigroup) are 4-regular and satisfy an additional condition. It also explains how 4-regular PMDs are connected to toroidal grids, and shows that every such PMD may be seen as a union of components, each of which is a toroidal grid.

Section 5 describes the structure of a toroidal grid that appears as a component of the PMD induced by a quadratical quasigroup. Section 6 starts by showing that each component may be transformed into another component by a process called skew expansion. This is then used to answer several problems formulated by Dudek and Monzo [4].

1. Laws

Let $\cdot$ be a binary operation upon a set Q. For $a \in Q$ denote by L_a the *left translation* $x \mapsto ax$, and by R_a the *right translation* $x \mapsto xa$. Say that $(Q, \cdot)$ is a *left quasigroup* if each L_a permutes Q. Similarly, $(Q, \cdot)$ is a *right quasigroup* if all right translations are permutations. Call $(Q, \cdot)$ a *quasigroup* if it is both a left and right quasigroup.

In a left quasigroup define the *left division* $x\backslash y = L_x^{-1}(y)$. Then $x(x\backslash y) = y$ and $x\backslash(xy) = y$, and these identities can be used to define left quasigroups alternatively as algebras with two operations in which these two identities hold. Right quasigroups satisfy $(y/x)x = y = (yx)/x$, where $y/x = R_x^{-1}(y)$.

Our first aim is to show that Q has to be a quasigroup if it is (a) a left or right quasigroup which satisfies the S3 law $(xy)(yx) = y$ or (b) a left quasigroup which satisfies the M4 law $(xy)(y(xy)) = x$. We shall also observe that if Q is a left quasigroup, then it satisfies S3 if and only if the left division satisfies M4, and reversely.

In the following an explicit occurrence of the operation symbol $\cdot$ will be used to indicate the precedence. Thus $(x \cdot yz)(xy \cdot z)$ is the same as $(x(yz))((xy)z)$.

Proposition 1.1. *Let $\cdot$ be a binary operation upon a set Q.*

(i) *If $\cdot$ satisfies M4, then $(Q, \cdot)$ is a right quasigroup and $(Q, /)$ satisfies M4 too.*

(ii) *The operation $\cdot$ satisfies M4 if and only if it satisfies*

$$(y \cdot xy)x = y. \tag{M4'}$$

Proof. If M4 holds, then $(y \cdot xy)x = (y \cdot xy)(xy \cdot (y \cdot xy))$. Set $z = xy$. By M4, $(y \cdot xy)x = yz \cdot (z \cdot yz) = y$. Hence M4 $\Rightarrow$ M4'.

Let $\cdot$ satisfy M4'. The law implies that each R_x is an onto mapping. To prove that R_y is a permutation assume that $x_1y = x_2y$. Set $a = y \cdot x_1y = y \cdot x_2y$. By M4', $ax_1 = y = ax_2$. Furthermore, $x_1 \cdot ax_1 = x_1y = x_2y = x_2 \cdot ax_2$. Thus $x_1 = (x_1 \cdot ax_1)a = (x_2 \cdot ax_2)a = x_2$. We have proved that $(Q, \cdot)$ is a right quasigroup. Now we shall show that this right quasigroup fulfils M4. Choose $x, y \in Q$ and put $a = y \cdot xy$ and $b = xy$. By M4', $(a \cdot ba)b = a$. This expands to

$$((y \cdot xy)((xy) \cdot (y \cdot xy))) \cdot xy = y \cdot xy.$$

By right cancellation $y = (y \cdot xy)(xy \cdot (y \cdot xy))$. This gives M4 since for all $y, z \in Q$ there exists $x \in Q$ such that $z = xy$.

Write $(y \cdot xy)x = y$ as $y = (y/x)/(xy)$. Replacing x by x/y yields $y = (y/(x/y))/x$. Thus $(Q, \cdot)$ satisfies M4' if and only if $(Q, /)$ satisfies M4'. □

Corollary 1.2. *Left quasigroups that fulfil M4 are quasigroups.*

Proposition 1.3. *If a left quasigroup $(Q, \cdot)$ satisfies one of the laws S3 and M4, then the left quasigroup $(Q, \backslash)$ satisfies the other law, and vice versa.*

Proof. Let us first prove that $(Q, \cdot)$ fulfils S3 if and only if $(Q, \backslash)$ fulfils M4. Now, $xy \cdot yx = y$ is equivalent to $yx = (xy)\backslash y$, and thus to $x = y\backslash((xy)\backslash y)$. Replacing y by $x\backslash y$ yields $x = (x\backslash y)\backslash(y\backslash(x\backslash y))$. Thus $(Q, \backslash)$ really fulfils M4. Nothing more is needed since in each left quasigroup $(Q, \cdot)$ the multiplication can be interpreted as the left division of the left quasigroup $(Q, \backslash)$. Hence $(Q, \backslash)$ satisfies S3 if and only if $(Q, \cdot)$ satisfies M4. □

Proposition 1.4. *Let $\cdot$ be a binary operation upon a set Q. If $\cdot$ satisfies S3, then $(Q, \cdot)$ is a left quasigroup if and only if it is a right quasigroup. If this is true, then $x\backslash(y\backslash x) = (y\backslash x)y = y/x$ and $(x/y)/x = y(x/y) = x\backslash y$ for all $x, y \in Q$.*

Proof. Suppose that $(Q, \cdot)$ is a left quasigroup that satisfies S3. If $xa = b$, then $a = b \cdot ax$, and $x = a\backslash(b\backslash a)$. Therefore the equation $xa = b$ possesses at most one solution. On the other hand, such a solution always exists and is equal to $(b\backslash a)b$ since $((b\backslash a)b)(b(b\backslash a)) = b$, by the S3 law. Hence $a\backslash(b\backslash a) = (b\backslash a)b$ for all $a, b \in Q$. The rest can be obtained by a mirror argument. □

It seems necessary to point out that in [11] Volenec has claimed to study right quasigroups that satisfy the *quadratical law* $xy \cdot x = zx \cdot yz$. However, his definition of a right quasigroup coincides with the prevailing definition of a left quasigroup. The following statement explains why this could not have caused a confusion:

Lemma 1.5. *Suppose that a binary operation $\cdot$ upon Q fulfils the quadratical law $xy \cdot x = zx \cdot yz$. If $\cdot$ is idempotent, then it satisfies the law S3. Furthermore, $(Q, \cdot)$ is a left quasigroup if and only if it is a right quasigroup. If $(Q, \cdot)$ is a quasigroup, then $xx = x$ for all $x \in Q$.*

Proof. Let $\cdot$ be quadratical. If it is idempotent, then $zx \cdot xz = xx \cdot x = x$ for all $x, z \in Q$. If $\cdot$ satisfies S3, then $(Q, \cdot)$ is a left quasigroup if and only if it is a right quasigroup, by Proposition 1.4. If $(Q, \cdot)$ is a left quasigroup, then $xx \cdot x = xx \cdot xx$ yields $xx = x$, for all $x \in Q$. Hence left quadratical quasigroups satisfy S3, and it remains to show that right quadratical quasigroups satisfy S3 as well. For that it suffices to show that they are idempotent.

Let $(Q, \cdot)$ be a right quadratical quasigroup. Then $zx \cdot xz = xx \cdot x$ for all $x, z \in Q$. Thus $xx \cdot xx = xx \cdot x = (xx \cdot x)(x \cdot xx) = (xx \cdot xx) \cdot (x \cdot xx) = (xx \cdot x) \cdot xx$. By cancellation, $xx = xx \cdot x$ and $x = xx$. □

Proposition 1.3 has the following immediate consequence:

Corollary 1.6. *A quasigroup $(Q, \cdot)$ is an S3-quasigroup if and only if $(Q, \backslash)$ is an M4-quasigroup. Similarly, $(Q, \cdot)$ is an M4-quasigroup if and only if $(Q, \backslash)$ is an S3-quasigroup.*

PMD$(v, 4)$s thus correspond to both M4- and S3-quasigroups. Of course, a decomposition of a complete oriented graph into 4-cycles may be associated with an idempotent binary operation that satisfies law M4 even when the decomposition is not perfect. Without giving details let it be remarked that this connection can be made one-to-one if the M4 operation is assumed to be *strongly idempotent*, i.e. if $x \in \{xy, yx\} \Leftrightarrow x = y$, for all $x, y \in Q$.

The rest of this section describes a combinatorial interpretation of strongly idempotent S3 operations. This may be regarded as a digression from the main line of the paper. It explains the relationship of idempotent S3 operations to quasigroups. There are conditions, like mediality, that force an idempotent S3 operation to be a quasigroup. However, non-quasigroup idempotent S3 operations exist. The construction described below shows how to interpret strongly idempotent S3 operations combinatorially, and establishes a connection between the S3 Law $(xy)(yx) = y$ and the Second Schröder's Law $(xy)(yx) = x$.

Define a *2,2-partition* upon a set Q as a collection $\mathcal{C}$ of unordered pairs $\{A, B\}$, where A and B are 2-element subsets of Q, $A \cap B = \emptyset$, such that for each 2-element subset $X \subseteq Q$ there exists exactly one $\{A, B\} \in \mathcal{C}$ for which $X \in \{A, B\}$. The simplest example is upon four elements, with two pairs formed by parallel sides of a square, and one pair by the diagonals.

An *ordering* of $\{A, B\}$ is any pair (α, β), where $\alpha = (\alpha_1, \alpha_2) \in Q^2$, $\beta = (\beta_1, \beta_2) \in Q^2$, and either $A = \{\alpha_1, \alpha_2\}$, $B = \{\beta_1, \beta_2\}$, or $A = \{\beta_1, \beta_2\}$, $B = \{\alpha_1, \alpha_2\}$. Put $\alpha^{op} = (\alpha_2, \alpha_1)$. Let $\sim$ be the least equivalence upon the orderings of $\{A, B\}$ such that $(\alpha, \beta) \sim (\beta^{op}, \alpha)$. This splits the orderings into two classes, one of which consists of (α, β), $(\alpha^{op}, \beta^{op})$, (β, α^{op}) and (β^{op}, α). Choosing one of the two classes will be regarded as a choice of *orientation* of $\{A, B\}$. An orientation is fully determined by any of its representatives. An *oriented 2,2-partition* is a 2,2-partition in which an orientation is chosen for each of its elements. An oriented 2,2-partition can be presented by a collection of pairs $((a_1, a_2), (a_3, a_4))$ such that the collection of sets $\{\{a_1, a_2\}, \{a_3, a_4\}\}$ is the 2,2-partition, and $((a_1, a_2), (a_3, a_4))$ represents the orientation chosen for $\{\{a_1, a_2\}, \{a_3, a_4\}\}$.

Suppose that $\mathcal{O}$ is an oriented 2,2-partition upon a set Q. Define an idempotent binary operation upon Q in such a way that if $\{\{x, y\}, \{u, v\}\}$ is a partition element and $((x, y), (u, v))$ is a representative of its ordering, then

$$xy = u, \quad yx = v, \quad uv = y \text{ and } vu = x.$$

The definition does not depend upon the choice of a representative since the same values are obtained if $((v, u), (x, y))$ is chosen. The operation is said to be *induced by* $\mathcal{O}$. It satisfies law S3 since $(xy)(yx) = uv = y$. It is also clear that $x \in \{xy, yx\} \Leftrightarrow x = y$, for all $x, y \in Q$.

Proposition 1.7. *Let $\cdot$ be a binary idempotent operation upon Q that fulfils law S3. If $xy = x$ implies $x = y$ for all $x, y \in Q$, then the operation is induced by a (unique) oriented 2,2-partition upon Q.*

Proof. Suppose that $xy = x$ implies $x = y$ for all $x, y \in Q$. Let $x, y \in Q$ be such that $yx = x$. Then $x = yx \cdot xy = x \cdot xy$. Hence $x = xy$ and $x = y$. It can be thus assumed that $\cdot$ is strongly idempotent. The set of all $\{\{x, y\}, \{xy, yx\}\}$ is a 2,2-partition since $y = xy \cdot yx$ and $x = yx \cdot xy$. Each element of the partition may be oriented as $((x, y), (xy, yx))$ since all other representatives of the same orientation, i.e. $((y, x), (yx, xy))$, $((yx, xy), (x, y))$ and $((xy, yx), (y, x))$, are of the

form $((a,b),(ab,ba))$ too. The operation induced by such an orientation coincides with $\cdot$, the given operation. □

The smallest nontrivial S3-quasigroup is upon a set of 5 elements. Nevertheless, upon a 4-element set there exists a strongly idempotent S3 operation since $\{\{1,2\},\{3,4\}\}$, $\{\{1,3\},\{2,4\}\}$, $\{\{1,4\},\{2,3\}\}$ is a 2,2-partition of $\{1,2,3,4\}$.

If Q is a nontrivial S3-quasigroup, $\mathcal{O}$ is the induced oriented 2,2-partition, and $\mathcal{O}'$ is obtained from $\mathcal{O}$ by a change of orientation in exactly one element of the partition, then $\mathcal{O}'$ induces an S3 operation that cannot be a quasigroup as in each row of the multiplication table a change occurs in at most one cell.

For some 2,2-partitions there exists no orientation that yields an S3-quasigroup. This is because in the quasigroup case for all $a,b \in Q$, $a \neq b$, there has to exist a partition element $\{\{x,y\},\{u,v\}\}$ such that $a \in \{x,y\}$ and $b \in \{u,v\}$. Constructing 2,2-partitions that do not satisfy such a property is easy. For example, consider a cube with sides $\mathcal{A} = (A_1, A_2, A_3, A_4)$ and $\mathcal{B} = (B_1, B_2, B_3, B_4)$, and edges $\{A_i, B_i\}$, $1 \leq i \leq 4$. Define a 2,2-partition so that it contains (1) parallel edges and diagonals of both $\mathcal{A}$ and $\mathcal{B}$, (2) diagonals of the four remaining sides, and (3) diagonals and parallel edges connecting $\mathcal{A}$ and $\mathcal{B}$ in (A_1, B_1, B_3, A_3) and (A_2, B_2, B_4, A_4). Then, say, for $a = A_1$ and $b = B_2$ there exists no partition element $\{\{x,y\},\{u,v\}\}$ such that $a \in \{x,y\}$ and $b \in \{u,v\}$.

A *symmetric orientation* of a 2,2-partition element is defined by an equivalence $\approx$ such that $(\alpha,\beta) \approx (\beta,\alpha)$ and $(\alpha,\beta) \approx (\alpha^{op},\beta^{op})$. The class of $((x,y),(u,v))$ thus consists of $((x,y),(u,v))$, $((u,v),(x,y))$, $((y,x),(v,u))$ and $((v,u),(y,x))$. Suppose that $\mathcal{S}$ is a 2,2-partition in which for every element there has been chosen a symmetric orientation. Define an operation $\cdot$ by

$$xy = u, \quad yx = v, \quad uv = x \text{ and } vu = y.$$

It is clear that the definition does not depend upon the choice of the representative, that the operation fulfils the identity $(xy)(yx) = x$ and that it is strongly idempotent. The operation is said to be *induced by symmetrically oriented 2,2-partition* $\mathcal{S}$.

Proposition 1.8. *Let Q be a set. Each strongly idempotent binary operation upon Q that fulfils the Second Schröder's Law $xy \cdot yx = x$ is induced by a (unique) symmetrically oriented 2,2-partition upon Q.*

Proof. Define the 2,2-partition as the set of all $\{\{x,y\},\{xy,yx\}\}$ and choose the symmetric orientation $((x,y),(xy,yx))$, for all $x,y \in Q$. □

Smith [8] has been concerned with similarities between Third Stein's Law and Second Schröder's Law as well. However, his viewpoint is different. He has suggested to call the Third Stein's Law *outer palindromic* and the Second Schröder's Law *inner palindromic*.

2. Flexibility

Lemma 2.1. *Let $\cdot$ be an S3 operation upon Q. For all $(a,b) \in Q^2$ there exists a unique $(x,y) \in Q^2$ such that $a = xy$ and $b = yx$.*

Proof. If $a = xy$ and $b = yx$, then $x = ba$ and $y = ab$. □

Lemma 2.2. *Let $\cdot$ be an S3 operation upon Q. Let $a,b,x,y \in Q$ be such that $a = xy$ and $b = yx$. Then $a \cdot ba = ab \cdot a$ if and only if $xy \cdot x = y \cdot xy$.*

Proof. Indeed, $a \cdot ba = a \cdot x = xy \cdot x$ and $ab \cdot a = y \cdot xy$. □

An operation $\cdot$ upon Q is called *strongly flexible* (strongly elastic) if $x \cdot yx = xy \cdot x = y \cdot xy$ for all $x, y \in Q$. Of course, then also $yx \cdot y = x \cdot yx$.

Lemmas 2.1 and 2.2 directly imply the following fact.

Corollary 2.3. *An S3 operation is flexible if and only if it is strongly flexible.*

Lemma 2.4. *Let Q be an M4-quasigroup. Then $x \cdot yx = xy \cdot x$ if and only if $(a\backslash b)\backslash a = b\backslash(a\backslash b)$, where $a = xy$ and $b = xy \cdot x$.*

Proof. Clearly, $(a\backslash b)\backslash a = y$. Hence $(a\backslash b)\backslash a = b\backslash(a\backslash b)$ if and only if $by = x$. This is the same as $x/y = xy \cdot x$. By Proposition 1.1, $x/y = x \cdot yx$. □

By coupling Lemmas 2.1, 2.2 and 2.4 with Proposition 1.3 it is immediately clear that if there are considered pairs (x, y) that satisfy the flexible law, then there is a bijection between such pairs in an M4-quasigroup $(Q, \cdot)$ and the S3-quasigroup $(Q, \backslash)$. In particular:

Corollary 2.5. *An M4-quasigroup $(Q, \cdot)$ is flexible if and only if the S3-quasigroup $(Q, \backslash)$ is flexible.*

Lemma 2.6. *Let $(Q, \cdot)$ be a strongly flexible quasigroup. Put $x \bullet y = xyx$ for all $x, y \in Q$. Then $(Q, \bullet)$ is a commutative flexible quasigroup.*

Proof. If $x \bullet y = z$, then $y = (x\backslash z)/x$. The operation $\bullet$ is commutative since $\cdot$ is strongly flexible. □

Let (x_1, x_2, x_3, x_4) be a block of a PMD$(v, 4)$. Say that z is the *centre* of the block if there exist y_i such that (x_{i+1}, z, x_i, y_i) is a block for each i, $1 \leq i \leq 4$ (indices are counted modulo 4). A PMD$(v, 4)$ is said to be *centred* if each block possesses a centre.

Proposition 2.7. *Suppose that a* PMD$(v, 4)$ *is determined by an S3-quasigroup or an M4-quasigroup. The PMD is centred if and only if the quasigroup is flexible.*

Proof. By Corollaries 1.6 and 2.5 it may be assumed that the PMD is determined by an S3-quasigroup. Consider a block (x, xy, y, yx). The block is centred if and only if there exists z such that $z = xy \cdot x = y \cdot xy = yx \cdot y = x \cdot yx$. The result thus follows from Corollary 2.3. □

If a PMD$(v, 4)$ is given by a flexible S3-quasigroup $(Q, \cdot)$, then the centre of a block (x, xy, y, yx) can be expressed as $x \bullet y$. Thus, by Lemma 2.6, for each $x, z \in Q$, $x \neq z$, there exists exactly one block with centre z that carries x.

Proposition 2.7 appears in [5] as Theorem 3.3. In centred PMDs the squares possess a structure that locally agrees with the structure of squares induced by a quadratical quasigroup, cf. Corollary 4.13.

The rest of this section is concerned with the connection of the S3 law to the medial law and the quadratical law.

Theorem 2.8. *Let $\cdot$ be a binary operation upon Q that satisfies the quadratical law $xy \cdot x = zx \cdot yz$. The following are equivalent:*

(i) *$(Q, \cdot)$ is a left quasigroup;*
(ii) *$(Q, \cdot)$ is a right quasigroup;*
(iii) *$xx = x$ for all $x \in Q$; and*

(iv) $xy \cdot yx = y$ *for all* $x, y \in Q$.

If these conditions hold, then $(Q, \cdot)$ *is a flexible quasigroup in which*

$$y/x = (x \cdot xy)(xy \cdot y) \cdot (xy \cdot y) \text{ and } x\backslash y = (y \cdot yx) \cdot (y \cdot yx)(yx \cdot x),$$

for all $x, y \in Q$.

Proof. By Lemma 1.5, (i) $\Leftrightarrow$ (ii), (ii) $\Rightarrow$ (iii) and (iii) $\Rightarrow$ (iv). It remains to prove (iv) $\Rightarrow$ (i) and to verify the division formulas. The first step is a proof of (iv) $\Rightarrow$ (iii).

Suppose that $\cdot$ fulfils both the quadratical law and the S3 law. Then $xx \cdot x = xx \cdot xx = x$, and so $xx = (x \cdot xx)(xx \cdot x) = (x \cdot xx)x = xx \cdot (xx \cdot x) = xx \cdot x = x$. Thus (iii) $\Leftrightarrow$ (iv). Hence $\cdot$ may be assumed to be both idempotent and fulfilling S3. Therefore it is also flexible, as $xy \cdot x = xx \cdot yx = x \cdot yx$. By Corollary 2.3, $zx \cdot yz = x \cdot yx = yx \cdot y = zy \cdot xz$ for all $x, y, z \in Q$. That makes the assumptions mirror symmetric. If $zx = zy$, then $y = zy \cdot yz = zx \cdot yz = xyx = yxy = zy \cdot xz = zx \cdot xz = x$. The operation $\cdot$ is thus cancellative.

Consider $x, y \in Q$ and put $a = (x \cdot xy)(xy \cdot y) \cdot (xy \cdot y)$. We first show that it suffices to prove that $yay = xy \cdot y$. Let the latter be true. Then $ya = xy$, $y \cdot ya = yxy = ax \cdot ya$, and so $y = ax$, by cancellation.

To prove $yay = xy \cdot y$ it thus suffices to find z such that $za \cdot yz = xy \cdot y$. Set $z = xy{\cdot}y$. Then $za = (xy{\cdot}y)(x{\cdot}xy)(xy{\cdot}y){\cdot}(xy{\cdot}y) = (y{\cdot}xy)(xy{\cdot}y){\cdot}(xy{\cdot}y) = xy{\cdot}(xy{\cdot}y)$, and $za \cdot yz = (xy \cdot (xy \cdot y))((xy \cdot y) \cdot xy) = xy \cdot y$. □

Formulas for y/x and $x\backslash y$ occurring in Theorem 2.8 are not new. They are taken from [11]. What is new is the fact that the quadratical law plus idempotency forces the quasigroup property.

Lemma 2.9. *Let* $(Q, \cdot)$ *be a strongly flexible quasigroup. Then* $xy = (y\backslash x)x = y(y/x)$, *for all* $x, y \in Q$.

Proof. Indeed, $xy = y(y\backslash x)y = (y\backslash x)y(y\backslash x) = (y\backslash x)x$. The other case is mirror symmetric. □

The next two statements are proved for the sake of completeness. The first of them coincides with [11, Theorems 2 and 3] and the second with [3, Theorem 2.14].

Theorem 2.10. *Each quadratical quasigroup is idempotent medial. It also fulfils the law* $x\backslash(yz) = (zx)/y$.

Proof. Let $(Q, \cdot)$ be a quadratical quasigroup. By Theorem 2.8, $(Q, \cdot)$ is a flexible S3-quasigroup, and thus strongly flexible. The first step is to prove left distributivity. By Lemma 2.9, $xy \cdot xz = xy \cdot ((z\backslash x)x) = z(z\backslash x) \cdot yz = x \cdot yz$. Thus $x \cdot yz = z(z\backslash(xy)) \cdot xz = x(z\backslash(xy))x$. Hence $yz = (z\backslash(xy))x$ and $(yz)/x = z\backslash(xy)$. Now, $xy \cdot uv = v(v\backslash(xy)) \cdot uv = xu \cdot (v\backslash(xy))x = xu \cdot ((yv)/x)x = xu \cdot yv$. □

Theorem 2.11. *Let* $\cdot$ *be an idempotent medial operation upon* Q *that satisfies the Third Stein's Law* $xy \cdot yx = y$. *Then* $(Q, \cdot)$ *is a quadratical quasigroup.*

Proof. By Theorem 2.8 it is enough to prove that the operation satisfies the quadratical law. An idempotent medial operation is both left distributive and flexible. Thus $zx \cdot yz = (zx \cdot y)(zx \cdot z) = (zx \cdot y)(xz \cdot x) = (zx \cdot xz) \cdot yx = x \cdot yx = xy \cdot x$, by Corollary 2.3. □

Corollary 2.12. *A quasigroup is quadratical if and only if it is a medial S3-quasigroup.*

Proof. If it is quadratical, use Theorems 2.8 and 2.10. The converse follows from Theorem 2.11. □

3. Classification of finite quadratical quasigroups

Lemma 3.1. *A quasigroup $(Q,\cdot)$ is medial if and only if $(Q,\backslash)$ is medial.*

Proof. Let x,y,u,v be elements of Q. To prove $(x\backslash y)\backslash(u\backslash v) = (x\backslash u)\backslash(y\backslash v)$ means to show that $v = u((x\backslash y)((x\backslash u)\backslash(y\backslash v))$. Define $b,c,d \in Q$ by $u = xd$, $y = xc$ and $v = (xc)(db)$. We thus want to prove that $(xc)(db) = (xd)(c\cdot(d\backslash(db)) = (xd)(cb)$. That is an instance of the medial law, and thus true. □

Another proof of Lemma 3.1 may be obtained by Toyoda's theorem which couples medial quasigroups with abelian groups.

In the rest of this section quasigroup operations will be denoted by $*$ or $\star$ to avoid confusion with structures that are used in their definition.

By Toyoda's theorem [10] each medial quasigroup operation $*$ can be obtained from an abelian group $(G,+)$, commuting automorphisms $\alpha,\beta \in \mathrm{Aut}(G)$ and an element $c \in G$ so that $x*y = \alpha(x)+\beta(y)+c$. Clearly, the operation $*$ is idempotent if and only if $c = 0$ and $\alpha+\beta = \mathrm{id}_G$.

The latter condition can be expressed by saying that α is a fixed-point free automorphism of G (i.e. $\alpha - \mathrm{id}_G$ permutes G). If $*$ is idempotent, then $x*y = \alpha(x-y)+y$, and $x*y*x = (x*y)*x = x*(y*x) = \alpha(\alpha(x-y)+y-x)+x = \alpha(\alpha-\mathrm{id}_G)(x-y)+x$.

Theorem 3.2. *Let α be a fixed point free automorphism of an abelian group $(G,+)$. Set $x*y = \alpha(x-y)+y$ for all $x,y \in G$. The following are true:*

(i) *If G contains an involution (i.e., an element of order 2), then $(G,*)$ is neither an M4-quasigroup nor an S3-quasigroup.*
(ii) *$(G,*)$ is an M4-quasigroup if and only if $\alpha^2 = -\mathrm{id}_G$. All medial M4-quasigroups can be expressed in this way.*
(iii) *$(G,*)$ is an S3-quasigroup if and only if $(\alpha^{-1}-\mathrm{id}_G)^2 = -\mathrm{id}_G$ (equivalently, $2\alpha^2 - 2\alpha + \mathrm{id}_G = 0$). All medial S3-quasigroups can be expressed in this way.*

Proof. Let us first discuss the structure of medial M4-quasigroups. By Proposition 1.1 it is enough to decide when $(x*y*x)*y = x$ holds for all $x,y \in G$. Since $(x*y*x)*y = \alpha(\alpha(\alpha-\mathrm{id}_G)(x-y)+x-y)+y = \alpha^2(\alpha-\mathrm{id}_G)(x-y)+\alpha(x-y)+y$, there is $(x*y*x)*y = x$ if and only if $(\alpha-\mathrm{id}_G)(\alpha^2+\mathrm{id}_G) = 0$. This is the same as $\alpha^2 = -\mathrm{id}_G$ since $\alpha-\mathrm{id}_G$ is a permutation. If $\alpha^2 = -\mathrm{id}_G$ and $2x = 0$, then $\alpha^2(x) = x$ and $x = 0$ because $(\alpha-\mathrm{id}_G)^2(x) = (\alpha-\mathrm{id}_G)(\alpha(x)-x) = 2x-\alpha(2x) = 0$. Let us now turn to S3-quasigroups. By direct computation, $(x*y)*(y*x) = y$ if and only if $\alpha(2\alpha(x-y)+(y-x))+\alpha(y-x)+x = y$, and that is the same as $2\alpha^2-2\alpha+\mathrm{id}_G = 0$. Hence $2x = 0$ implies $x = 0$. To finish, note that $2\alpha^2-2\alpha+\mathrm{id}_G = 0$ if and only if $(\alpha^{-1}-\mathrm{id}_G)^2 = -\mathrm{id}_G$. □

Abelian groups with no involution are often called *uniquely 2-divisible* since they satisfy the implication $2x = 2y \Rightarrow x = y$. A stronger condition is that $x \mapsto 2x$ is a permutation of G. As we shall see this condition has to hold if G can give rise to

a medial M4- or S3-quasigroup. If this condition holds and $x, y \in G$, then $2x = y$ will be often written as $y = x/2$.

Lemma 3.3. *Let α be a fixed point free automorphism of an abelian group $(G, +)$. Let $\backslash$ be the left division of the quasigroup $x * y = \alpha(x - y) + y$. Then $x\backslash y = \beta(x - y) + y$, where $\beta = (\alpha - \mathrm{id}_G)^{-1} + \mathrm{id}_G$.*

Proof. Express $x * y$ as $(\alpha - \mathrm{id}_G)(x - y) + x$. Now,

$$\begin{aligned} x * (\beta(x - y) + y) &= x * ((\alpha - \mathrm{id}_G)^{-1}(x - y) + x) \\ &= (\alpha - \mathrm{id}_G)(-(\alpha - \mathrm{id}_G)^{-1}(x - y)) + x = (y - x) + x = y. \end{aligned}$$

□

By Corollary 1.6, Lemma 3.3 may be used to pass between medial S3-quasigroups and medial M4-quasigroups.

Idempotent medial S3-quasigroups are exactly the quadratical quasigroups, by Theorems 2.10 and 2.11. The S3 part of Theorem 3.2 appeared in an equivalent form in [2], and, essentially, already in [11]. Nevertheless, a complete classification of finite quadratical quasigroups does not seem to have been published (while [2] and [3] contain many examples). As we shall see such a classification is easy to provide when the multiplication is replaced by the left division, i.e., when the law S3 is replaced by the law M4. This is because the condition $\alpha^2 = -\mathrm{id}_G$ is easier to handle than the condition $2\alpha^2 - 2\alpha + \mathrm{id}_G = 0$.

Suppose that $(G_i, +)$ is an abelian group, $i \in \{1, 2\}$, and that $(G_i, *)$ is a medial quasigroup with operation $\alpha_i(x) + \beta_i(x) + c_i$, where α_i and β_i are commuting automorphisms of $(G_i, +)$, and c_i is an element of G_i. If $(G_1, *) \cong (G_2, *)$, then $(G_1, +)$ is isotopic to $(G_2, +)$, and hence $(G_1, +) \cong (G_2, +)$, by Albert's theorem. The existence of an isomorphism $(G_1, *) \cong (G_2, *)$ can be thus reduced to the situations in which $(G_1, +) = (G_2, +)$.

The ensuing classification is based upon the following consequence of a result obtained by Stanovský and Vojtěchovský [9].

Proposition 3.4. *Let $(G, +)$ be an abelian group and let α_i be fixed point free automorphisms of $(G, +)$, $i \in \{1, 2\}$. Quasigroups $(G, *_i)$, $x *_i y = \alpha_i(x - y) + y$ for all $x, y \in G$, are isomorphic if and only if α_1 and α_2 are conjugate in $\mathrm{Aut}(G, +)$.*

Proof. Let $\alpha_i, \beta_i \in \mathrm{Aut}(G, +)$ be such that $\alpha_i\beta_i = \beta_i\alpha_i$, $i \in \{1, 2\}$. Let Q_i be the medial quasigroup with operation $\alpha_i(x) + \beta_i(y)$. By [9, Theorem 2.4], $Q_1 \cong Q_2$ if and only if there exists $\psi \in \mathrm{Aut}(G, +)$ such that $\alpha_1^\psi = \alpha_2$ and $\beta_1^\psi = \beta_2$. Thus if $\beta_i = \mathrm{id}_G - \alpha_i$, $i \in \{1, 2\}$, then $Q_1 \cong Q_2$ if and only if α_1 and α_2 are conjugate in $\mathrm{Aut}(G)$. □

An abelian group G may be regarded as a $\mathbb{Z}$-module. A pair (G, φ), $\varphi \in \mathrm{End}(G)$ may be identified with a $\mathbb{Z}[x]$-module in which $xg = \varphi(g)$ for every $g \in G$. Let us denote such a $\mathbb{Z}[x]$ module by $G[\varphi]$. If $a = \sum a_i x^i \in \mathbb{Z}[x]$, then $ag = \sum a_i \varphi^i(g)$.

Proposition 3.5. *For $i = 1, 2$ let α_i be a fixed point free automorphism of an abelian group G_i, and $Q_i = (G_i, *_i)$ the quasigroup in which $x *_i y = \alpha_i(x - y) + y$ for all $x, y \in G_i$. Then $Q_1 \cong Q_2$ if and only if $G_1[\alpha_1] \cong G_2[\alpha_2]$.*

Proof. First note that $G_1[\alpha_1] \cong G_2[\alpha_2]$ if and only if there exists $\psi\colon G_1 \cong G_2$ such that $\alpha_2\psi = \psi\alpha_1$. If $G_1 = G_2$, then the existence of such ψ is equivalent to $Q_1 \cong Q_2$, by Proposition 3.4.

In the general case both $Q_1 \cong Q_2$ and $G_1[\alpha_1] \cong G_2[\alpha_2]$ imply the existence of a group isomorphism $\gamma\colon G_1 \cong G_2$. Clearly, $\gamma\colon G_2[\alpha_2] \cong G_1[\gamma\alpha_2\gamma^{-1}]$ and $\gamma\colon Q_2 \cong (G_1, *)$, where $*$ is defined by $x * y = \gamma^{-1}\alpha_2\gamma(x - y)$, for all $x, y \in G$. Thus $G_1[\alpha_1] \cong G_2[\alpha_2] \Leftrightarrow G_1[\alpha_1] \cong G_1[\gamma\alpha_2\gamma^{-1}]$ and $Q_1 \cong Q_2 \Leftrightarrow Q_1 \cong (G_1, *)$, and the first part of the proof may be used. □

Let M be a module over a ring R. Say that $r \in R$ *acts invertibly* on M if $m \mapsto rm$ is a permutation of M (and thus an automorphism of the abelian group $(M, +)$). Note that r acts invertibly if and only if r^2 acts invertibly, and that if $s \in R$ acts invertibly, then rs acts invertibly if and only if r does. Therefore, if R is the ring of Gaussian integers $\mathbb{Z}[\mathrm{i}]$, then i always acts invertibly as $\mathrm{i}^2 = -1$, while $\mathrm{i}{-}1$ acts invertibly if and only if 2 does since $(\mathrm{i}{-}1)^2 = -2\mathrm{i}$.

Theorem 3.6. *Let M be a $\mathbb{Z}[\mathrm{i}]$-module such that 2 acts invertibly on M. Then $x * y = \mathrm{i}x + (1{-}\mathrm{i})y$ defines upon M a medial M4-quasigroup, and all medial M4-quasigroups can be obtained in this way. Furthermore, $x \star y = \big((1{-}\mathrm{i})x + (1{+}\mathrm{i})y\big)/2$ defines upon M a quadratical quasigroup, and all quadratical quasigroups can be obtained in this way.*

If N is another $\mathbb{Z}[\mathrm{i}]$-module upon which 2 acts invertibly, then $(M, *) \cong (N, *) \Leftrightarrow M \cong N \Leftrightarrow (M, \star) \cong (N, \star)$.

Proof. Consider a pair (G, α) from point (ii) of Theorem 3.2. This pair can be treated as a $\mathbb{Z}[x]$-module $G[\alpha]$. Because of the condition $\alpha^2 = -\mathrm{id}_G$, $G[\alpha]$ can be regarded as a $\mathbb{Z}[\mathrm{i}]$-module in which $\mathrm{i}g = \alpha(g)$ for all $g \in G$. If M is a $\mathbb{Z}[\mathrm{i}]$ module, then $\alpha\colon m \mapsto \mathrm{i}m$ is always an automorphism of the underlying abelian group. This automorphism is fixed point free if and only if $\mathrm{i}{-}1$ acts invertibly, i.e., if and only if 2 acts invertibly. The connection to quadratical quasigroups follows from Corollary 1.6 and Lemma 3.3. The statement about isomorphisms is a consequence of Proposition 3.5. □

If M is a $\mathbb{Z}[\mathrm{i}]$-module such that 2 acts invertibly on M, then $(M, *)$ will be called the *M4-quasigroup induced* by M, and $(M, \star)$ the *quadratical quasigroup induced* by M. Note that $M \mapsto (M, *)$ is a functor from the variety of $\mathbb{Z}[\mathrm{i}]$-modules in which 2 acts invertibly to the variety of medial M4-quasigroups. In terms of category theory the functor is essentially surjective and conservative. It is clear that it preserves products. That will be of certain importance below. Similar comments apply to the functor $M \mapsto (M, \star)$.

Proposition 3.7. *Let $n > 1$ be an odd integer. The M4-quasigroup induced by $\mathbb{Z}[\mathrm{i}]/(n)$ is isomorphic to a quasigroup upon $\mathbb{Z}_n \times \mathbb{Z}_n$ with operation*

$$(x_1, x_2) * (y_1, y_2) = (y_1 + y_2 - x_2, x_1 + y_2 - y_1). \tag{3.1}$$

The quadratical quasigroup induced by $\mathbb{Z}[\mathrm{i}]/(n)$ is isomorphic to a quasigroup upon $\mathbb{Z}_n \times \mathbb{Z}_n$ with operation

$$(x_1, x_2) \star (y_1, y_2) = \frac{1}{2}\big(x_1 + x_2 + y_1 - y_2, x_2 - x_1 + y_1 + y_2\big). \tag{3.2}$$

Proof. Indeed, $\mathrm{i}(x_1 + \mathrm{i}x_2) + (1{-}\mathrm{i})(y_1 + \mathrm{i}y_2) = (y_1 + y_2 - x_2) + \mathrm{i}(x_1 + y_2 - y_1)$ and $(1{-}\mathrm{i})(x_1 + \mathrm{i}x_2) + (1{+}\mathrm{i})(y_1 + \mathrm{i}y_2) = (x_1 + x_2 + y_1 - y_2) + \mathrm{i}(x_2 - x_1 + y_1 + y_2)$. □

Proposition 3.8. *Let $n > 1$ be an odd integer, and let $\kappa \in \mathbb{Z}_n$ be such that $n \mid \kappa^2{+}1$. Then there exists a (unique) $\mathbb{Z}[\mathrm{i}]$-module M upon $\mathbb{Z}_n$ such that $\mathrm{i}x = \kappa x$*

for each $x \in \mathbb{Z}_n$. If $a, b \in \mathbb{Z}$ are such that $a^2 + b^2 = n$ and $\gcd(a, n) = 1$, then κ may be chosen in such a way that $a\kappa \equiv b \pmod{n}$. In that case $M \cong \mathbb{Z}[\mathrm{i}]/(a + \mathrm{i}b)$.

The module M induces an M4-quasigroup with operation $x * y = \kappa x + (1-\kappa)y$. The operation of the induced quadratical quasigroup is $x \star y = \big((1-\kappa)x + (1+\kappa)y\big)/2$.

Proof. Since $\kappa^2 + 1 = 0$ is assumed to hold in $\mathbb{Z}_n$, $(\kappa^2+1)x = 0$ for all $x \in \mathbb{Z}_n$ and M is a $\mathbb{Z}[\mathrm{i}]$-module. Formulas for $x * y$ and $x \star y$ directly follow from Theorem 3.6.

Suppose that $n = a^2 + b^2$ and that $\gcd(a, n) = 1$. The condition $a\kappa \equiv b \pmod{n}$ determines κ uniquely modulo n, and such a κ satisfies $\kappa^2 + 1 \equiv 0 \pmod{n}$. The mapping $x + \mathrm{i}y \mapsto x + y\kappa$ is a surjective homomorphism $\mathbb{Z}[\mathrm{i}] \to M$ of $\mathbb{Z}[\mathrm{i}]$-modules. Denote its kernel by I. Then $x + \mathrm{i}y \in I \Leftrightarrow n \mid (ax+yb)$. Hence $a + \mathrm{i}b \in I$ and $n \in I$. To see that $I = (a + \mathrm{i}b)$ it thus suffices to show that $\mathbb{Z}[\mathrm{i}]/(a + \mathrm{i}b)$ contains at most n elements. That is clear since $\gcd(n, b) = 1$ and $n \in (a + \mathrm{i}b)$ imply that each $x + \mathrm{i}y$ is modulo $a + \mathrm{i}b$ equivalent to some $z \in \mathbb{Z}_n$. □

Denote by $\mathbb{M}_n$ and $\mathbb{S}_n$ the M4- and S3-quasigroups defined in Proposition 3.7, and by $\mathbb{M}_{n,\kappa}$ and $\mathbb{S}_{n,\kappa}$ the quasigroups of Proposition 3.8. Let n be odd. An integer κ such that $\kappa^2 + 1 \equiv 0 \pmod{n}$ exists if and only if all prime divisors of n are $\equiv 1 \pmod 4$. If $n = p^k$, $k \geq 1$ and p a prime $\equiv 1 \pmod 4$, then there are exactly two such κ. In $\mathbb{Z}_n$ they are mutually inverse. Let us assume that for each $n = p^k$ one such κ is chosen, and write $\mathbb{M}_{n,+}$ and $\mathbb{S}_{n,+}$ in these cases. Similarly, write $\mathbb{M}_{n,-}$ and $\mathbb{S}_{n,-}$ when κ^{-1} is used.

Theorem 3.9. *Each finitely generated medial M4-quasigroup is finite, and is a product of quasigroups $\mathbb{M}_{p^r}$, $p \equiv 3 \pmod 4$ a prime, $r \geq 1$, and quasigroups $\mathbb{M}_{p^r,+}$ and $\mathbb{M}_{p^r,-}$ where $p \equiv 1 \pmod 4$ is a prime and $r \geq 1$.*

Each finitely generated quadratical quasigroup is finite, and is a product of quasigroups $\mathbb{S}_{p^r}$, $p \equiv 3 \pmod 4$ a prime, $r \geq 1$, and quasigroups $\mathbb{S}_{p^r,+}$ and $\mathbb{S}_{p^r,-}$ where $p \equiv 1 \pmod 4$ is a prime and $r \geq 1$.

In both cases the components of the product determine, up to order, the isomorphism type of the quasigroup.

Proof. Because $\mathbb{Z}[\mathrm{i}]$ is a principal ideal domain, each finitely generated $\mathbb{Z}[\mathrm{i}]$-module can be expressed as $U \oplus T$, where U is a sum of finitely many copies of $\mathbb{Z}[\mathrm{i}]$, and T is the torsion part. The torsion part can be uniquely expressed as $\bigoplus T_{(\pi)}$ where π runs through a list of representatives of irreducible elements ("primes"). Each $T_{(\pi)}$ is isomorphic to a direct sum $\mathbb{Z}[\mathrm{i}]/(\pi^{r_1}) \oplus \cdots \oplus \mathbb{Z}/(\pi^{r_k})$, where $k \geq 0$ and $r_1 \geq \cdots \geq r_k \geq 1$ are uniquely determined. Of course, $k = k_\pi > 0$ for only finitely many irreducible elements π. By Theorem 3.6 only modules in which 2 acts invertibly can be used. This means that $U = 0$ and that $\pi \neq 1+i$. Hence either $\pi = p$ is a prime $\equiv 3 \pmod 4$, or $\pi = a_p \pm \mathrm{i}b_p$, where $p \equiv 1 \pmod 4$ is a prime and a_p and b_p are the uniquely determined integers such that $a_p > b_p > 0$ and $a_p^2 + b_p^2 = p$. If $n = p^r$, $r \geq 1$, and $(a_p + \mathrm{i}b_p)^r = c + \mathrm{i}d$, then $c^2 + d^2 = p^r$. Hence Propositions 3.7 and 3.8 really yield the structure of all M4- and S3-quasigroups induced by $\mathbb{Z}[\mathrm{i}]/(\pi^r)$. The rest follows from Theorem 3.6 since both constructions preserve products. □

For a finite abelian group G denote by μ_G the number of isomorphism classes of quadratical quasigroups (equivalently, medial M4-quasigroups) that are isotopic to G.

Corollary 3.10. *Let G be a nontrivial finite abelian group.*

(i) *If $G = H \times K$, H and K of coprime orders, then $\mu_G = \mu_H \mu_K$.*
(ii) *If G is a 2-group, then $\mu_G = 0$.*
(iii) *Let G be a p-group, $p \equiv 3 \pmod 4$. If there exists $H \leq G$ such that $G = H \times H$, then $\mu_G = 1$. Otherwise $\mu_G = 0$.*
(iv) *Let $G = C_1^{m_1} \times \cdots \times C_r^{m_r}$, where C_i is a cyclic group of order p^{k_i}, p a prime, $p \equiv 1 \pmod 4$, $1 \leq i \leq r$ and $k_1 > \cdots > k_r \geq 1$. Then $\mu_G = (m_1+1)\cdots(m_r+1)$.*

Proof. The structure of G is determined by the structure of a given medial M4- or S3-quasigroup, by Theorem 3.9. If $p \equiv 3 \pmod 4$, then the p-component of G has to be a square upon which the quasigroup operation is determined by (3.1) or (3.2), by Theorem 3.9 and Proposition 3.7. On the other hand, if $p \equiv 1 \pmod 4$, then each cyclic group in the decomposition of the p-component has two possibilities of choosing $\sqrt{-1}$, by Theorem 3.9 and Proposition 3.8. □

In [2, 3] the number of quadratical quasigroups isotopic to $G = \mathbb{Z}_3 \times \mathbb{Z}_3$ is said to be six. This is based on representing automorphisms of G by matrices and on enumeration of all regular matrices that correspond to the condition given in point (iii) of Theorem 3.2. However, all of the six matrices obtained yield isomorphic quasigroups.

Lists of quadratical quasigroups of certain order that appear in [2, 3, 4] should not be considered as classifications up to isomorphism, despite a suggestive wording.

The remaining part of this section is concerned with selfconverse PMD$(v, 4)$s in the setting of medial quasigroups.

Proposition 3.11. *Let H be an abelian group in which $x \mapsto 2x$ is a permutation of H. Let Q be the quasigroup defined upon $H \times H$ by formula (3.2). Then Q is a quadratical quasigroup, and $(x, y) \mapsto (y, x)$ is an isomorphism $Q \cong Q^{op}$.*

Proof. This can be proved in many ways. To couple the proof with Theorem 3.6 consider two $\mathbb{Z}[\mathrm{i}]$-modules upon $H \times H$, one with $\mathrm{i}(x_1, x_2) = (-x_2, x_1)$ and the other with $\mathrm{i}(x_1, x_2) = (x_2, -x_1)$. Then the switch $(x, y) \mapsto (y, x)$ is an isomorphism of these modules, and thus also an isomorphism of the induced quadratical quasigroups. The former module yields the quasigroup Q, by Theorem 3.6. Hence the product of (x_1, x_2) with (y_1, y_2) in the quadratical quasigroup induced by the latter module is equal to the switch of $(x_2, x_1) \star (y_2, y_1)$, where $\star$ is the operation described by (3.2) (the operation of Q). That gives $(x_1 - x_2 + y_1 + y_2, x_1 + x_2 + y_2 - y_1)$, and that is the same as $(y_1, y_2) \star (x_1, x_2)$. The product induced by the latter module thus coincides with the product of Q^{op}. □

If two PMD$(v, 4)$s are determined by S3-quasigroups Q_1 and Q_2, then the designs are isomorphic if and only if $Q_1 \cong Q_2$. This is also true if the designs are determined by M4-quasigroups.

A *converse* design is obtained from a PMD by considering each block in the reverse orientation. The relationship between quasigroups and the PMD$(v, 4)$ is clear enough to state the following facts without a proof.

Proposition 3.12. *If a* PMD$(v, 4)$ *is given by an M4-quasigroup $(Q, \cdot)$, then the converse design is given by the M4-quasigroup $(Q, /)$. If a* PMD$(v, 4)$ *is given by an S3-quasigroup Q, then the converse design is given by the S3-quasigroup Q^{op}.*

Lemma 3.13. *Let $n > 1$ be odd, and let $\kappa \in \mathbb{Z}_n$ be such that $\kappa^2 + 1 \equiv 0 \pmod n$. Then $\mathbb{S}_{n,\kappa}^{op} \cong \mathbb{S}_{n,\kappa^{-1}}$ and $\mathbb{S}_n \cong \mathbb{S}_{n,\kappa} \times \mathbb{S}_{n,\kappa^{-1}}$.*

Proof. The mapping $x \mapsto \kappa x$ is an isomorphism $\mathbb{S}^{op}_{n,\kappa} \cong \mathbb{S}_{n,\kappa^{-1}}$ since in $\mathbb{Z}_n$ both $(1-\kappa)\kappa = \kappa(1+\kappa^{-1})$ and $(1+\kappa)\kappa = \kappa(1-\kappa^{-1})$ are true. To get the other isomorphism it suffices, by Theorem 3.6, to prove that the following two $\mathbb{Z}[\mathrm{i}]$-modules upon $\mathbb{Z}_n \times \mathbb{Z}_n$ are isomorphic. In one of them, say M_1, $\mathrm{i}(x,y) = (-y,x)$. In the other module, say M_2, $\mathrm{i}(x,y) = (\kappa x, \kappa^{-1}y)$. The mapping $f\colon (x,y) \mapsto (\kappa x - y, x + \kappa^{-1}y)$ is an automorphism of the abelian group $\mathbb{Z}_n \times \mathbb{Z}_n$. Furthermore, f maps $(-y,x)$ upon $(-x-\kappa y, \kappa^{-1}x - y) = (\kappa(\kappa x - y), \kappa^{-1}(x + \kappa^{-1}y))$. Thus $f\colon M_1 \cong M_2$. □

Call a PMD$(v,4)$ *selfconverse* if it is isomorphic to the converse PMD$(v,4)$. By Proposition 3.12 this is equivalent to the existence of an isomorphism $Q \cong Q^{op}$ where Q is the S3-quasigroup that determines the design.

Proposition 3.14. *Let Q be a finite quadratical quasigroup that is isotopic to an abelian group G. Then $Q \cong Q^{op}$ if and only if Q is isomorphic to a quasigroup defined upon $H \times H$ by (3.2), where H is an abelian group of odd order.*

Proof. Let Q be equal to one of the quasigroups described in Theorem 3.9. If $p \equiv 1 \pmod 4$ and $r \geq 1$ is such that the $\mathbb{S}_{p^r,+}$ yields a different number of components than $\mathbb{S}_{p^r,-}$, then the quasigroup cannot be isomorphic to the mirror quasigroup by Lemma 3.13. If the numbers never differ, then $Q \cong Q^{op}$ by Proposition 3.11 and Lemma 3.13. □

4. Components and permutations

Let $\mathcal{D}$ be a PMD$(v,4)$ upon a set Q, $|Q| = v$. Say that blocks B_1, B_2 *neighbour* each other if there exist $x, y \in Q$ such that $B_1 = (x, y, \dots)$ and $B_2 = (y, x, \dots)$. Let $\sim$ be the equivalence closure upon $\mathcal{D}$ of the relation "to be a neighbour". A class of $\sim$ will be called a *component*.

Note that a neighbour to a block B is fully determined by any pair $\{x,y\}$ of vertices, where x and y occur in B next to one another. Such a pair is called a *common edge* of the neighbouring blocks. A cyclic sequence of blocks $C = (B_1, \dots, B_k)$ is called a *block cycle* if

(1) blocks $B_1, \dots, B_k$ are pairwise distinct;
(2) there exist $x_1, \dots, x_k \in Q$ and $z \in Q$ such that $\{x_i, z\}$ is a common edge of B_i and B_{i+1}, and $B_i = (z, x_i, \dots)$, $1 \leq i \leq k$. (Indices are counted modulo k).

The element z is called the *centre* of C.

We are mainly interested in finite PMD$(v,4)$. However, because of algebraic connections, some infinite PMD$(v,4)$ will still be allowed at this point. Say that a PMD$(v,4)$ is of *finite degree* if it contains no infinite sequence of blocks $(z, x_0, \dots)$, $(z, x_1, \dots)$, $\dots$ such that $x_i \neq x_j$ whenever $0 \leq i < j$.

An M4- or S3-quasigroup Q is said to be of *finite degree* if the induced PMD$(v,4)$ is of finite degree too. If Q is an M4-quasigroup, then this clearly means that for all $x, y \in Q$ there exists $k = k(x,y) \geq 1$ such that $R_x^k(y) = y$.

The following two statements assume that $\mathcal{D}$ is of finite degree. They have a common proof.

Lemma 4.1. *Let $C = (B_1, \dots, B_k)$ be a block cycle, and let x_i and z be as above. Then $k \geq 3$, z is the only centre of C and elements $x_1, \dots, x_k$ are pairwise distinct.*

Lemma 4.2. *Let B be a block of $\mathcal{D}$ and let $z \in Q$ be incident to B. Then there exists exactly one block cycle C that carries B and for which z is the centre.*

Proof. Let $C = (B_1, \dots, B_k)$ be a block cycle, where $B_i = (z, x_i, \dots)$. By the definition, $B_{i+1} = (x_i, z, x_{i+1}, y_{i+1})$ for some $y_{i+1} \in Q$. Thus $B_i = (z, x_i, y_i, x_{i-1})$, $1 \le i \le k$. Any (z, x_i) determines C completely, since it determines B_i, B_i determines x_{i+1} etc. If $x_i = x_j$, then $B_i = B_j$ and $i = j$. Hence $x_1, \dots, x_k$ are pairwise distinct. If $k = 2$, then both $\{x_1, z\}$ and $\{x_2, z\}$ are common edges of B_1 and B_2. That cannot be since in such a case $\{x_1, x_2\}$ would be a common diagonal of B_1 and B_2.

If $y_1 = y_2 = y$, then $\{y, z\}$ is a common diagonal of B_1 and B_2. Thus $y_1 \neq y_2$. If $z' = x_1$ is another centre of C, then $B_1 = (z', y_1, \dots)$, $B_2 = (y_2, z', \dots)$ and $y_1 = y_2 = y$. Hence no x_i is a centre. However, y_1 is also not a centre. Indeed, we have proved that $y_1 \neq y_2$. Therefore if y_1 occurs in B_2 then $y_1 = x_2$. That cannot be since x_2 is not a centre. Thus no y_i is a centre of C. The centre z is determined uniquely.

We have proved that if a block B is incident to z, then B occurs in at most one block cycle C for which z is a centre. Denote B as B_1 and assume that $B_1 = (z, x_1, \dots)$. Build a sequence of blocks $B_1, B_2, \dots$ such that $B_i = (z, x_i, \dots)$ and $\{z, x_i\}$ is a common edge of B_i and B_{i+1}. Let $k \ge 1$ be the least such that $B_{k+1} = B_j$, $1 \le j \le k$. If $j > 1$, then $B_k = B_{j-1}$, since B_{i+1} determines B_i completely. Hence $j = 1$ and $(B_1, \dots, B_k)$ is a block cycle. □

The centre of a block cycle $C = (B_1, \dots, B_k)$ will be denoted by $z(C)$. If $z = z(C)$ and $B_i = (z, x_i, \dots)$, then the cyclic sequence $(x_1, \dots, x_k)$ will be denoted by $s(C)$ and called the *star* of C. The integer $k \ge 3$ is called the *valency* of C. Note that $z(C)$ and $s(C)$ determine C completely—in fact $z(C)$ and any element of $s(C)$ determine C completely.

Lemma 4.3. *Let $\mathcal{D}$ be the design given by a finite-degree M4-quasigroup Q. Let C be a block cycle, $z = z(C)$ and $(x_1, \dots, x_k) = s(C)$. Then $R_z^i(x_j) = x_{i+j}$ for all integers i and j (indices counted modulo k).*

Proof. Proceed by induction on $i \ge 0$. Assume $R_z^i(x_j) = x_{i+j}$ and note that $(z, x_{i+j+1}, y, x_{i+j})$ is a block, for some $y \in Q$. Hence $R_z(x_{i+j}) = x_{i+j+1}$. □

Say that a PMD$(v, 4)$ is *k-regular* if each block cycle is of valency k.

Corollary 4.4. *Let $k \ge 3$ be a prime or let $k = 4$. Then the class of M4-quasigroups that give a k-regular PMD is the quasigroup variety determined by $yy = (y \cdot xy)x = y$ and $(\ ((xy)y)\dots)y = x$, y occurring k times.*

Proof. Consider $x \neq y$. If the PMD$(v, 4)$ is k-regular, then $R_y^k(x) = x$, by Lemmas 4.2 and 4.3. When Q is assumed to fulfil the identities of the statement, then Lemmas 4.2 and 4.3 imply that $R_y^\ell(x) = x$ for some $\ell > 1$ dividing k. Furthermore, $\ell \neq 2$, by Lemma 4.1. □

Consider a component $\mathbf{C}$ of a PMD$(v, 4)$. If a block B belongs both to $\mathbf{C}$ and to a block cycle C, then all blocks of C belong to $\mathbf{C}$. Denote by $V(\mathbf{C})$ the set of all block cycles the elements of which belong to $\mathbf{C}$. Define $E(\mathbf{C})$ as the set of edges $\{C, D\}$ such that $C, D \in V(\mathbf{C})$, $C \neq D$, and C and D share a block $(z(C), z(D), \dots)$. The pair $(V(\mathbf{C}), E(\mathbf{C}))$ will be known as the *graph* of $\mathbf{C}$.

To avoid a misunderstanding let us give an informal description of the graph (V, E) that is defined as a disjoint union of all graphs $(V(\mathbf{C}), E(\mathbf{C}))$, where $\mathbf{C}$ runs through all components of a given PMD$(v, 4)$. A point of the design, say a, is blown

up into as many vertices as many there are block cycles of which a is the centre. The number of edges $|E|$ is equal to $\binom{v}{2}$ since each pair of distinct points, say $\{a, b\}$, induces exactly one edge. This edge connects those two block cycles that simultaneously carry blocks $(a, b, \dots)$ and $(b, a, \dots)$. The centre of one of these block cycles is a, and the centre of this other is b. All blocks in these two block cycles belong to the same component since from block to another there exists a sequence of neigbouring blocks. This implies that the connectivity components of (V, E) are exactly the graphs $(V(\mathbf{C}), E(\mathbf{C}))$.

Proposition 4.5. *Let* $\mathbf{C}$ *be a component of a finite-degree* PMD$(v, 4)$. *The graph of* $\mathbf{C}$ *is an ordinary graph (i.e., no loops, no multiple edges) and is connected. The degree of* $D \in V(\mathbf{C})$ *is equal to the valency* k *of* D. *There exists a unique cyclic ordering* $(C_1, \dots, C_k)$ *of vertices adjacent to* D *such that* $s(D) = (z(C_1), \dots, z(C_k))$.

Furthermore, there exist unique vertices $D_1, \dots, D_k \in V(\mathbf{C})$ *such that* $\{D_i, C_i\}$ *and* $\{D_i, C_{i-1}\}$ *belong to* $E(\mathbf{C})$, *and* $D \neq D_i$, *for each* $i \in \{1, \dots, k\}$ *(with indices counted modulo* k*). For* $i \in \{1, \dots, k\}$ *set* $B_i = (z(D), z(C_i), z(D_i), z(C_{i-1}))$. *Then* $C = (B_1, \dots, B_k)$.

Proof. First note that if a block $(z(C), z(D), \dots)$ occurs in both $C, D \in V(\mathbf{C})$, then $(z(D), z(C), \dots)$ also occurs in both C and D, by the definition of block cycles. For $C, D \in V(\mathbf{C})$ there exists at most one block $(z(C), z(D), \dots)$. Hence the graph of $\mathbf{C}$ is really an ordinary graph. Fix now $D \in V(\mathbf{C})$ and suppose that $s(D) = (x_1, \dots, x_n)$. Let C_i be the block cycle with $z(C_i) = x_i$ that contains the block $B_i = (z(D), x_i, \dots)$. If $\{C, D\} \in E(\mathbf{C})$, then $(z(D), z(C), \dots) \in D$, and therefore $z(C) = x_i$ for some $i \in \{1, \dots, k\}$. Hence $C = C_i$. The cyclic ordering $(C_1, \dots, C_k)$ is unique since the star $s(D)$ is defined uniquely. Block cycles $C_1, \dots, C_k$ are pairwise distinct as their centres are pairwise distinct.

Consider again blocks B_i that have been defined above. By the definition of $s(D)$ there have to exist points y_i such that $B_i = (z(D), x_i, y_i, x_{i-1})$. Recall that $x_i = z(C_i)$. Thus $B_i \in C_i \cap C_{i-1} \cap D$. Choose D_i as the block cycle that carries B_i and has y_i as its centre. □

An *oriented quadrangulation* means here a triple (V, E, F) such that

(1) (V, E) is a connected ordinary graph;
(2) F consists of oriented 4-cycles (x_0, x_1, x_2, x_3) such that $\{x_i, x_{i+1}\} \in E$ if $0 \leq i \leq 3$ (indices computed modulo 4) and $x_i \neq x_j$ if $0 \leq i < j \leq 3$;
(3) for each $\{a, b\} \in E$ there exist unique $(x_0, x_1, \dots), (y_0, y_1, \dots) \in F$ such that $x_0 = a = y_1$ and $x_1 = b = y_0$; and
(4) for each $a \in V$ there exist $b_1, \dots, b_k \in V$ and $c_1, \dots, c_k \in V$ such that $(a, b_i, c_i, b_{i-1}) \in F$ (with indices computed modulo k), $b_i \neq b_j$ if $1 \leq i < j \leq k$, $k \geq 3$, and $b = b_i$ for some $i \in \{1, \dots, k\}$ whenever $\{a, b\} \in E$.

Elements of V are the *vertices*, elements of E are the *edges*, and elements of F are the *(oriented) faces*.

Theorem 4.6. *Let* $\mathbf{C}$ *be a component of finite-degree* PMD$(v, 4)$. *For each* $B = (x_0, x_1, x_2, x_3) \in \mathbf{C}$ *and* $i \in \{0, 1, 2, 3\}$ *there exists a unique block cycle* C_i *such that* $x_i = z(C_i)$ *and* B *is incident to* C_i. *Put* $\hat{B} = (C_0, C_1, C_2, C_3)$ *and* $F(\mathbf{C}) = \{\hat{B}; B \in \mathbf{C}\}$. *The triple* $(V(\mathbf{C}), E(\mathbf{C}), F(\mathbf{C}))$ *forms an oriented quadrangulation.*

Proof. The existence and uniqueness of C_i directly follows from Lemma 4.2. Let us consider the definition of oriented quadrangulation. Point (1) follows from Proposition 4.5. Each $\{C_i, C_{i+1}\}$ belongs to $E(\mathbf{C})$, by the definition of the latter. This yields (2). Consider a vertex $D \in V(\mathbf{C})$. By Proposition 4.5, the vertices connected to D can be cyclically ordered as $(C_1, \ldots, C_k)$, $k \geq 3$, in such a way that $s(C) = (z(C_1), \ldots, z(C_k))$, and, consequently, all blocks from $\mathbf{C}$ that are incident to $z(D)$ are the blocks B_i (as described in Proposition 4.5). Therefore all elements of $F(\mathbf{C})$ incident to D are the blocks $\widehat{B_i}$. Hence both (3) and (4) are true. □

The definition of $(V(\mathbf{C}), E(\mathbf{C}), F(\mathbf{C}))$ follows the usual process of splitting pinch points of an oriented pseudosurface to form an oriented surface.

By an *oriented grid* we shall understand an oriented quadrangulation such that each vertex is of degree 4. Note that in the finite case this will be toroidal.

Proposition 4.7. *Let λ and ρ permute a set X in such a way that $\langle \lambda, \rho \rangle$ is a finite transitive abelian group. Assume $|\lambda| \geq 3$, $|\rho| \geq 3$ and $\lambda \neq \rho^{\pm 1}$. Then the set of all cyclic sequences $(x, \lambda(x), \rho\lambda(x), \rho(x))$, $x \in X$, provides faces of an oriented grid. The edges of this grid are all of the pairs $\{x, \lambda(x)\}$ and $\{x, \rho(x)\}$, $x \in X$.*

Proof. Since $\langle \lambda, \rho \rangle$ is a transitive abelian group, it is regular. Hence all of its nonidentity elements are fixed point free. The quadruples $(x, \lambda(x), \rho\lambda(x), \rho(x))$ thus consist of four different elements, since $\lambda \neq \rho^{\pm 1}$. Together with $|\lambda|, |\rho| \geq 3$ this also implies that the elements $\lambda(x)$, $\lambda^{-1}(x)$, $\rho(x)$ and $\rho^{-1}(x)$ are pairwise distinct, for every $x \in X$. It remains to observe that faces incident to x can be listed as $(x, \lambda(x), \rho\lambda(x), \rho(x))$, $(x, \rho^{-1}(x), \rho^{-1}\lambda(x), \lambda(x))$, $(x, \lambda^{-1}(x), \lambda^{-1}\rho^{-1}(x), \rho^{-1}(x))$ and $(x, \rho(x), \rho\lambda^{-1}(x), \lambda^{-1}(x))$. □

The oriented grid induced by λ and ρ will be denoted by $G(\lambda, \rho)$. Note that if permutations λ and ρ do not satisfy the conditions of Proposition 4.7, then the construction of the statement does not yield an oriented grid in the sense of the definition above.

Proposition 4.8. *Oriented grids $G(\alpha, \beta)$ and $G(\lambda, \rho)$ coincide if and only if (α, β) is one of (λ, ρ), (ρ, λ^{-1}), $(\lambda^{-1}, \rho^{-1})$ and (ρ^{-1}, λ). Furthermore, $G(\rho, \lambda)$ is the grid of an opposite orientation.*

Proof. There must be $\alpha \in \{\lambda^{\pm 1}, \rho^{\pm 1}\}$ since $\{\alpha^{-1}(x), x\}$ and $\{x, \alpha(x)\}$ are opposite edges, and $\langle \lambda, \rho \rangle$ is abelian transitive. The rest is easy. □

We now turn our attention to the (classical) fact that each oriented grid can be expressed as $G(\lambda, \rho)$. Let us assume that $G = (V(G), E(G), F(G))$ is an oriented grid. Edges $\{x, y\}$ and $\{u, v\}$ are called *opposite* if there exist $z, x_i, y_i \in V(G)$, $i \in \{1, 2, 3, 4\}$, such that $\{x, y\} = \{x_i, z\}$ and $\{u, v\} = \{x_{i+2}, z\}$, where (z, x_i, y_i, x_{i-1}) are all the faces incident to z. Note that an edge is never opposite to itself.

Lemma 4.9. *Let $x_0, x_1, \ldots, x_k \in V(G)$, $k \geq 2$, be such that $x_0 = x_k$, $x_i \neq x_j$ if $1 \leq i < j \leq k$ and $\{x_i, x_{i+1}\} \in E(G)$, $0 \leq i < k$. If every edge $\{x_{i-1}, x_i\}$ is opposite to $\{x_i, x_{i+1}\}$, $1 \leq i < k$, then $k \geq 3$ and $\{x_0, x_1\}$ is opposite to $\{x_{k-1}, x_k\}$.*

Proof. The graph $(V(G), E(G))$ is assumed to be ordinary. Hence no edge is opposite to itself. Therefore $k \geq 3$. Start from the contrary and choose a counterexample such that k is the least possible. It can be assumed that there exists y_1 such

that (x_0, x_1, y_1, x_{k-1}) is an oriented face since the orientation may be reversed if needed. This face possesses a neighbour (x_1, x_2, y_2, y_1). Proceeding further establishes the existence of faces $(x_i, x_{i+1}, y_{i+1}, y_i)$, $1 \leq i \leq k-2$. Edges $\{x_{k-2}, x_{k-1}\}$ and $\{x_{k-1}, x_0\}$ are assumed to be opposite. Hence blocks $(x_{k-2}, x_{k-1}, y_{k-1}, y_{k-2})$ and (x_{k-1}, x_0, x_1, y_1) share edges $\{x_{k-1}, y_{k-1}\}$ and $\{x_{k-1}, y_1\}$. Therefore $y_1 = y_{k-1}$ and $y_{k-2} \neq x_1$. The block $(x_1.x_2, y_2, y_1)$ thus differs from the preceding two blocks. This implies $y_{k-2} \neq y_2$ and $k \geq 4$. The elements $y_1, y_2, \ldots, y_{k-1}$ have been constructed in such a way that $\{y_i, y_{i+1}\}$ is opposite to $\{y_{i+1}, y_{i+2}\}$, $1 \leq i \leq k-3$. Blocks $(x_1.x_2, y_2, y_1)$ and $(x_{k-2}, x_{k-1}, y_1, y_{k-2})$ share no edge. Hence $\{y_{k-1}, y_1\}$ is not opposite to $\{y_1, y_2\}$. That contradicts the choice of k. □

Proposition 4.10. *Each oriented grid G is equal to $G(\lambda, \rho)$ for some permutations λ and ρ.*

Proof. Consider a sequence $x_0, x_1, x_2, \ldots$ by choosing opposite edges. Suppose first that there exists $n > 0$ such that x_n is equal to some x_i, $0 \leq i < n$. Let n be the least possible. Note that $n \geq 3$. There must be $i = 0$ since if $i \geq 1$ then $x_{n-1} = x_{i-1}$ as both $\{x_{n-1}, x_n\}$ and $\{x_{i-1}, x_i\}$ are opposite edges to $\{x_i, x_{i+1}\}$. Choose an orientation $(x_1, \ldots, x_n)$ and consider faces $(x_i, x_{i+1}, y_{i+1}, y_i)$, $1 \leq i \leq n$. This yields a cyclic sequence $(y_1, \ldots, y_n)$. Elements $y_1, \ldots, y_n$ are pairwise distinct since $x_1, \ldots, x_n$ are pairwise distinct. Clearly, $y_i \neq x_j$ if $j \equiv i, i \pm 1 \pmod{k}$. Suppose that $y_i = x_j$ for some other j. Now, x_j is connected to x_{j-1}, x_{j+1} and y_j. Since y_j is not equal to $y_{i\pm1}$, there must be $\{x_{j-1}, x_{j+1}\} = \{y_{i-1}, y_{i+1}\}$. If $x_{j-1} = y_{i+1}$, then

$$(x_i, x_{i+1}, y_{i+1}, y_i) = (y_j, y_{j-1}, x_{j-1}, x_j),$$

implying thus $x_i = y_j$ and $x_{i+1} = y_{j-1}$. Proceeding further we get $x_{i+2} = y_{j-2}$ etc. There exists s such that $i + s \equiv j - s \pmod{k}$ or $i + s \equiv j - s + 1 \pmod{k}$, and that means the existence of h such that $x_h \in \{y_h, y_{h+1}\}$, which is a contradiction. Therefore $x_{j-1} = y_{i-1}$, and thus $x_{j-s} = y_{i-s}$ for every integer s. Therefore there exist $d \in \{2, \ldots, k-2\}$ such that $y_i = x_{i+d}$. Defining λ as the cyclic permutation $x_i \mapsto x_{i+1}$ yields $G = G(\lambda, \lambda^d)$.

If the starting sequence $x_0, x_1, \ldots$ is infinite, then by the preceding part of the proof there exists an infinite sequence $\ldots, x_{-1}, x_0, x_1 \ldots$ in which all vertices x_i are pairwise different. This yields a sequence $\ldots, y_{-1}, y_0, y_1, \ldots$ and faces $(x_i, x_{i+1}, y_{i+1}, y_i)$. The points y_i have to be pairwise distinct as well. If there exist i and j such that $x_i = y_j$, then proceeding like above yields an expression in the form $G(\lambda, \lambda^d)$, where $d \geq 2$ and $\lambda(x_i) = x_{i+1}$.

Suppose now that the method above never yields $(x_1, \ldots, x_k)$ and $(y_1, \ldots, y_k)$ that share a vertex. (A similar assumption may also be made in the infinite case.) In the finite case there exist $k \geq 3$ and $h \geq 2$ and vertices $x_{i,j}$, $1 \leq i \leq h$ and $1 \leq j \leq k$ with faces $(x_{i,j}, x_{i,j+1}, x_{i+1,j+1}, x_{i+1,j})$, $1 \leq i < h$ and $1 \leq j \leq k$, where j is computed modulo k. Suppose that h is maximal possible. Then it may be assumed that $x_{h,1}$ is connected to $x_{1,d}$ for some $d \in \{1, \ldots, k\}$. Hence there exists an oriented face $(x_{1,d-1}, x_{1,d}, x_{h,1}, \ldots)$ or an oriented face $(x_{1,d+1}, x_{1,d}, x_{h,1}, \ldots)$. The existence of the face $(x_{1,d-1}, x_{1,d}, x_{2,d}, x_{2,d+1})$ excludes the latter possibility. Thus the face in question has to be equal to $(x_{1,d+1}, x_{1,d}, x_{h,1}, x_{h,2})$ and, by induction, $x_{h,j}$ is connected to $x_{1,j+d-1}$. It remains to define λ by $x_{i,j} \mapsto x_{i,j+1}$ and ρ by $x_{h,j} \mapsto x_{1,j+d-1}$ and $x_{i,j} \mapsto x_{i+1,j}$, $1 \leq i < h$.

In the infinite case let it first be assumed that there exists a cyclic sequence $(x_1, \ldots, x_k)$ induced by a sequence of opposite edges. Then the vertices can be labelled $x_{i,j}$, with i counted modulo k and $j \in \mathbb{Z}$ in such a way that every face is equal to $(x_{i,j}, x_{i,j+1}, x_{i+1,j+1}, x_{i+1,j})$ for some i and j. If no $(x_1, \ldots, x_k)$ exists, then the grid can be expressed as $G(\lambda, \rho)$, where $\langle \lambda, \rho \rangle$ is a free abelian group of rank two. □

Lemma 4.11. *Let Q be a flexible quasigroup that satisfies the law M4. Then $xyx = x/y = y(x\backslash y)$ and $((xy \cdot y)y)y = x$, for all $x, y \in Q$.*

Proof. The identity $xyx = x/y$ follows immediately from the law M4' (cf. Proposition 1.1). Thus $y(x\backslash y)y = y/(x\backslash y) = x$, for all $x, y \in Q$. Hence $y(x\backslash y) = x/y$. Plugging $y = xz$ yields $xz \cdot z = x/(xz) = x \cdot xzx$. By M4' this is equal to $(xzx)z(xzx) = (xzx)/z = (x/z)/z$. Thus $((xz \cdot z)z)z = x$. □

Theorem 4.12. *Each centred* PMD$(v, 4)$ *is 4-regular. A 4-regular* PMD$(v, 4)$ *is centred if and only if (x_4, x_3, x_2, x_1) is a block of the PMD for every block cycle C, $s(C) = (x_1, x_2, x_3, x_4)$. If the* PMD$(v, 4)$ *is centred and C is a block cycle, then the centre of $s(C)^{op} = (x_4, x_3, x_2, x_1)$ is equal to $z(C)$.*

Proof. Suppose that the PMD is given by an M4-quasigroup Q. If the PMD is centred, then Q is flexible, by Proposition 2.7, and the PMD is 4-regular, by Corollary 4.4 and Lemma 4.11. Suppose that the PMD is 4-regular and consider elements x and z, $x \neq z$. By Lemma 4.2 there exists a block cycle C such that $z(C) = z$, $s(C) = (x_1, x_2, x_3, x_4)$ and $x_1 = x$. Now, $x_2x_1 = x_4$ is equivalent to $xz \cdot x = x \cdot zx$ since $x_1z = x_2$ and $x_4 = x_1 \cdot zx_1$. The rest is clear. □

If $\mathbf{C}$ is a component of a PMD$(v, 4)$, then the mapping $C \mapsto z(C)$ sends vertices of $\mathbf{C}$ upon points and faces of $\mathbf{C}$ upon blocks. Theorem 4.12 thus immediately yields the following consequence.

Corollary 4.13. *Let (a, b_0, c_0, b_1) be a block of a centred* PMD$(v, 4)$*. Then there exist blocks (a, b_1, c_1, b_2), (a, b_2, c_2, b_3) and (a, b_3, c_3, b_0). These blocks are uniquely determined. Furthermore, (b_0, b_1, b_2, b_3) is also a block, and a is the centre of this block.*

Corollary 4.14. *Let $\mathbf{C}$ be a component of a centred* PMD$(v, 4)$*. Then there exist permutations λ and ρ of $V(\mathbf{C})$, i.e. of the vertex set of $\mathbf{C}$, such that $\mathbf{C} = G(\lambda, \rho)$.*

Proof. A centred PMD$(v, 4)$ is 4-regular, by Theorem 4.12. By Theorem 4.6 the component $\mathbf{C}$ yields an oriented quadrangulation. By Proposition 4.5 vertices of this quadrangulation have degree 4. Hence $\mathbf{C}$ yields an oriented grid. The rest follows from Proposition 4.10. □

To conclude this section we summarize the hierarchy of some quasigroups discussed in this paper. By Proposition 2.7, centred PMD$(v, 4)$s correspond to flexible S3-quasigroups, and also to flexible M4-quasigroups. From Theorem 4.12, every centred PMD$(v, 4)$ is 4-regular. Thus $v \equiv 1 \pmod 4$, by Lemma 4.3.

Centred PMD$(v, 4)$s, i.e. flexible S3-quasigroups are enumerated in [5] for $v \leq 13$. Comparing these results with Corollary 3.10 shows that all these quasigroups are medial, i.e. quadratical.

However, by [5] there exist flexible S3-quasigroups of order 21. There is no quadratical quasigroup of order 21. The variety of quadratical quasigroups is thus strictly smaller than the variety of flexible S3-quasigroups.

On the other hand, the variety of flexible S3-quasigroups is strictly smaller than the variety of S3-quasigroups that yield 4-regular PMDs (cf. Corollary 4.4). This can be deduced from the existence of the so called reverse centred PMD$(v, 4)$ [5].

5. Grids induced by quadratical quasigroups

A PMD$(v, 4)$ uniquely determines the operation of the associated M4-quasigroup, and an M4-quasigroup uniquely determines a PMD$(v, 4)$. Two PMD$(v, 4)$s are isomorphic if and only if the associated M4-quasigroups are isomorphic. The same is true for the associated S3-quasigroups.

An S3-quasigroup Q is medial if and only if it is quadratical (Corollary 2.12). Furthermore, Q is medial if and only the associated M4-quasigroup $(Q, \backslash)$ is also medial (Proposition 1.3 and Lemma 3.1). Medial M4-quasigroups are in a 1-to-1 correspondence with $\mathbb{Z}[\mathrm{i}]$-modules upon which 2 acts invertibly (Theorem 3.6). Isomorphism types of PMD$(v, 4)$s given by quadratical quasigroups thus correspond to isomorphism types of such $\mathbb{Z}[\mathrm{i}]$-modules. The formula for the operation $*$ of a medial M4-quasigroup corresponding to a $\mathbb{Z}[\mathrm{i}]$-module M is $x * y = \mathrm{i}x + (1-\mathrm{i})y$. As can be easily verified, blocks of the PMD$(v, 4)$ given by such a M4-quasigroup are

$$(x,\ y,\ \mathrm{i}x + (1-\mathrm{i})y, (\mathrm{i}+1)x - \mathrm{i}y) \quad \text{where } x, y \in M \text{ and } x \neq y. \tag{5.1}$$

This will be known as the PMD$(v, 4)$ *given by a* $\mathbb{Z}[\mathrm{i}]$*-module* M.

To avoid an exceptional treatment of the zero $\mathbb{Z}[\mathrm{i}]$-module $M = 0$, let us make a convention that it corresponds to PMD$(1, 4)$, i.e. to the trivial design with no block and one point.

Lemma 5.1. *Let* $B = (x, x+z, \dots)$ *be a block of the* PMD$(v, 4)$ *given by a* $\mathbb{Z}[\mathrm{i}]$*-module* M*, and let* $\mathbf{C}$ *be the component that carries* B*. Then*

$$\big(x+(r-s\mathrm{i})z,\ x+((r+1)-s\mathrm{i})z,\ x+((r+1)-(s+1)\mathrm{i})z,\ x+(r-(s+1)\mathrm{i})z\big) \tag{5.2}$$

are all the blocks of the component $\mathbf{C}$*, with* r *and* s *running through* $\mathbb{Z}$*.*

Proof. The 4-cycles occurring in (5.2) form a block since

$$\mathrm{i}(r - s\mathrm{i}) + (1 - \mathrm{i})((r + 1) - s\mathrm{i}) = (r + 1) - (s + 1)\mathrm{i} \quad \text{and}$$
$$(\mathrm{i} + 1)(r - s\mathrm{i}) - \mathrm{i}((r + 1) - s\mathrm{i}) = r - (s + 1)\mathrm{i}$$

imply the compatibility with (5.1). Denote this block by $B(r, s)$ and observe that the neighbouring blocks are equal to $B(r, s-1)$, $B(r+1, s)$, $B(r, s+1)$ and $B(r-1, s)$. □

Corollary 5.2. *Let* $\mathbf{C}$ *be a component of the* PMD$(v, 4)$ *given by a* $\mathbb{Z}[\mathrm{i}]$*-module* M*, and let* x *be an element of* M*. Then* $x+\mathbf{C} = \{(x+a, x+b, x+c, x+d);\ (a, b, c, d) \in \mathbf{C}\}$ *is a component too.*

Proof. This follows directly from Lemma 5.1. □

If $\mathbf{C}$ is a component of a PMD$(v, 4)$, then $C \mapsto z(C)$ sends a vertex $C \in V(\mathbf{C})$ (i.e., a block cycle) upon the (only) point that that is shared by all blocks of C (i.e., the centre of the block cycle C). Cf. Section 4.

Corollary 5.3. *Let* $\mathbf{C}$ *be a component of the* PMD$(v, 4)$ *given by a* $\mathbb{Z}[\mathrm{i}]$*-module* M*. The mapping* $V(\mathbf{C}) \to M$*,* $C \mapsto z(C)$*, is injective.*

Proof. Let $B = (x, x+z, x+(1-\mathrm{i})z, x-\mathrm{i}z)$ be a block of $\mathbf{C}$, and let this block belong to a block cycle $C \in V(\mathbf{C})$. Suppose that $z(C) = x$, and let $D \in V(\mathbf{C})$ be such that $z(D) = x$ as well. By Lemma 5.1 the block cycle D contains a block given by (5.2) for which $x+(r-s\mathrm{i})z = x$. This implies that $(r-s\mathrm{i})z = 0$, and that this block coincides with the block B. Since C and D share a block, and $z(C) = z(D)$, the block cycles C and D coincide too. □

A module M over a ring R is said to be *cyclic* if there exists $y \in M$ such that $Ry = M$.

Proposition 5.4. *Let M be a $\mathbb{Z}[\mathrm{i}]$-module upon which 2 acts invertibly. The module M is cyclic if and only if the* PMD$(v, 4)$ *given by M contains a component $\mathbf{C}$ such that every element of M occurs in at least one block of $\mathbf{C}$ (i.e., if $z(V(\mathbf{C})) = M$).*

Proof. Let $y \in M$ be such that $\mathbb{Z}[\mathrm{i}]y = M$. By (5.1) the PMD$(v, 4)$ contains a block $(0, y, (1-\mathrm{i})y, -\mathrm{i}y)$. By Lemma 5.1 the component of this block covers each element $(r+s\mathrm{i})y$, where $r, s \in \mathbb{Z}$. The set of these elements coincides with $\mathbb{Z}[\mathrm{i}]y$. For the converse direction first note that $\mathbf{C}$ covers all of M if and only if $x + \mathbf{C}$ covers all of M, by Corollary 5.2, for each $x \in M$. Hence it may be assumed that M is covered by a component that contains a block $(0, z, \dots)$. If this is true, then $M = \mathbb{Z}[\mathrm{i}]z$, again by Lemma 5.1. □

For an odd $n > 1$ denote by $\mathbb{Z}_n[\mathrm{i}]$ be the $\mathbb{Z}[\mathrm{i}]$-module with underlying abelian group $\{x+\mathrm{i}y;\ x, y \in \mathbb{Z}_n\}$ in which $\mathrm{i}(x+\mathrm{i}y) = -y+\mathrm{i}x$.

Furthermore, if $\kappa \in \mathbb{Z}_n$ is such that $\kappa^2 + 1 = 0$, denote by $\mathbb{Z}_n(\kappa)$ the $\mathbb{Z}[\mathrm{i}]$-module upon $\mathbb{Z}_n$ for which $\mathrm{i}x = \kappa x$, for every $x \in \mathbb{Z}_n$.

Proposition 5.5. *Each cyclic $\mathbb{Z}[i]$-module upon which 2 acts invertibly is isomorphic to exactly one of the modules $\mathbb{Z}_n[\mathrm{i}]$, $\mathbb{Z}_m(\kappa)$ and $\mathbb{Z}_n[\mathrm{i}] \times \mathbb{Z}_m(\kappa)$, with $n, m > 1$ being odd, $\kappa^2 \equiv -1 \pmod m$, and $\gcd(n, m) = 1$.*

Proof. Since $\mathbb{Z}[\mathrm{i}]$ is a Principal Ideal Domain, the Chinese Remainder Theorem applies. Each proper factor of $\mathbb{Z}[\mathrm{i}]$ is hence a product of factors over primary ideals (the ideals (π^r), π irreducible, $r \geq 1$). Now, $\mathbb{Z}[\mathrm{i}]/(\pi^r)$ is isomorphic either to $\mathbb{Z}_{p^r}[\mathrm{i}]$, p an odd prime $\equiv 3 \pmod 4$, or to $\mathbb{Z}_{p^r}(\kappa)$, p an odd prime $\equiv 1 \pmod 4$, $\kappa^2 \equiv -1 \pmod p^r$, (cf. Section 3). A sum $\mathbb{Z}[i]/(\pi_1)^{r_1} \oplus \cdots \oplus \mathbb{Z}[i]/(\pi_k^{r_k})$, with all $r_1, \dots, r_k$ positive integers, is a cyclic module if and only if there are no i and j such that $\pi = \pi_i = \pi_j$ and $1 \leq i < j \leq k$. This is true for every principal ideal domain. To see it directly in the present context note that if there were such $\pi_i = \pi = \pi_j$, then $\mathbb{Z}[i]/(\pi) \oplus \mathbb{Z}[i]/(\pi)$ would be cyclic, by factorization. But that is never true, since neither $\mathbb{Z}_p[\mathrm{i}] \oplus \mathbb{Z}_p[\mathrm{i}]$ nor $\mathbb{Z}_p(\kappa) \oplus \mathbb{Z}_p(\kappa)$ are cyclic. Furthermore, if n and m are coprime odd integers, then $\mathbb{Z}_n[\mathrm{i}] \oplus \mathbb{Z}_m[\mathrm{i}] \cong \mathbb{Z}_{nm}[\mathrm{i}]$ and $\mathbb{Z}_n(\kappa_1) \oplus \mathbb{Z}_m(\kappa_2) \cong \mathbb{Z}_{nm}(\kappa)$, where $\kappa \cong \kappa_1 \pmod n$ and $\kappa \cong \kappa_2 \pmod m$. Finally, $\mathbb{Z}_n(\kappa) \oplus \mathbb{Z}_n(\kappa^{-1}) \cong \mathbb{Z}_n[\mathrm{i}]$, cf. Lemma 3.13. □

If y is a nonzero element of M, then $\mathbf{C}_y$ will denote the component of the PMD given by M that contains the block $(0, y, \dots)$. If $M = 0$, then $\mathbf{C}_0$ denotes the only component of the PMD$(1, 4)$ (the component consists one vertex and contains no face).

Lemma 5.6. *Let y be a nonzero element of a cyclic $\mathbb{Z}[i]$-module upon which 2 acts invertibly. Then $z(V(\mathbf{C}_y)) = \mathbb{Z}[\mathrm{i}]y$.*

Proof. This follows directly from Lemma 5.1. (In (5.2) set $x = 0$ and $z = y$.) □

Lemma 5.7. *Let M be a cyclic $\mathbb{Z}[i]$-module upon which 2 acts invertibly, and let $\mathbf{C}$ be a component of the* PMD$(v, 4)$ *given by M. Then $z(V(\mathbf{C})) = M$ if and only if there exists $y \in M$ such that $\mathbf{C} = \mathbf{C}_y$ and $\mathbb{Z}[\mathrm{i}]y = M$.*

Proof. Suppose that $z(V(\mathbf{C})) = M$. Then $\mathbf{C}$ contains a vertex, say C, that is sent by z to 0. Recall that a vertex is formed by a cycle of four blocks that share the point that is the image of the vertex. Hence each of the four blocks contributing to C is of the form $(0, y, \dots)$. For each of them $\mathbf{C} = \mathbf{C}_y$. By Lemma 5.6, $\mathbb{Z}[\mathrm{i}]y = z(V(\mathbf{C}_y)) = M$. Conversely, if $\mathbb{Z}[\mathrm{i}]y = M$ and $\mathbf{C} = \mathbf{C}_y$, then $z(V(\mathbf{C}_y)) = M$. □

For the sake of brevity assume that both $\mathbb{Z}_1[\mathrm{i}]$ and $\mathbb{Z}_1(1)$ denote the zero module 0. The latter convention allows to express Proposition 5.4 in this form: *Each cyclic $\mathbb{Z}[i]$-module upon which 2 acts invertibly is isomorphic to $\mathbb{Z}_n[\mathrm{i}]\times\mathbb{Z}_m(\kappa)$, where n and m are uniquely determined coprime positive odd integers and $\kappa^2 \equiv -1 \pmod m$.*

Our next aim is to describe, up to isomorphism, those grids $G(\lambda, \rho)$ that are induced by $\mathbb{Z}[i]$-modules upon which 2 acts invertibly. For $n, m \geq 1$ and $\kappa \in \mathbb{Z}_m^*$ define λ and ρ as permutations of $\mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_m$ such that

$$\lambda\colon (a, b, c) \mapsto (a{+}1, b, c{+}1) \quad \text{and} \quad \rho\colon (a, b, c) \mapsto (a, b{-}1, c{-}\kappa).$$

It is clear that $\lambda\rho = \rho\lambda$, that $\langle\lambda, \rho\rangle$ is a transitive abelian group, and that $\lambda \neq \rho^{\pm1}$ if $n > 1$ or $\kappa \neq \pm1$. Hence, assuming that the latter condition is true, $G(\lambda, \rho)$ is a toroidal grid, by Proposition 4.7. It will be denoted by $G[n, m, \kappa]$. The faces of $G[n, m, \kappa]$ are

$$((a, b, c),\ (a{+}1, b, c{+}1),\ (a{+}1, b{-}1, c{+}1{-}\kappa)\,(a, b{-}1, c{-}\kappa)). \tag{5.3}$$

Theorem 5.8. *Let n and m be coprime odd positive integers, and let $\kappa \in \mathbb{Z}_m^*$ be such that $\kappa^2 \equiv -1 \pmod m$. Then $M = \mathbb{Z}_n[\mathrm{i}] \oplus \mathbb{Z}_m(\kappa)$ is a cyclic $\mathbb{Z}[\mathrm{i}]$-module, and each cyclic $\mathbb{Z}[\mathrm{i}]$-module upon which 2 acts invertibly can be expressed in this way, up to isomorphism. If $y \in M$ is a generator of M, i.e. if $M = \mathbb{Z}[\mathrm{i}]y$, then*

$$\sigma_y\colon (r{+}s\mathrm{i})y \to (r \bmod n, s \bmod n, (r{+}\kappa s) \bmod m)$$

is a bijection $M \to \mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_m$. The mapping $C \mapsto \sigma_y z(C)$ is an isomorphism of the component $\mathbf{C}_y$ and the grid $G[n, m, \kappa]$. (A grid isomorphism bijectively sends vertices upon vertices, and faces upon faces.)

Proof. If $y, y' \in M$ are two generators, then $(r{+}s\mathrm{i})y = 0 \Leftrightarrow (r{+}s\mathrm{i})y' = 0$. Since y' may be chosen as $(1, 1) \in \mathbb{Z}_n[\mathrm{i}] \oplus \mathbb{Z}_m(\kappa)$, it is clear that

$$(r{+}s\mathrm{i})y = 0 \quad \Longleftrightarrow \quad n \mid r,\ n \mid s \text{ and } m \mid r + \kappa s, \tag{5.4}$$

for all $r, s \in \mathbb{Z}$. Define a homomorphism of abelian groups $\sigma\colon \mathbb{Z}[\mathrm{i}] \to \mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_m$ by $r{+}s\mathrm{i} \mapsto (r \bmod n, s \bmod n, (r{+}\kappa s) \bmod m)$. Since $r{+}s\mathrm{i} \in \mathrm{Ker}(\sigma)$ if and only if the right hand side of (5.4) holds, σ_y is an isomorphism $(M, +) \cong \mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_m$, by the First Isomorphism Theorem. A face of $\mathbf{C}_y$ is mapped by $z\colon V(\mathbf{C}_y) \to M$ upon a block $((r{+}s\mathrm{i})y, (r{+}1{+}s\mathrm{i})y, (r{+}1{+}s\mathrm{i}{-}\mathrm{i})y, (r{+}s\mathrm{i}{-}\mathrm{i})y)$, by Lemma 5.1. If $\sigma_y((r{+}s\mathrm{i})y) = (a, b, c)$, then this block is mapped by σ_y upon $((a, b, c), (a{+}1, b, c{+}1), (a{+}1, b{-}1, c{+}1{-}\kappa), (a, b{-}1, c{-}\kappa))$, which agrees with (5.3). The rest follows from Corollary 5.3 and Proposition 5.5. □

Corollary 5.9. *Let M be a $\mathbb{Z}[\mathrm{i}]$-module upon which 2 acts invertibly, and let $\mathbf{C}$ be a component of a* PMD$(v,4)$ *given by M. Then there exist coprime odd integers $n, m \geq 1$, and $\kappa \in \mathbb{Z}_m$, $\kappa^2 \equiv -1 \pmod{m}$, such that $\mathbf{C}$ is isomorphic to $G[n,m,\kappa]$, and $\mathbb{Z}_n[\mathrm{i}] \oplus \mathbb{Z}_m(\kappa)$ is isomorphic to a cyclic submodule of M.*

Proof. By Corollary 5.2 the component $\mathbf{C}$ is isomorphic to a component $\mathbf{C}_y$, $y \in M$. Now, $\mathbf{C}_y$ is also a component of the PMD given by $\mathbb{Z}[\mathrm{i}]y$, a cyclic submodule of M. That makes Theorem 5.8 applicable. □

6. Skew squares and skew expansion

Let $ABCD$ be a square in a Euclidean plane. Interpret it as a block (A,B,C,D) of the PMD that is induced by the quadratical operation that defines $X \cdot Y$ as a point Z such that the angle XZY is right and $|XZ| = |ZY|$. This is the operation that has been discussed at the beginning of this paper and that stands at the beginning of all research on quadratical quasigroups. Note that $B = A \cdot C$ and $D = C \cdot A$. Put $X = A \cdot B$, $Y = B \cdot C$, $U = C \cdot D$ and $V = D \cdot A$. Then $XYUV$ is a square and (X,Y,U,V) is a block, see Fig. 4. It will be called the *skew expansion* of (A,B,C,D). This notion can be generalized to all quadratical quasigroups:

Lemma 6.1. *Let $(Q,\cdot)$ be a quadratical quasigroup and let (x_1,x_2,x_3,x_4) be a block of the associated* PMD$(v,4)$. *Then $(x_1x_2, x_2x_3, x_3x_4, x_4x_1)$ is also a block.*

Proof. We have $x_2 = x_1x_3$ and $x_4 = x_3x_1$. By mediality and S3, $x_1x_2 \cdot x_3x_4 = (x_1 \cdot x_1x_3)(x_3 \cdot x_3x_1) = (x_1x_3)(x_1x_3 \cdot x_3x_1) = x_1x_3 \cdot x_3 = x_2x_3$. □

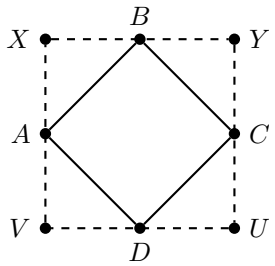

FIGURE 4. The skew expansion (X,Y,U,V) of the block (A,B,C,D).

Let $B = (x_1,x_2,x_3,x_4)$ be a block induced by a quadratical quasigroup. The block $(x_1x_2, x_2x_3, x_3x_4, x_4x_1)$ is called the *skew expansion* of B. It will be denoted by $\mathbf{e}(B)$.

Proposition 6.2. *Let $\mathbf{C}$ be a component of a* PMD$(v,4)$ *given by a $\mathbb{Z}[\mathrm{i}]$-module M upon which 2 acts invertibly. Then $\mathbf{e}(\mathbf{C}) = \{\mathbf{e}(B);\, B \in \mathbf{C}\}$ is also a component, and $z(\mathbf{e}(\mathbf{C})) = z(\mathbf{C})$.*

Proof. The quadratical operation induced by M is $(x,y) \mapsto ((1{-}\mathrm{i})x + (1{+}\mathrm{i})y)/2$, by Theorem 3.6. If a block B is of a form $(u, u{+}y, u{+}(1{-}\mathrm{i})y, u{-}\mathrm{i}y)$, then $\mathbf{e}(B)$ is equal to $(w, w{+}(1{-}\mathrm{i})y, w{-}2\mathrm{i}y, w{-}(1{+}\mathrm{i})y)$, where $w = u{+}(1{+}\mathrm{i})y/2$. By Lemma 5.1 there exist $y, z \in M$ such that the blocks B that constitute $\mathbf{C}$ are all the blocks $B(r,s)$, where $r,s \in \mathbb{Z}$ and $u = u(r,s) = z{+}(r{+}s\mathrm{i})y$. Since 2 acts invertibly upon

M, the cyclic module $\mathbb{Z}[\mathrm{i}]y$ is equal to $\{((2r+1)+(2s+1)\mathrm{i})y/2;\ r,s\in\mathbb{Z}\}$. Hence the set of all $\mathbf{e}(B(r,s))$ coincides with the set of all

$$B'(r,s)=(u(r,s),u(r,s)+(1-\mathrm{i})y,u(r,s)-2\mathrm{i}y,u(r,s)-(1+\mathrm{i})y).$$

The four neighbours of $B'(r,s)$ are $B'(r+1,s+1)$, $B'(r+1,s-1)$, $B'(r-1,s-1)$ and $B'(r-1,s+1)$. Hence $B'(r,s+2)$ is a neighbour of a neighbour of $B'(r,s)$, and this is also true for $B'(r+2,s)$. Since 2 acts invertibly, all blocks $B'(r,s)$ belong to the same component. □

If $B=(a,b,c,d)$ is a block of a PMD$(v,4)$ that is associated with a quadratical quasigroup $(Q,\cdot)$, then the centre of the block is equal to $aba=bcb=cdc=dad$. By Theorem 3.6 the quasigroup Q may be obtained from a $\mathbb{Z}[\mathrm{i}]$-module M, with multiplication $(x,y)\mapsto((1-\mathrm{i})x+(1+\mathrm{i})y)/2$. The centre is thus equal to $(a+c)/2=(b+d)/2$. Define $E^k(B)$, $k\geq 0$, so that $E^0(B)=\{(a+c)/2\}$ and $E^{k+1}(B)=E^k(B)\cup\{x,y,u,v\}$, where $(x,y,u,v)=\mathbf{e}^{k+1}(B)$.

In [4] Dudek and Monzo say that a quadratical quasigroup Q is of *form* Qn if $E^n(B)=Q$. In Section 4 of [4] they prove that a quadratical quasigroup of order 9 is of form $Q2$. In Section 6 they present operational tables of quadratical quasigroups of order 13 and 17, and prove that they are of forms $Q3$ and $Q4$, respectively. In Section 7 they show that there is no quadratical quasigroup of form $Q6$. At the end of the paper they formulate a number of questions, some of which are answered below.

Proposition 6.3. *Let M be a $\mathbb{Z}[\mathrm{i}]$-module upon which 2 acts invertibly, and let B be a block of the* PMD$(v,4)$ *given by M. If there exists $k\geq 0$ such that $E^k(B)=M$, then the module M is cyclic.*

Let $y\in M$ be such that $M=\mathbb{Z}[\mathrm{i}]y$. For $k\geq 0$ set

$$\mathcal{A}_k(y)=\{2^i(1+\mathrm{i})y,2^i(1-\mathrm{i})y,2^i(-1+\mathrm{i})y,2^i(-1-\mathrm{i})y;\ -1\leq i\leq k-2\}\ \textit{and}$$
$$\mathcal{B}_k(y)=\{2^iy,-2^iy,2^i\mathrm{i}y,-2^i\mathrm{i}y;\ 0\leq i\leq k-1\}.$$

Assume $k\geq 0$. Then

$$M=E^{2k}(B)\iff M=\{0\}\cup\mathcal{A}_k(y)\cup\mathcal{B}_k(y),\ \textit{and}$$
$$M=E^{2k+1}(B)\iff M=\{0\}\cup\mathcal{A}_{k+1}(y)\cup\mathcal{B}_k(y).$$

Proof. Let B belong to a component $\mathbf{C}$. By Proposition 6.2 the block $\mathbf{e}^i(B)$ is in the component $\mathbf{e}^i(\mathbf{C})$, and that component carries the same points as $\mathbf{C}$, i.e. $z(\mathbf{C})=z(\mathbf{e}^i(\mathbf{C}))$. Hence if $E^k(B)=M$, then B must belong to a component $\mathbf{C}$ with $z(\mathbf{C})=M$. By Proposition 5.4 this happens if and only if M is cyclic.

Suppose that $M=\mathbb{Z}[\mathrm{i}]y$. Let B a block of $\mathbf{C}$, and B' a block of $\mathbf{C}'$, where $z(\mathbf{C})=z(\mathbf{C}')=M$. By Corollary 5.2 and Lemma 5.7, $E^k(B)=M$ if and only if $E^k(B')=M$. Because of that we may start from the component $\mathbf{C}_y$ and the block

$$B=\left(\frac{-1+\mathrm{i}}{2}y,\frac{1+\mathrm{i}}{2}y,\frac{1-\mathrm{i}}{2}y,\frac{-1-\mathrm{i}}{2}y\right).$$

The rest of the statement follows from the fact that if $k\geq 0$, then

$$\mathbf{e}^{2k}(B)=(2^k\mathrm{i}y,\ 2^ky,\ -2^k\mathrm{i}y,\ -2^ky),\ \text{and}$$
$$\mathbf{e}^{2k+1}(B)=((-1+\mathrm{i})2^ky,(1+\mathrm{i})2^ky,(1-\mathrm{i})2^ky,(-1-\mathrm{i})2^ky).$$

□

Define the 2-*exponent* $\exp_2(M)$ as ∞ if there is no block B such that $E^k(B) = M$ for some $k \geq 0$. If such a block exists define $\exp_2(M)$ as the value of the least possible k for which $M = E^k(B)$. By Proposition 6.3, a quadratical quasigroup induced by M is of form Qn, $n < \infty$, if and only if $\exp_2(M) = n$.

Lemma 6.4. *Let M and N be $\mathbb{Z}[\mathrm{i}]$-modules upon which 2 acts invertibly. Suppose that N is a homomorphic image of M. Then $\exp_2(N) \leq \exp_2(M)$.*

Proof. Let $M = \mathbb{Z}[\mathrm{i}]y$ and $N = \mathbb{Z}[\mathrm{i}]y'$, and let $\varphi\colon M \to N$ be the homomorphism that sends y upon y'. Then φ maps $\mathcal{A}_k(y)$ upon $\mathcal{A}_k(y')$ and $\mathcal{B}_k(y)$ upon $\mathcal{B}_k(y')$. □

Proposition 6.5. *Let M be a nonzero $\mathbb{Z}[\mathrm{i}]$-module upon which 2 acts invertibly. Suppose that $\exp_2(M) < \infty$. Then either $M \cong \mathbb{Z}_3[\mathrm{i}]$ or there exists a prime $p \equiv 1 \pmod 4$ such that $M \cong \mathbb{Z}_p(\kappa)$, $\kappa^2 \equiv -1 \pmod p$.*

Proof. Let us first observe that $\exp_2(\mathbb{Z}_n[\mathrm{i}]) = \infty$ whenever n is an odd integer greater than 3. This is because 1+2i is equal neither to 1−i nor to any other member of $\mathcal{A}_k(1) \cup \mathcal{B}_k(1)$, $k \geq 1$. Consider now $\mathbb{Z}_n(\kappa)$, $\kappa^2 \equiv 1 \pmod n$, where $n > 1$ is odd. All integers 2^i, $i \geq 0$, are invertible when considered as elements of $\mathbb{Z}_n(\kappa)$. This is also true for -1, κ, $\kappa-1$ and $\kappa+1$. Therefore each element of $\mathcal{A}_k(1) \cup \mathcal{B}_k(1)$ is invertible, for any $k \geq 1$. If n is not a prime, then $\mathbb{Z}_n(\kappa)$ contains elements that are not invertible. This argument may also be used to exclude the case $M \cong \mathbb{Z}_3[\mathrm{i}] \oplus \mathbb{Z}_p(\kappa)$. □

We can thus answer in negative [4, Problem 3].

Corollary 6.6. *There exists no quadratical quasigroup $(Q, \cdot)$ of form Qn such that $Q \cong Q^{op}$ and $|Q| > 9$.*

Proof. If Q is a quadratical quasigroup such that $Q \cong Q^{op}$, then Q cannot be isomorphic to $\mathbb{Z}_p(\kappa)$, by Proposition 3.14. □

Lemma 6.7. *Let M be a $\mathbb{Z}[\mathrm{i}]$-module upon which 2 acts invertibly, and let Q be the S3-quasigroup obtained from M by means of the operation $(x, y) \mapsto ((1-\mathrm{i})x + (1+\mathrm{i})y)/2$. If $M \cong \mathbb{Z}_p[\mathrm{i}]$, where p is a prime $\equiv 3 \pmod 4$, or if $M \cong \mathbb{Z}_p(\kappa)$, where p is a prime $\equiv 1 \pmod 4$, $\kappa^2 \equiv -1 \pmod m$, then any two distinct elements of Q generate Q.*

Proof. This follows straightforwardly from the fact that if M fulfils the assumptions of the statement, then M has no proper nontrivial submodule. □

We can thus answer in positive [4, Problem 4].

Corollary 6.8. *If Q is a quadratical quasigroup of form Qn, then Q is generated by each of its 2-element subsets.*

As already indicated by Propositions 6.3 and 6.5, the 2-exponent of a $\mathbb{Z}[\mathrm{i}]$-module M, $|M| > 9$, depends only upon properties of a prime $p \equiv 1 \pmod 4$:

Proposition 6.9. *Let $p \equiv 1 \pmod 4$ be a prime, and let $\kappa \in \mathbb{Z}_p$ be such that $\kappa^2 \equiv -1 \pmod p$. Then $\exp_2(\mathbb{Z}_p(\kappa)) = \exp_2(\mathbb{Z}_p(\kappa^{-1}))$. Furthermore, $\exp_2(\mathbb{Z}_p(\kappa)) < \infty$ if and only if $\mathbb{Z}_p^*$ is generated by 2 and $\kappa+1$.*

Proof. The first part of the statement follows from the fact that the quadratical quasigroups induced by $\mathbb{Z}_p(\kappa)$ and $\mathbb{Z}_p(\kappa^{-1})$ are opposite each to other, by

Lemma 3.13. The second part follows from Proposition 6.3 and from the ensuing identities that are true in $\mathbb{Z}_p^*$:

$$\kappa^2 = -1,\ \kappa^{-1} = -\kappa,\ (\kappa{+}1)^2 = 2\kappa \text{ and } (\kappa{+}1)^{-1} = (1{-}\kappa)/2. \tag{6.1}$$

□

Theorem 6.10. *Let $p \equiv 1 \pmod 4$ be a prime. The value of $\exp_2(\mathbb{Z}_p(\kappa))$ is independent of the choice of $\kappa \in \mathbb{Z}_p^*$, $\kappa^2 = -1$. Denote this value by $e(p)$. Denote by D_p the subgroup of $\mathbb{Z}_p^*$ generated by 2, and put $d_p = |D_p| = \mathrm{ord}_p(2)$. These are the only cases when $e(p) < \infty$:*

1. *$p = 16k + 9$ and $d_p = 2k + 1$.*
2. *$p = 16k + 9$ and $d_p = 4k + 2$.*
3. *$p = 16k + 9$, $d_p = 8k + 4$ and $\kappa{+}1$ is a nonsquare.*
4. *$p = 16k + 1$ and $d_p = 8k$.*
5. *$p = 8k + 5$ and $d_p = p{-}1$.*

In all these cases $e(p) = (p{-}1)/4$.

Proof. If $d_p = 2h$, then $2^h = -1$. Suppose that $d_p = 2k + 1$ is odd. Then $-1 \notin D_p$, and each two elements from the set

$$\{1, -1, \kappa, -\kappa, (\kappa{+}1)/2, -(\kappa{+}1)/2, (\kappa{-}1)/2, -(\kappa{-}1)/2\}$$

belong to a different coset of D_p in $\mathbb{Z}_p^*$, as follows from (6.1). By Proposition 6.3, $e(p) < \infty$ if and only if $|\mathbb{Z}_p^* : D_p| = 8$.

From here on we shall assume that $-1 \in D_p$. Let us have $\kappa \notin D_p$. Since κ and $-\kappa$ are the only elements of $\mathbb{Z}_p^*$ that are of order 4, there must be $d_p = 4k + 2$, for some $k \geq 0$. The cosets D_p, κD_p, $(\kappa{+}1)D_p$ and $(\kappa{-}1)D_p$ are pairwise different. Hence $e(p) < \infty$ if and only if $|\mathbb{Z}_p^* : D_p| = 4$.

From here on $\kappa \in D_p$ will be assumed. Then $d_p = 4h$, and κ may be set to be equal to 2^h. If there exists ℓ such that $\kappa{+}1 = 2^\ell$, then $2\ell \equiv 1{+}h \pmod 4 h$ since $(\kappa{+}1)^2 = 2\kappa$, by (6.1). This is not possible if h is even. In such a case $d_p = 8k$, $\kappa{+}1 \notin D_p$, and $e(p) < \infty$ if and only if $p = 16k + 1$.

Suppose that h is odd. If $p = 8t + 1$, then there cannot be $d_p = p - 1$ since 2 is a square. Hence if $e(p) < \infty$, then there must be $d_p = (p{-}1)/2 = 4t = 8k + 4$, and $\kappa{+}1$ has to be a nonsquare.

Let us have $p = 8k + 5$. Since d_p has to be divisible by 4, there cannot be $d_p = 4k + 2$. The only possibility hence is that that $D_p = \mathbb{Z}_p^*$.

To see that $e(p) = (p{-}1)/4$ in cases (1)–(4) is straightforward since the underlying coset structure may be used. In the last case we argue as follows. Suppose that $(\kappa{+}1)/2 = 2^s$. Then $2^{2s} = \kappa/2 = 2^{2k+1}/2$. Hence $s = k$ may be assumed. That implies that $\mathcal{A}_{k+1}(1) \cap \mathcal{B}_k(1) = \emptyset$. □

Theorem 6.10 thus gives a tool to decide whether there exists a quadratical quasigroup of form Qn. This question appears as Problem 1 in [4]. We see that $4n{+}1$ has to be equal to 9 or to a prime p. This is a necessary condition. The sufficient conditions are formulated in Theorem 6.10. Their main feature is the requirement that the order of 2 modulo p is big.

Tools developed in this paper may be used to answer various further questions concerning quadratical quasigroups.

The concept of components, as described in Section 4, applies to all PMD$(v, 4)$s. It seems that in particular the theory of centered PMD$(v, 4)$s might gain by generalizing the ensuing concepts, as developed in Sections 5 and 6.

References

[1] F. E. Bennett: *The spectra of a variety of quasigroups and related combinatorial designs*, Discrete Math. **77** (1989), 29–50.

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

[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: *Translatable Quadratical Quasigroups*, Quasigroups and Related Systems **28** (2020), 203–228.

[5] T. S. Griggs, A. Drápal and A. R. Kozlik: *Quasigroups constructed from perfect Mendelsohn designs with block size 4*, J. Combin. Des. **28** (2020), 489–508.

[6] N. S. Mendelsohn: *Perfect cyclic designs*, Discrete Math. **20** (1977), 63–68.

[7] A. Sade: *Quasigroupes obéissant á certaines lois*, Rev. Fac. Sci. Univ. Istambul, Sér. **22** (1957), 151–184.

[8] J. D. H. Smith: *Palindromic and Sudoku quasigroups*, JCMCC **88** (2014), 85–94.

[9] D. Stanovský and P. Vojtěchovský: *Central and Medial Quasigroups of Small Order*, Bul. Acad. Ştiinţe Repub. Mold. Mat. **80** (2016), 24–40.

[10] K. Toyoda: *On axioms of linear functions*, Proc. Imp. Acad. Tokyo **17** (1941), 221–227.

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

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

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

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

Dept. of Algebra, Charles University, Sokolovská 83, 186 75 Praha 8, Czech Rep.

Dept. of Mathematics and Statistics, The Open University, Walton Hall, Milton Keynes MK7 6AA, United Kingdom

Dept. of Algebra, Charles University, Sokolovská 83, 186 75 Praha 8, Czech Rep.
Email address: drapal@karlin.mff.cuni.cz
Email address: terry.griggs@open.ac.uk
Email address: andrew.kozlik@gmail.com