

# IDEMPOTENT SOLUTIONS OF THE YANG-BAXTER EQUATION AND TWISTED GROUP DIVISION

DAVID STANOVSKÝ AND PETR VOJTĚCHOVSKÝ

**ABSTRACT.** Idempotent left nondegenerate solutions of the Yang-Baxter equation are in one-to-one correspondence with twisted Ward left quasigroups, which are left quasigroups satisfying the identity  $(x*y)*(x*z) = (y*y)*(y*z)$ . Using combinatorial properties of the Cayley kernel and the squaring mapping, we prove that a twisted Ward left quasigroup of prime order is either permutational or a quasigroup. Up to isomorphism, all twisted Ward quasigroups  $(X, *)$  are obtained by twisting the left division operation in groups (that is, they are of the form  $x * y = \psi(x^{-1}y)$  for a group  $(X, \cdot)$  and its automorphism  $\psi$ ), and they correspond to idempotent latin solutions. We solve the isomorphism problem for idempotent latin solutions.

## 1. INTRODUCTION

We continue our program of studying left nondegenerate set-theoretic solutions of the Yang-Baxter equation from an algebraic perspective, taking advantage of the associated left quasigroups [2, 12].

It is well-known that the algebraic counterpart to derived left nondegenerate solutions of the Yang-Baxter equation are *racks*, which are left quasigroups satisfying the identity

$$(x * y) * (x * z) = x * (y * z). \quad (1.1)$$

There is vast literature on racks, on idempotent racks (i.e., *quandles*), and on their usage in knot theory [1, 7, 9, 15, 21].

Jones [11] and Turaev [22] showed that Yang-Baxter operators  $r : V \otimes V \rightarrow V \otimes V$  that satisfy a quadratic equation  $r^2 = ar + b$  give rise to polynomial invariants of knots. In the realm of set-theoretic solutions, the quadratic equation reduces to either  $r^2 = 1$  (the *involution* case) or  $r^2 = r$  (the *idempotent* case).

Rump showed in [20] that the algebraic counterpart to involutive left nondegenerate solutions are *cycle sets*, which are left quasigroups satisfying the identity

$$(x * y) * (x * z) = (y * x) * (y * z). \quad (1.2)$$

We have renamed cycle sets *Rump left quasigroups* in [2] and we continue to use this terminology here.

In this paper we focus on idempotent left nondegenerate solutions. In Section 2 we provide a uniform treatment to the correspondences for derived, involutive and idempotent left nondegenerate solutions. We recover the above correspondences for derived and involutive left nondegenerate

---

*Date:* February 10, 2020.

*1991 Mathematics Subject Classification.* 16T25, 20N05.

*Key words and phrases.* Quantum Yang-Baxter equation, set-theoretical solution to Yang-Baxter equation, braiding, idempotent braiding, twisted Ward quasigroup, Ward quasigroup.

The paper is written within the framework of the cooperation grant LTAUSA19070. David Stanovský partially supported by the GAČR grant 18-20123S. Petr Vojtěchovský partially supported by the 2019 PROF grant of the University of Denver.

solutions, and we prove that the algebraic counterpart to idempotent left nondegenerate solutions are left quasigroups satisfying the identity

$$(x * y) * (x * z) = (y * y) * (y * z), \quad (\text{tW})$$

which we call *twisted Ward left quasigroups* for reasons explained below.

In Section 3 we completely classify twisted Ward quasigroups and hence idempotent latin solutions of the Yang-Baxter equation, cf. Theorem 3.10. First we show that, unlike in the case of latin racks and Rump quasigroups, every twisted Ward quasigroup is isotopic to a group. In fact, every twisted Ward quasigroup has the form  $(X, *)$  with  $x * y = c\psi(x^{-1}y)$ , where  $(X, \cdot)$  is a group,  $\psi$  is an automorphism of  $(X, \cdot)$  and  $c \in X$ . Classifying these quasigroups up to isomorphism, it suffices to consider groups  $(X, \cdot)$  up to isomorphism, automorphisms  $\psi$  up to conjugation in the automorphism group of  $(X, \cdot)$ , and  $c = 1$ . Summarizing, *idempotent latin solutions of the Yang-Baxter equation are in one-to-one correspondence with conjugacy classes of automorphisms of groups*.

The above representation theorem is the reason why we have chosen the terminology “twisted Ward quasigroup.” Quasigroups  $(X, *)$  defined over groups  $(X, \cdot)$  via  $x * y = x^{-1}y$  were first investigated by Ward in [23] and later became known as *Ward quasigroups*. They are precisely the quasigroups satisfying the identity

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

and they can be thought of as groups axiomatized by left division instead of multiplication, cf. [10, 18, 19, 23].

In Section 4 we classify twisted Ward left quasigroups of prime order. We consider two equivalence relations on a twisted Ward left quasigroup, namely the Cayley kernel and the kernel of the squaring map, and we show that, in the finite case, each of the equivalences has blocks of uniform size. Consequently, a twisted Ward left quasigroup of prime order is either permutational or a quasigroup. This complements the result of Etingof, Soloviev and Guralnick [8] who classified all indecomposable nondegenerate solutions to the Yang-Baxter equation with a prime number of elements.

## 2. THREE CLASSES OF LEFT NONDEGENERATE BRAIDINGS

A binary algebraic structure  $(X, *)$  is a *left quasigroup* if all left translations  $L_x : X \rightarrow X$ ,  $y \mapsto x * y$  are bijections of  $X$ . In a left quasigroup  $(X, *)$  we can define the left division operation by  $x \setminus y = L_x^{-1}(y)$  and observe that, obviously,

$$x \setminus (x * y) = y = x * (x \setminus y) \quad (2.1)$$

holds for all  $x, y \in X$ . Conversely, if  $(X, *, \setminus)$  is a set equipped with two binary operations satisfying the identity (2.1), then  $(X, *)$  is a left quasigroup with left division  $\setminus$ . Note that if  $(X, *)$  is a left quasigroup with left division  $\setminus$ , then  $(X, \setminus)$  is a left quasigroup with left division  $*$  [17].

Dually,  $(X, *)$  is a *right quasigroup* if all right translations  $R_x : X \rightarrow X$ ,  $y \mapsto y * x$  are bijections of  $X$ . The right division operation is then defined by  $x /_* y = R_y^{-1}(x)$ . A left quasigroup that is also a right quasigroup is called a *quasigroup*.

A *set-theoretic solution* of the Yang-Baxter equation

$$(r \times 1)(1 \times r)(r \times 1) = (1 \times r)(r \times 1)(1 \times r) \quad (\text{YB})$$

is a mapping  $r : X \times X \rightarrow X \times X$  such that (YB) holds as an equality of mappings  $X \times X \times X \rightarrow X \times X \times X$  under composition [5]. Set-theoretic solutions of (YB) are also known as *braidings* [13].

For any mapping (not necessarily a braiding)  $r : X \times X \rightarrow X \times X$  we write

$$r(x, y) = (x \circ y, x \bullet y)$$

for suitable binary operations  $\circ$  and  $\bullet$  on  $X$ . Straightforward calculation then shows that  $r$  is a braiding if and only if the following three identities hold:

$$x \circ (y \circ z) = (x \circ y) \circ ((x \bullet y) \circ z), \quad (\text{YB1})$$

$$(x \circ y) \bullet ((x \bullet y) \circ z) = (x \bullet (y \circ z)) \circ (y \bullet z), \quad (\text{YB2})$$

$$(x \bullet y) \bullet z = (x \bullet (y \circ z)) \bullet (y \bullet z). \quad (\text{YB3})$$

A mapping  $r : X \times X \rightarrow X \times X$  is said to be *left nondegenerate* if  $(X, \circ)$  is a left quasigroup; *nondegenerate* if  $(X, \circ)$  is a left quasigroup and  $(X, \bullet)$  is a right quasigroup; *latin* if  $(X, \circ)$  is a quasigroup; *derived* if  $x \bullet y = x$  for every  $x, y \in X$ ; *involutive* if  $r^2 = 1$  [20]; and *idempotent* if  $r^2 = r$  [13].

We are mostly interested in braidings where one of the two operations  $\circ, \bullet$  is either trivial or can be reconstructed from the other one. The following result gives three classes of mappings with such a property.

**Lemma 2.1.** *Let  $r : X \times X \rightarrow X \times X$  be a mapping,  $r(x, y) = (x \circ y, x \bullet y)$ . Then:*

- (i)  *$r$  is derived if and only if  $x \bullet y = x$ .*
- (ii)  *$r$  is involutive and left nondegenerate if and only if  $(X, \circ)$  is a left quasigroup and  $x \bullet y = (x \circ y) \circ x$ .*
- (iii)  *$r$  is idempotent and left nondegenerate if and only if  $(X, \circ)$  is a left quasigroup and  $x \bullet y = (x \circ y) \circ (x \circ y)$ .*

*Proof.* Part (i) holds by definition. For (ii), note that  $r$  is involutive if and only if the identities

$$(x \circ y) \circ (x \bullet y) = x, \quad (x \circ y) \bullet (x \bullet y) = y$$

hold. If  $r$  is also left nondegenerate then  $x \bullet y = (x \circ y) \circ x$  is equivalent to the first identity, and the second identity becomes

$$((x \circ y) \circ ((x \circ y) \circ x)) \circ (x \circ y) = y,$$

which holds in any left quasigroup  $(X, \circ)$ . Finally, for (iii), note that  $r$  is idempotent if and only if the identities

$$(x \circ y) \circ (x \bullet y) = x \circ y, \quad (x \circ y) \bullet (x \bullet y) = x \bullet y$$

hold. If  $r$  is also left nondegenerate then  $x \bullet y = (x \circ y) \circ (x \circ y)$  is equivalent to the first identity, and the second identity becomes

$$(z \circ (z \circ z)) \circ (z \circ (z \circ z)) = z \circ z$$

with  $z = x \circ y$ , which holds in any left quasigroup  $(X, \circ)$ . □

The proof of the following result is somewhat involved. Nevertheless it is purely equational and can be verified in a fraction of a second by an automated theorem prover, such as `Prover9` [14].

**Proposition 2.2.** *Let  $r : X \times X \rightarrow X \times X$  be a mapping. Then:*

- (i)  *$r$  is a derived braiding if and only if  $x \bullet y = x$  and*

$$x \circ (y \circ z) = (x \circ y) \circ (x \circ z). \quad (2.2)$$

- (ii)  *$r$  is an involutive left nondegenerate braiding if and only if  $(X, \circ)$  is a left quasigroup,  $x \bullet y = (x \circ y) \circ x$  and*

$$x \circ (y \circ z) = (x \circ y) \circ (((x \circ y) \circ x) \circ z). \quad (2.3)$$

- (iii)  *$r$  is an idempotent left nondegenerate braiding if and only if  $(X, \circ)$  is a left quasigroup,  $x \bullet y = (x \circ y) \circ (x \circ y)$  and*

$$x \circ (y \circ z) = (x \circ y) \circ (((x \circ y) \circ (x \circ y)) \circ z). \quad (2.4)$$

*Proof.* (i) By Lemma 2.1,  $r$  is a derived mapping if and only if  $x \bullet y = x$  holds. Then (YB1) is equivalent to (2.2), (YB2) is equivalent to the trivial identity  $x \circ y = x \circ y$ , and (YB3) is equivalent to the trivial identity  $x = x$ .

For the rest of the proof, let us write  $xy$  instead of  $x \circ y$ ,  $x \setminus y$  instead of  $x \circ y$ , and  $[x, y]$  instead of  $x \bullet y$  to save space and improve legibility. The identities (YB1)–(YB3) then become

$$\begin{aligned} x(yz) &= (xy)([x, y]z), \\ [xy, [x, y]z] &= [x, yz][y, z], \\ [[x, y], z] &= [[x, yz], [y, z]]. \end{aligned}$$

(ii) By Lemma 2.1,  $r$  is an involutive left nondegenerate mapping if and only if  $(X, \cdot)$  is a left quasigroup and  $[x, y] = (xy) \setminus x$ . Hence (YB1) holds if and only if (2.3) holds. Suppose that (YB1) holds and let us rewrite it as  $(xy) \setminus (x(yz)) = [x, y]z$ . Upon substituting  $y \setminus z$  for  $z$ , we obtain

$$(xy) \setminus (xz) = [x, y](y \setminus z). \quad (2.5)$$

Using (YB1), the left hand side of (YB2) can be written as  $[xy, [x, y]z] = ((xy)([x, y]z)) \setminus (xy) = (x(yz)) \setminus (xy)$ . Upon substituting  $y \setminus z$  for  $z$  into (YB2), we therefore obtain the identity

$$(xz) \setminus (xy) = [x, z][y, y \setminus z] = [x, z](z \setminus y),$$

which is (2.5) with  $y$  and  $z$  interchanged. Hence (YB2) holds. To show that (YB3) also holds, first note that (2.3) can be written as  $L_x L_y = L_{xy} L_{(xy) \setminus x}$ . Substituting  $x \setminus y$  for  $y$ , we obtain  $L_x L_{x \setminus y} = L_y L_{y \setminus x}$ , and taking inverses yields

$$L_{x \setminus y}^{-1} L_x^{-1} = L_{y \setminus x}^{-1} L_y^{-1}. \quad (2.6)$$

We will return to (2.6) shortly. By (YB1), the left hand side of (YB3) is equal to

$$[[x, y], z] = ([x, y]z) \setminus [x, y] = ((xy) \setminus (x(yz))) \setminus ((xy) \setminus x).$$

By (YB2) and (YB1), the right hand side of (YB3) is equal to

$$\begin{aligned} [[x, yz], [y, z]] &= ([x, yz][y, z]) \setminus [x, yz] = [xy, [x, y]z] \setminus [x, yz] \\ &= [xy, (xy) \setminus (x(yz))] \setminus [x, yz] = ((x(yz)) \setminus (xy)) \setminus ((x(yz)) \setminus x). \end{aligned}$$

Upon substituting  $y \setminus z$  for  $z$ , we see that (YB3) is then equivalent to

$$((xy) \setminus (xz)) \setminus ((xy) \setminus x) = ((xz) \setminus (xy)) \setminus ((xz) \setminus x),$$

which is further equivalent, upon substitution of  $x \setminus y$  for  $y$  and  $x \setminus z$  for  $z$ , to

$$(y \setminus z) \setminus (y \setminus x) = (z \setminus y) \setminus (z \setminus x).$$

But this says  $L_{y \setminus z}^{-1} L_y^{-1} = L_{z \setminus y}^{-1} L_z^{-1}$ , which is (2.6) with the variables renamed.

(iii) By Lemma 2.1,  $r$  is an idempotent left nondegenerate mapping if and only if  $(X, \cdot)$  is a left quasigroup and  $[x, y] = (xy) \setminus (xy)$ . Hence (YB1) holds if and only if (2.4) holds. Suppose that (YB1) holds. As in (ii), we obtain the equivalent identity (2.5). Using (YB1), the left hand side of (YB2) can be written as  $((xy)([x, y]z)) \setminus ((xy)([x, y]z)) = (x(yz)) \setminus (x(yz))$ . Upon substituting  $y \setminus z$  for  $z$  into (YB2), we therefore obtain the identity

$$(xz) \setminus (xz) = [x, z][y, y \setminus z] = [x, z](z \setminus z),$$

which is an instance of (2.5) with  $y = z$ . Hence (YB2) holds. To see that (YB3) also holds, note that (2.4) is equivalent to  $L_x L_y = L_{xy} L_{(xy) \setminus (xy)}$ , which is the same as  $L_x L_{x \setminus y} = L_y L_{y \setminus y}$  and hence

$$L_{x \setminus y}^{-1} L_x^{-1} = L_{y \setminus y}^{-1} L_y^{-1}. \quad (2.7)$$

Following the same series of steps as in (ii), we can rewrite (YB3) as

$$((xy) \setminus (x(yz))) \setminus ((xy) \setminus (x(yz))) = ((x(yz)) \setminus (x(yz))) \setminus ((x(yz)) \setminus (x(yz))),$$

which is equivalent, upon substitution of  $y \setminus z$  for  $z$ , to

$$((xy) \setminus (xz)) \setminus ((xy) \setminus (xz)) = ((xz) \setminus (xz)) \setminus ((xz) \setminus (xz)),$$

and hence to

$$(y \setminus z) \setminus (y \setminus z) = (z \setminus z) \setminus (z \setminus z).$$

But this is implied by  $L_{y \setminus z}^{-1} L_y^{-1} = L_{z \setminus z}^{-1} L_z^{-1}$ , which is (2.7) with the variables renamed.  $\square$

As has become clear from the proof of Proposition 2.2, the identities (2.3) and (2.4) are somewhat inconvenient to work with. We will therefore employ the following syntactic trick due to Rump [20] to arrive at simpler left quasigroup identities that correspond to the same braidings as in Proposition 2.2 (but not necessarily to the same left quasigroups).

Given a left nondegenerate mapping  $r : X \times X \rightarrow X \times X$ , the trick is to write

$$r(x, y) = (x \setminus^\circ y, x \bullet y)$$

and express the equations (YB1)–(YB3) in terms of the operations  $\circ$  and  $\bullet$ , rather than  $\setminus^\circ$  and  $\bullet$ .

**Proposition 2.3.** *Let  $r : X \times X \rightarrow X \times X$  be a left nondegenerate mapping written as  $r(x, y) = (x \setminus^\circ y, x \bullet y)$ . Then:*

- (i)  *$r$  is a derived left nondegenerate braiding if and only if  $(X, \circ)$  is a left quasigroup,  $x \bullet y = x$  and*

$$(x \circ y) \circ (x \circ z) = x \circ (y \circ z). \quad (2.8)$$

- (ii)  *$r$  is an involutive left nondegenerate braiding if and only if  $(X, \circ)$  is a left quasigroup,  $x \bullet y = (x \setminus^\circ y) \circ x$  and*

$$(x \circ y) \circ (x \circ z) = (y \circ x) \circ (y \circ z). \quad (2.9)$$

- (iii)  *$r$  is an idempotent left nondegenerate braiding if and only if  $(X, \circ)$  is a left quasigroup,  $x \bullet y = (x \setminus^\circ y) \circ (x \setminus^\circ y)$  and*

$$(x \circ y) \circ (x \circ z) = (y \circ y) \circ (y \circ z). \quad (2.10)$$

*Proof.* (i) By Proposition 2.2,  $r$  is a derived left nondegenerate braiding if and only if  $(X, \setminus^\circ)$  is a left quasigroup (equivalently,  $(X, \circ)$  is a left quasigroup),  $x \bullet y = x$  and

$$x \setminus^\circ (y \setminus^\circ z) = (x \setminus^\circ y) \setminus^\circ (x \setminus^\circ z).$$

In terms of the left translations in  $(X, \circ)$ , the last identity is equivalent to  $L_x^{-1} L_y^{-1} = L_{x \setminus^\circ y}^{-1} L_x^{-1}$ . Taking inverses on both sides, we obtain the equivalent identity  $L_y L_x = L_x L_{x \setminus^\circ y}$ . Substituting  $x \circ y$  for  $y$ , we obtain  $L_{x \circ y} L_x = L_x L_y$ , which is (2.8).

(ii) By Proposition 2.2,  $r$  is an involutive left nondegenerate braiding if and only if  $(X, \circ)$  is a left quasigroup,  $x \bullet y = (x \setminus^\circ y) \circ x$  and

$$x \setminus^\circ (y \setminus^\circ z) = (x \setminus^\circ y) \setminus^\circ (((x \setminus^\circ y) \circ x) \setminus^\circ z).$$

This says  $L_x^{-1} L_y^{-1} = L_{x \setminus^\circ y}^{-1} L_{(x \setminus^\circ y) \circ x}^{-1}$ , which is equivalent to  $L_{x \circ y} L_x = L_{y \circ x} L_y$ , i.e., to (2.9).

(iii) By Proposition 2.2,  $r$  is an idempotent left nondegenerate braiding if and only if  $(X, \circ)$  is a left quasigroup,  $x \bullet y = (x \setminus^\circ y) \circ (x \setminus^\circ y)$  and

$$x \setminus^\circ (y \setminus^\circ z) = (x \setminus^\circ y) \setminus^\circ (((x \setminus^\circ y) \circ (x \setminus^\circ y)) \setminus^\circ z).$$

This says  $L_x^{-1} L_y^{-1} = L_{x \setminus^\circ y}^{-1} L_{(x \setminus^\circ y) \circ (x \setminus^\circ y)}^{-1}$ , which is equivalent to  $L_{x \circ y} L_x = L_{y \circ y} L_y$ , i.e., to (2.10).  $\square$

Recall from the introduction that a left quasigroup  $(X, *)$  is a *rack* (resp. *Rump left quasigroup*, resp. *twisted Ward left quasigroup*) if it satisfies (1.1) (resp. (1.2), resp. (tW)).

Part (i) of Theorem 2.4 is well-known and part (ii) can be found in [20, Proposition 1].

**Theorem 2.4.** *Let  $X$  be a set. Denote a typical braiding on  $X$  by  $r(x, y) = (x \circ y, x \bullet y)$ . Then:*

- (i) There is a one-to-one correspondence between derived left nondegenerate braidings on  $X$  and racks on  $X$ , given by

$$r \mapsto (X, *), \quad x * y = x \circlearrowleft y, \quad (X, *) \mapsto r, \quad r(x, y) = (x \circlearrowleft y, x).$$

- (ii) There is a one-to-one correspondence between involutive left nondegenerate braidings on  $X$  and Rump left quasigroups on  $X$ , given by

$$r \mapsto (X, *), \quad x * y = x \circlearrowleft y, \quad (X, *) \mapsto r, \quad r(x, y) = (x \circlearrowleft y, (x \circlearrowleft y) * x).$$

- (iii) There is a one-to-one correspondence between idempotent left nondegenerate braidings on  $X$  and twisted Ward left quasigroups on  $X$ , given by

$$r \mapsto (X, *), \quad x * y = x \circlearrowleft y, \quad (X, *) \mapsto r, \quad r(x, y) = (x \circlearrowleft y, (x \circlearrowleft y) * (x \circlearrowleft y)).$$

*Proof.* It is clear that in each case the two mappings are mutually inverse. The rest follows from Proposition 2.3.  $\square$

**Remark 2.5.** (a) As we have shown, the identities  $x \circ (y \circ z) = (x \circ y) \circ (x \circ z)$  and  $x \circlearrowleft (y \circlearrowleft z) = (x \circlearrowleft y) \circlearrowleft (x \circlearrowleft z)$  are equivalent in the variety of left quasigroups. It is therefore customary to replace the correspondence from Theorem 2.4(i) with the correspondence

$$r \mapsto (X, *), \quad x * y = x \circ y, \quad (X, *) \mapsto r, \quad r(x, y) = (x * y, x).$$

Our version of the correspondence for racks fits better with the uniform approach employed here.

(b) Neither of the identities (2.3) and (2.9) implies the other in the variety of left quasigroups. Likewise, neither of the identities (2.4) and (2.10) implies the other in the variety of left quasigroups. Therefore, in both cases, there are two varieties of left quasigroups that can be chosen to correspond to the braidings in question.

**Corollary 2.6.** *Let  $X$  be a set,  $|X| \geq 2$ . Then every idempotent braiding on  $X$  is degenerate.*

*Proof.* Let  $r(x, y) = (x \circ y, x \bullet y)$  be an idempotent nondegenerate braiding and let  $(X, *)$  be the corresponding twisted Ward left quasigroup, i.e.,  $x * y = x \circlearrowleft y$ . For every  $y \in X$ , the right translation  $x \mapsto x \bullet y = (x \circlearrowleft y) * (x \circlearrowleft y)$  is a bijection of  $X$ , which immediately implies that the squaring mapping  $\sigma : x \mapsto x * x$  is onto  $X$ . We will prove that  $\sigma$  is also injective. First observe that  $x \bullet (x * y) = (x \circlearrowleft (x * y)) * (x \circlearrowleft (x * y)) = y * y$ , hence  $x = (y * y) \bullet (x * y)$  is independent of  $y$ , and thus  $x = (x * x) \bullet (x * x)$ . Consequently, if  $\sigma(u) = \sigma(v)$ , we have  $u = (u * u) \bullet (u * u) = (v * v) \bullet (v * v) = v$ .

Now,  $\sigma(x * y) = (x * y) * (x * y) = (y * y) * (y * y) = \sigma(y * y)$  is an instance of (tW), and since  $\sigma$  is bijective, we have  $x * y = \sigma(y)$  for every  $x, y \in X$ . But then  $x \bullet y = (x \circlearrowleft y) * (x \circlearrowleft y) = \sigma(x \circlearrowleft y) = \sigma(\sigma^{-1}(y)) = y$ , hence  $r$  is right degenerate, a contradiction.  $\square$

The following are examples of twisted Ward left quasigroups.

**Example 2.7.** Let  $(X, *)$  be an elementary abelian 2-group. Then  $(x * y) * (x * z) = y * z = (y * y) * (y * z)$ , so  $(X, *)$  is a twisted Ward (left) quasigroup.

**Example 2.8.** Let  $(X, +)$  be an abelian group,  $\varphi \in \text{End}(X, +)$ ,  $\psi \in \text{Aut}(X, +)$  and  $c \in X$ . Define a binary operation  $*$  on  $X$  by

$$x * y = \varphi(x) + \psi(y) + c.$$

It is easy to check that the resulting left quasigroup  $(X, *)$  satisfies (tW) if and only if

$$\varphi\psi = \psi\varphi \quad \text{and} \quad \varphi^2 + \varphi\psi = 0.$$

**Example 2.9.** Let  $x * y = f(y)$  for some bijection  $f$  of  $X$ . Then  $(X, *)$  is clearly a left quasigroup, usually called a *permutational left quasigroup*. Every permutational left quasigroup satisfies (tW).

**Lemma 2.10.** *Let  $(X, *)$  be a twisted Ward left quasigroup. Then the following conditions are equivalent:*

- (i)  $(X, *)$  is a rack,
- (ii)  $(X, *)$  is a Rump left quasigroup,
- (iii)  $(X, *)$  is permutational.

*Proof.* If  $(X, *)$  is permutational then it satisfies both (1.1) and (1.2). If  $(X, *)$  satisfies (1.1) then  $x * (y * z) = (x * y) * (x * z) = (y * y) * (y * z)$  and substituting  $y \setminus^* z$  for  $z$  yields  $x * z = (y * y) * z$ , which means that all left translations are the same and  $(X, *)$  is permutational. If  $(X, *)$  satisfies (1.2) then  $(y * x) * (y * z) = (x * y) * (x * z) = (y * y) * (y * z)$  and substituting  $y \setminus^* z$  for  $z$  and  $y \setminus^* x$  for  $x$  again yields  $x * z = (y * y) * z$ .  $\square$

We will return to twisted Ward left quasigroups in Section 4.

### 3. TWISTED WARD QUASIGROUPS

A quasigroup  $(X, *)$  is a *twisted Ward quasigroup* if it satisfies the identity (tW).

Note that in Example 2.8,  $(X, *)$  is a quasigroup if and only if  $\varphi \in \text{Aut}(X, +)$ , in which case  $(X, *)$  satisfies (tW) if and only if  $\varphi = -\psi$ . This motivates the following construction.

**Example 3.1.** Let  $(X, \cdot)$  be a group,  $\psi \in \text{Aut}(X, \cdot)$  and  $c \in X$ . Then  $(X, *) = \text{tWq}(X, \cdot, \psi, c)$  defined by

$$x * y = c\psi(x^{-1}y)$$

is a twisted Ward quasigroup. Indeed, to verify (tW), we compute

$$(x * y) * (x * z) = (c\psi(x^{-1}y)) * (c\psi(x^{-1}z)) = c\psi((c\psi(x^{-1}y))^{-1}c\psi(x^{-1}z)) = c\psi(\psi(y^{-1}z)),$$

which is independent of  $x$  and therefore equal to  $(y * y) * (y * z)$ .

As we shall see in Theorem 3.7, all twisted Ward quasigroups are of the form  $\text{tWq}(X, \cdot, \psi, c)$ . We start by proving in two ways that every twisted Ward quasigroup is isotopic to a group. The first proof uses the quadrangle criterion known from the theory of latin squares and the second proof is based on the structure of the displacement group.

Recall that two quasigroups  $(X, \cdot), (Y, *)$  are *isotopic* if there are bijections  $\alpha, \beta, \gamma : X \rightarrow Y$  such that  $\alpha(x) * \beta(y) = \gamma(x \cdot y)$  for every  $x, y \in X$ . Replacing  $(Y, *)$  with an isomorphic copy, we can assume that  $\gamma = 1$  in an isotopism [17, Theorem III.1.4].

**Proposition 3.2** ([3, p. 18] or [6, Theorem 2.2]). *A quasigroup  $(X, *)$  is isotopic to a group if and only if it satisfies the quadrangle criterion, i.e., for every  $a_i, b_i, c_i, d_i \in X$ , if  $a_1 * c_1 = a_2 * c_2$ ,  $a_1 * d_1 = a_2 * d_2$  and  $b_1 * c_1 = b_2 * c_2$  then  $b_1 * d_1 = b_2 * d_2$ .*

**Lemma 3.3.** *Let  $(X, *)$  be a twisted Ward quasigroup and  $a_1, a_2, c_1, c_2 \in X$ . Then:*

- (i) *The squaring map  $x \mapsto x * x$  is constant.*
- (ii) *If  $a_1 * c_1 = a_2 * c_2$ , then  $L_{a_1}L_{c_1}^{-1} = L_{a_2}L_{c_2}^{-1}$ .*

*Proof.* (i) From (tW),  $(x * y) * (x * y) = (y * y) * (y * y)$  for every  $x, y \in X$ . Upon substituting  $x \setminus^* y$  for  $x$ , we see that  $x * x$  is independent of  $x$ .

(ii) Let us again write  $x * y = xy$ . Note that  $(xx)(x(y \setminus z)) = (yx)(y(y \setminus z)) = (yx)z$  is an instance of (tW) and therefore  $(c_2c_2)(c_2(a_2 \setminus (a_1x))) = (a_2c_2)(a_1x) = (a_1c_1)(a_1x) = (c_1c_1)(c_1x)$ , using (tW) again in the last step. Canceling the unique square and dividing on the left by  $c_2$ , we get  $a_2 \setminus (a_1x) = c_2 \setminus (c_1x)$ . Substituting  $c_1 \setminus x$  for  $x$  and multiplying on the left by  $a_2$ , we finally get  $a_1(c_1 \setminus x) = a_2(c_2 \setminus x)$ .  $\square$

**Proposition 3.4.** *Every twisted Ward quasigroup is isotopic to a group.*

*Proof.* Suppose that  $(X, \cdot)$  is a twisted Ward quasigroup and the assumptions of the quadrangle criterion are satisfied. Applying Lemma 3.3(ii) to equalities  $a_1c_1 = a_2c_2$  and  $b_1c_1 = b_2c_2$ , we get  $d_2 = a_2 \setminus (a_2d_2) = a_2 \setminus (a_1d_1) = a_2 \setminus (a_1(c_1 \setminus (c_1d_1))) = a_2 \setminus (a_2(c_2 \setminus (c_1d_1))) = c_2 \setminus (c_1d_1)$  and thus  $b_2d_2 = b_2(c_2 \setminus (c_1d_1)) = b_1(c_1 \setminus (c_1d_1)) = b_1d_1$ . We are done by Proposition 3.2.  $\square$

The *left multiplication group* of a quasigroup  $(X, *)$  is the permutation group generated by all left translations, i.e.,

$$\text{LMlt}(X) = \langle L_x : x \in X \rangle.$$

As in [2], we define the *positive* (resp. *negative*) *displacement group* of  $(X, *)$  as the subgroup of  $\text{LMlt}(X)$  generated by all positive (resp. negative) displacements, that is,

$$\text{Dis}^+(X) = \langle L_x L_y^{-1} : x, y \in X \rangle, \quad \text{Dis}^-(X) = \langle L_x^{-1} L_y : x, y \in X \rangle.$$

The *displacement group* of  $(X, *)$  is then the group

$$\text{Dis}(X) = \langle L_x L_y^{-1}, L_x^{-1} L_y : x, y \in X \rangle.$$

Note that  $\text{Dis}^+(X) = \langle L_e L_x^{-1} : x \in X \rangle$  for any fixed  $e \in X$  since  $L_x L_y^{-1} = (L_e L_x^{-1})^{-1} (L_e L_y^{-1})$ , and  $\text{Dis}^-(X) = \langle L_x^{-1} L_e : x \in X \rangle$  since  $L_x^{-1} L_y = (L_x^{-1} L_e) (L_y^{-1} L_e)^{-1}$ .

A permutation group  $G$  acts *regularly* on a set  $X$  if for every  $x, y \in X$  there is a unique  $g \in G$  such that  $g(x) = y$ . Recall the following result of Drápal:

**Proposition 3.5.** [4, Proposition 5.2] *A quasigroup  $X$  is isotopic to a group if and only if  $\text{Dis}^+(X)$  acts regularly on  $X$ . In such a case,  $X$  is isotopic to  $\text{Dis}^+(X)$ .*

It follows from Propositions 3.4 and 3.5 that every twisted Ward quasigroup  $X$  is isotopic to the group  $\text{Dis}^+(X)$ , which acts regularly on  $X$ . Here is an alternative proof of this fact which does not refer to Propositions 3.2 and 3.5.

**Lemma 3.6.** *Let  $X = (X, *)$  be a twisted Ward quasigroup and let  $e$  denote the unique square in  $X$ . Then:*

- (i)  $\text{Dis}(X) = \text{Dis}^+(X) = \text{Dis}^-(X)$ .
- (ii)  $(L_x^{-1} L_e)(L_y^{-1} L_e) = L_{(x/*e)*(e*y)}^{-1} L_e$  and  $(L_x^{-1} L_e)^{-1} = L_{(e*x)*e}^{-1} L_e$  for every  $x, y \in X$ .
- (iii)  $\text{Dis}(X)$  is equal to  $\{L_x^{-1} L_e : x \in X\}$  and is isomorphic to the group isotope  $(X, \diamond)$ , where  $x \diamond y = (x/*e) * (e*y)$ .

*Proof.* (i) The identity (tW) says  $L_{x*y} L_x = L_{y*y} L_y = L_e L_y$  and hence is equivalent to  $L_x L_y^{-1} = L_{x*y}^{-1} L_e$ , which shows that  $\text{Dis}^+(X) \leq \text{Dis}^-(X)$ . Replacing  $y$  with  $x*y$ , we obtain the identity

$$L_x L_{x*y}^{-1} = L_y^{-1} L_e, \tag{3.1}$$

which implies  $\text{Dis}^-(X) \leq \text{Dis}^+(X)$ . Hence  $\text{Dis}(X) = \text{Dis}^+(X) = \text{Dis}^-(X)$ .

(ii) Fix  $x, y \in X$  and let  $u = x/*e$  so that  $u*x = e$ . By a repeated application of (3.1), we have

$$\begin{aligned} (L_x^{-1} L_e)(L_y^{-1} L_e) &= (L_u L_{u*x}^{-1})(L_e L_{e*y}^{-1}) = L_u (L_{u*x}^{-1} L_e) L_{e*y}^{-1} \\ &= L_u L_{e*y}^{-1} = L_u L_{u*(u*(e*y))}^{-1} = L_{u*(e*y)}^{-1} L_e = L_{(x/*e)*(e*y)}^{-1} L_e. \end{aligned}$$

Using (3.1) again, we also have

$$(L_x^{-1} L_e)^{-1} = (L_e L_{e*x}^{-1})^{-1} = L_{e*x} L_e^{-1} = L_{e*x} L_{(e*x)*((e*x)*e)}^{-1} = L_{(e*x)*e}^{-1} L_e.$$

(iii) Part (ii) proves that  $\text{Dis}(X) = \text{Dis}^-(X)$  is equal to  $\{L_x^{-1} L_e : x \in X\}$  and is isomorphic to  $(X, \diamond)$ , where  $x \diamond y = (x/*e) * (e*y)$ , which therefore has to be a group. Clearly,  $(X, \diamond)$  is isotopic to  $(X, *)$ .  $\square$

We proceed to describe all twisted Ward quasigroups.



**Theorem 3.7.** *Let  $(X, *)$  be a quasigroup. Then  $(X, *)$  is a twisted Ward quasigroup if and only if there is a group  $(X, \cdot)$ ,  $\psi \in \text{Aut}(X, \cdot)$  and  $c \in X$  such that  $x * y = c\psi(x^{-1}y)$  for every  $x, y \in X$ .*

*Proof.* We have verified the converse implication in Example 3.1. For the direct implication, suppose that  $(X, *)$  is a twisted Ward quasigroup. By Proposition 3.4,  $(X, *)$  is isotopic to a group  $(X, \cdot)$ , i.e., there are permutations  $\varphi, \psi$  of  $X$  such that  $x * y = \varphi(x)\psi(y)$  for all  $x, y \in X$ . We may assume without loss of generality that  $\psi(1) = 1$ , otherwise set  $\bar{\varphi}(x) = \varphi(x)\psi(1)$  and  $\bar{\psi}(y) = \psi(1)^{-1}\psi(y)$  to obtain  $x * y = \bar{\varphi}(x)\bar{\psi}(y)$  and  $\bar{\psi}(1) = 1$ .

Writing (tW) in terms of  $\cdot, \varphi$  and  $\psi$ , and replacing  $z$  with  $\psi^{-1}(z)$ , we have

$$\varphi(\varphi(x)\psi(y)) \cdot \psi(\varphi(x)z) = \varphi(\varphi(y)\psi(y)) \cdot \psi(\varphi(y)z)$$

for all  $x, y, z \in X$ . Rearranging this, we have

$$\varphi(\varphi(y)\psi(y))^{-1} \cdot \varphi(\varphi(x)\psi(y)) = \psi(\varphi(y)z) \cdot \psi(\varphi(x)z)^{-1}.$$

Note that the left hand side is independent of  $z$ . Comparing the right hand sides upon substituting  $z = 1$  and  $z = \varphi(x)^{-1}$ , respectively, we obtain

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

for all  $x, y \in X$ , where we have used  $\psi(1) = 1$ . Since  $\varphi$  is bijective, this is equivalent to

$$\psi(y)\psi(x)^{-1} = \psi(yx^{-1})$$

for all  $x, y \in X$ , and thus  $\psi$  is an automorphism of the group  $(X, \cdot)$ .

Writing (tW) in terms of  $\cdot, \varphi$  and  $\psi$  again and substituting  $y = z = 1$ , we have

$$\varphi(\varphi(x)) \cdot \psi(\varphi(x)) = \varphi(\varphi(1)) \cdot \psi(\varphi(1))$$

for every  $x \in X$ , with the right hand side being constant, say equal to  $c$ . Since  $\varphi$  is bijective, this is equivalent to  $\varphi(x)\psi(x) = c$ . Then  $\varphi(x) = c\psi(x)^{-1}$  and  $x * y = c\psi(x)^{-1}\psi(y) = c\psi(x^{-1}y)$  for every  $x, y \in X$ .  $\square$

Since isotopic groups are isomorphic [17, Corollary III.2.3], the following result solves the isomorphism problem for twisted Ward quasigroups.

**Proposition 3.8.** *Let  $(X, \cdot)$  be a group,  $\varphi, \psi \in \text{Aut}(X, \cdot)$  and  $c \in X$ . Then:*

- (i) *The mapping  $x \mapsto cx$  is an isomorphism  $\text{tWq}(X, \cdot, \varphi, 1) \rightarrow \text{tWq}(X, \cdot, \varphi, c)$ .*
- (ii) *The twisted Ward quasigroups  $\text{tWq}(X, \cdot, \varphi, 1)$  and  $\text{tWq}(X, \cdot, \psi, 1)$  are isomorphic if and only if  $\varphi, \psi$  are conjugate in  $\text{Aut}(X, \cdot)$ .*

*Proof.* Let us denote the multiplication in  $\text{tWq}(X, \cdot, \varphi, c)$  by  $*_{\varphi, c}$ .

- (i) For every  $x, y \in X$ , we have  $(cx) *_{\varphi, c} (cy) = c\varphi((cx)^{-1}(cy)) = c\varphi(x^{-1}y) = c(x *_{\varphi, 1} y)$ .
- (ii) If  $\psi = \rho\varphi\rho^{-1}$  for some  $\rho \in \text{Aut}(X, \cdot)$ , then

$$\rho(x *_{\varphi, 1} y) = \rho\varphi(x^{-1}y) = \psi\rho(x^{-1}y) = \psi(\rho(x)^{-1}\rho(y)) = \rho(x) *_{\psi, 1} \rho(y).$$

Conversely, if  $\rho$  is an isomorphism  $\text{tWq}(X, \cdot, \varphi, 1) \rightarrow \text{tWq}(X, \cdot, \psi, 1)$  then

$$\rho\varphi(x^{-1}y) = \psi(\rho(x)^{-1}\rho(y)) \tag{3.2}$$

for every  $x, y \in X$ . Upon substituting  $x = 1$  into (3.2) we obtain  $\rho\varphi = \psi\rho$ . Applying  $\psi^{-1}$  to both sides of (3.2), we then get  $\rho(x^{-1}y) = \rho(x)^{-1}\rho(y)$ , so  $\rho \in \text{Aut}(X, \cdot)$ .  $\square$

For a group  $G$ , let  $cc(G)$  denote the number of conjugacy classes of  $G$ .

**Corollary 3.9.** *The number of twisted Ward quasigroups of order  $n$  up to isomorphism is*

$$q(n) = \sum_G cc(\text{Aut}(G)),$$

where the summation runs over all groups  $G$  of order  $n$  up to isomorphism.

Returning to braidings, we deduce:

**Theorem 3.10.** *Let  $r : X \times X \rightarrow X \times X$  be given by  $r(x, y) = (x \circ y, x \bullet y)$ . Then  $r$  is an idempotent latin braiding if and only if there is a group  $(X, \cdot)$ , an automorphism  $\varphi \in \text{Aut}(X, \cdot)$  and  $c \in X$  such that*

$$r(x, y) = (x\varphi(c)^{-1}\varphi(y), c).$$

Moreover, up to isomorphism, we can take  $c = 1$  and  $\varphi$  up to conjugation in  $\text{Aut}(X, \cdot)$ .

*Proof.* By Theorem 2.4,  $r$  is an idempotent left nondegenerate braiding if and only if  $r(x, y) = (x \setminus y, (x \setminus y) * (x \setminus y))$  for a twisted Ward left quasigroup  $(X, *)$ , and  $r$  is latin if and only if  $(X, *)$  is a twisted Ward quasigroup. Then, by Theorem 3.7,  $x * y = c\psi(x^{-1}y)$  for some group  $(X, \cdot)$ ,  $\psi \in \text{Aut}(X, \cdot)$  and  $c \in X$ . Then certainly  $(x \setminus y) * (x \setminus y) = c$ , and since  $x \setminus y = x\psi^{-1}(c^{-1}y)$ , we can write  $x \circ y = x \setminus y = x\varphi(c)^{-1}\varphi(y)$  by taking  $\varphi = \psi^{-1}$ . The last part follows by Proposition 3.8.  $\square$

#### 4. THE CAYLEY KERNEL, SQUARING AND TWISTED WARD LEFT QUASIGROUPS OF PRIME ORDER

For an equivalence relation  $R$  on a set  $X$ , let  $X_R$  be a complete set of representatives of the equivalence classes of  $R$  and let  $[x]_R$  denote the equivalence class of  $R$  containing the element  $x$ .

On a left quasigroup  $(X, \cdot)$  define two equivalence relations

$$\begin{aligned} x \sim y &\Leftrightarrow L_x = L_y, \\ x \equiv y &\Leftrightarrow xx = yy. \end{aligned}$$

The equivalence relation  $\sim$  is usually called the *Cayley kernel* in this context. If  $\sim$  is the full equivalence  $X \times X$  then  $(X, \cdot)$  is called *permutational*, cf. Example 2.9. If  $\sim$  is the equality relation  $\{(x, x) : x \in X\}$  then  $(X, \cdot)$  is called *faithful*.

**Lemma 4.1.** *Let  $(X, \cdot)$  be a left quasigroup. Then the equivalence relations  $\sim$  and  $\equiv$  intersect trivially and the following inequalities hold for every  $x \in X$ :*

- (i)  $|[x]_{\equiv}| \leq |X_{\sim}|$ ,
- (ii)  $|[x]_{\sim}| \leq |X_{\equiv}|$ ,
- (iii)  $|X| \leq |X_{\sim}| \cdot |X_{\equiv}|$ .

*Proof.* Let  $x \sim y$  and  $x \equiv y$ . Then  $xy = yy = xx$  and left cancellation yields  $x = y$ . The inequalities (i) and (ii) are then immediate consequences. Finally,  $|X| = \sum_{x \in X_{\sim}} |[x]_{\sim}| \leq |X_{\sim}| \cdot |X_{\equiv}|$  by (ii).  $\square$

In general left quasigroups, neither of the two equivalences is a congruence. In finite twisted Ward left quasigroups, the Cayley kernel is not always a congruence (cf. Example 4.2) but  $\equiv$  is a congruence (cf. Proposition 4.3). We do not know whether  $\equiv$  is a congruence in infinite Ward left quasigroups, too.

**Example 4.2.** In the twisted Ward left quasigroup with multiplication table

	1	2	3	4
1	1	3	2	4
2	1	3	2	4
3	4	2	3	1
4	4	2	3	1

the Cayley kernel is not a congruence:  $L_1 = L_2$  and  $L_{2,1} = L_1 \neq L_3 = L_{2,2}$ .

**Proposition 4.3.** *In a finite twisted Ward left quasigroup, the equivalence  $\equiv$  is a congruence.*

*Proof.* Since  $(xz)(xz)$  does not depend on  $x$  by (tW), we always have  $xz \equiv yz$ . If  $x \equiv y$  then  $(zx)(zx) = (xx)(xx) = (yy)(yy) = (zy)(zy)$  by (tW), and hence  $zx \equiv zy$ . By finiteness,  $\equiv$  is invariant under left division, too.  $\square$

We proceed towards a classification of twisted Ward left quasigroups of prime order.

**Lemma 4.4.** *Let  $(X, \cdot)$  be a twisted Ward left quasigroup and  $x, y \in X$ . If  $L_x, L_y$  agree at a point then  $L_x = L_y$ . In particular, every finite faithful twisted Ward left quasigroup is a quasigroup.*

*Proof.* Assume that  $xc = yc$  for some  $c \in X$ . Then for every  $z \in X$  we have  $(xc)(xz) = (cc)(cz) = (yc)(yz) = (xc)(yz)$  and we obtain  $xz = yz$  by left cancellation.  $\square$

**Proposition 4.5.** *Let  $(X, \cdot)$  be a twisted Ward left quasigroup. Then the following conditions hold for every  $x \in X$ :*

- (i)  $|[x]_{\equiv}| = |X_{\sim}|$ ,
- (ii) *if  $X$  is finite then*  $|[x]_{\sim}| = |X_{\equiv}|$ ,
- (iii)  $|X| = |X_{\equiv}| \cdot |X_{\sim}|$ .

*Proof.* (i) Fix  $z \in X$  and observe that for every  $x \in X$  we have  $(xz)(xz) = (zz)(zz)$ . Hence the elements  $R_z(X) = \{xz : x \in X\}$  in the column indexed by  $z$  all have the same square. By Lemma 4.4, the cardinality of  $R_z(X)$  is equal to  $|X_{\sim}|$ . Hence  $|[u]_{\equiv}| \geq |X_{\sim}|$  for every  $u \in R_z(x)$ , and Lemma 4.1(i) asserts equality. By varying  $z$ , we will encounter all elements of  $X$  in this fashion.

(iii) By (i), all blocks of  $\equiv$  have the same size  $|X_{\sim}|$ , so  $|X| = |X_{\equiv}| \cdot |X_{\sim}|$ .

(ii) By Lemma 4.1(ii) and by part (iii), we have  $|X| = \sum_{x \in X_{\sim}} |[x]_{\sim}| \leq |X_{\sim}| \cdot |X_{\equiv}| = |X|$ . Hence we have an equality and  $|[x]_{\sim}| = |X_{\equiv}|$  follows because  $|[x]_{\sim}| \leq |X_{\equiv}|$  for every  $x \in X$ .  $\square$

**Example 4.6.** The sets  $X_{\sim}, X_{\equiv}$  may have different cardinalities. For instance, in the twisted Ward left quasigroup  $X$  with multiplication table

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

we have  $|[x]_{\sim}| = 3$  and  $|[x]_{\equiv}| = 2$  for every  $x \in X$ . Note that  $X$  is neither permutational nor a quasigroup.

**Theorem 4.7.** *Every twisted Ward left quasigroup of prime order is either permutational or a quasigroup.*

*Proof.* Let  $X$  be a twisted Ward left quasigroup of prime order. By Proposition 4.5, all equivalence classes of  $\sim$  have the same cardinality. Since  $X$  is of prime order, it follows that either  $\sim$  has a single equivalence class or all equivalence classes of  $\sim$  are singletons. In the former case,  $X$  is permutational. In the latter case,  $X$  is faithful and thus a quasigroup by Lemma 4.4.  $\square$

**Corollary 4.8.** *Let  $q(n)$  (resp.  $\ell(n)$ ) denote the number of twisted Ward quasigroups (resp. twisted Ward left quasigroups) of order  $n$  up to isomorphism. Let  $p(n)$  be the partition number, i.e., the number of ways in which  $n$  can be written as a sum of nonincreasing positive integers. Then  $\ell(n) \geq q(n) + p(n)$  if  $n > 1$ . Moreover, if  $n$  is prime then  $\ell(n) = q(n) + p(n) = n - 1 + p(n)$ .*

*Proof.* Denote by  $(X, f)$  the permutational (Ward) left quasigroup with multiplication given by  $x * y = f(y)$ . It is easy to see that  $(X, f)$  is isomorphic to  $(X, g)$  if and only if  $f$  and  $g$  are conjugate in the symmetric group  $S_X$ . Recall that there are  $p(|X|)$  conjugacy classes in  $S_X$ . Moreover, if  $|X| > 1$  then  $(X, f)$  is never a quasigroup. Hence  $\ell(n) \geq q(n) + p(n)$  if  $n > 1$ .

Suppose that  $n$  is prime. By Theorem 4.7,  $\ell(n) = q(n) + p(n)$ . The only group of order  $n$  is the cyclic group  $C_n$ . Since  $\text{Aut}(C_n)$  is an abelian group of order  $n - 1$ , we have  $q(n) = n - 1$  by Corollary 3.9.  $\square$

The following table summarizes the numbers of twisted Ward left quasigroups  $\ell(n)$  and twisted Ward quasigroups  $q(n)$  of order  $n \leq 11$  up to isomorphism, as well as the partition number  $p(n)$ .

$n$	1	2	3	4	5	6	7	8	9	10	11
$\ell(n)$	1	3	5	14	11	31	21	93	64	?	66
$q(n)$	1	1	2	5	4	5	6	25	14	9	10
$p(n)$	1	2	3	5	7	11	15	22	30	42	56

Neither of the sequences  $(\ell(n))$ ,  $(q(n))$  appears in the Online Encyclopedia of Integer Sequences [16]. It is not difficult to calculate the numbers  $q(n)$  for small values of  $n$  by hand, using Corollary 3.9. We can then calculate  $\ell(n)$  for prime orders  $n$  from Corollary 4.8. The remaining values  $\ell(n)$  (and for independent verification also all other values except for  $\ell(10)$  and  $\ell(11)$ ) were calculated by the finite model builder Mace4 [14].

We conclude the paper with a construction that yields all finite twisted left Ward quasigroups in principle.

**Proposition 4.9.** *Let  $X$  and  $A$  be sets. For every  $x \in X$ , let  $f_x$  be a bijection on  $X \times A$  and let us write  $f_x(y, b) = (f_x^{[1]}(y, b), f_x^{[2]}(y, b))$ . Define  $(X \times A, *)$  by*

$$(x, a) * (y, b) = f_x(y, b).$$

*Then  $(X \times A, *)$  is a twisted Ward left quasigroup if and only if*

$$f_{f_x^{[1]}(y, b)} f_x \tag{4.1}$$

*is independent of  $x$ . Moreover, every finite twisted Ward left quasigroup is isomorphic to one of this form.*

*Proof.* The groupoid  $(X \times A, *)$  is a left quasigroup. The identity (tW) requires that the expression  $((x, a) * (y, b)) * ((x, a) * (z, c))$  is independent of  $(x, a)$ . Expanding the expression, we obtain

$$f_x(y, b) * f_x(z, c) = (f_x^{[1]}(y, b), f_x^{[2]}(y, b)) * f_x(z, c) = f_{f_x^{[1]}(y, b)} f_x(z, c).$$

Hence  $(X \times A, *)$  satisfies (tW) if and only if (4.1) is independent of  $x$ .

By Proposition 4.5, the Cayley kernel of a finite twisted Ward left quasigroup  $W$  has blocks of the same size, say each bijectively mapped onto a fixed set  $A$ . We can then represent the underlying set of  $W$  as  $X \times A$  for a suitable set  $X$ . The product  $(x, a)$  and  $(y, b)$  in  $W$  depends only on  $x$ ,  $y$  and  $b$ . Moreover, for a fixed  $(x, a)$ , the left translation by  $(x, a)$  in  $W$  is a bijection of  $X \times A$  depending on  $x$  only, and this is how we obtain the mappings  $f_x$ .  $\square$

## REFERENCES

- [1] N. Andruskiewitsch and M. Graña, *From racks to pointed Hopf algebras*, Adv. Math. **178** (2003), no. **2**, 177–243.
- [2] M. Bonatto, M. Kinyon, D. Stanovský, P. Vojtěchovský, *Latin involutive solutions of the Yang-Baxter equation*, submitted.
- [3] J. Dénes and A.D. Keedwell, *Latin squares and their applications*, Academic Press, New York and London, 1974.
- [4] A. Drápal, *Group isotopes and a holomorphic action*, Result. Math. **54/3–4** (2009), 253–272.
- [5] V. G. Drinfeld, *On unsolved problems in quantum group theory*, Quantum Groups, Lecture Notes in Math. **1510**, Springer-Verlag, Berlin, 1992, 1–8.
- [6] A.B. Evans, *Orthogonal Latin Squares Based on Groups*, Developments in Mathematics **57**, Springer, 2018.
- [7] M. Elhamedi and S. Nelson, *Quandlesan introduction to the algebra of knots*, Student Mathematical Library **74**, American Mathematical Society, Providence, RI, 2015.
- [8] P. Etingof, A. Soloviev, R. Guralnick, *Indecomposable set-theoretical solutions to the quantum Yang-Baxter equation on a set with a prime number of elements*. J. Algebra **242** (2001), no. **2**, 709–719.
- [9] R. Fenn and C. Rourke, *Racks and links in codimension two*, J. Knot Theory Ramifications **1** (1992), no. **4**, 343–406.
- [10] K. W. Johnson and P. Vojtěchovský, *Right division in groups, Dedekind-Frobenius group matrices, and Ward quasigroups*, Abh. Math. Sem. Univ. Hamburg **75** (2005), 121–136.

- [11] V.F.R. Jones, *Hecke algebra representations of braid groups and link polynomials*, Ann. of Math. (2) **126** (1987), no. **2**, 335–388.
- [12] A. Hulpke, D. Stanovský and P. Vojtěchovský, *Connected quandles and transitive groups*, Journal of Pure and Applied Algebra **220** (February 2016), no. **2**, 735–758.
- [13] V. Lebed, *Cohomology of idempotent braidings with applications to factorizable monoids*, Internat. J. Algebra Comput. **27** (2017), no. **4**, 421–454.
- [14] W. McCune, *Mace4 and Prover9*, <https://www.cs.unm.edu/~mccune/prover9>
- [15] T. Nosaka, *Quandles and topological pairs. Symmetry, knots, and cohomology*. Springer Briefs in Mathematics. Springer, Singapore, 2017.
- [16] OEIS Foundation Inc. (2019), The On-Line Encyclopedia of Integer Sequences, <http://oeis.org>
- [17] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Sigma Ser. Pure Math. **7**, Heldermann, Berlin, 1990.
- [18] M. Polonijo, *A note on Ward quasigroups*, An. Ştiinţ. Univ. “Al. I. Cuza” Iaşi Sect. I a Mat. (N.S.) **32** (1986), no. **2**, 5–10.
- [19] D. G. Rabinow, *Independent sets of postulates for abelian groups and fields in terms of the inverse operations*, American Journal of Mathematics **59**, no. **1** (Jan., 1937), 211–224.
- [20] W. Rump, *A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation*, Adv. Math. **193** (2005), 40–55.
- [21] D. Stanovský, *A guide to self-distributive quasigroups, or latin quandles*, Quasigroups and Related Systems **23/1** (2015), 91–128.
- [22] V.G. Turaev, *The Yang-Baxter equation and invariants of links*, Invent. Math. **92** (1988), no. **3**, 527–553.
- [23] M. Ward, *Postulates for the inverse operations in a group*, Transactions of the American Mathematical Society **32**, no. **3** (Jul., 1930), 520–526.

DEPARTMENT OF ALGEBRA, FACULTY OF MATHEMATICS AND PHYSICS, CHARLES UNIVERSITY, PRAGUE, CZECHIA  
*E-mail address:* [stanovsk@karlin.mff.cuni.cz](mailto:stanovsk@karlin.mff.cuni.cz)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF DENVER, DENVER (CO), USA  
*E-mail address:* [petr@math.du.edu](mailto:petr@math.du.edu)