

## QUASIGROUP AUTOMORPHISMS AND THE NORTON-STEIN COMPLEX

BRENT L. KERBY AND JONATHAN D. H. SMITH

(Communicated by Jonathan I. Hall)

ABSTRACT. Suppose that  $d > 1$  is the largest power of two that divides the order of a finite quasigroup  $Q$ . It then follows that each automorphism of  $Q$  must contain a cycle of length not divisible by  $d$  in its disjoint cycle decomposition. The proof is obtained by considering the action induced by the automorphism on a certain orientable surface originally described in a more restricted context by Norton and Stein.

### 1. INTRODUCTION

For an automorphism of a finite quasigroup (or Latin square)  $Q$ , the multiset of cycle lengths in the disjoint cycle decomposition of the automorphism is called the *cycle structure* of the automorphism. It is then natural to pose the following question:

Given a positive integer  $n$ , what are the possible cycle structures of automorphisms of quasigroups of order  $n$ ?

The question was addressed in [2] for small values of  $n$  and in [1] for the special case of automorphisms having only one nontrivial cycle. The general case remains unsolved, but in this paper we use methods from algebraic topology to resolve some of the more difficult cases.

Algebraic topology normally proceeds by a functorial association of algebraic objects to topological spaces. We reverse this procedure in §2 by constructing an orientable surface  $S_Q$  for each finite quasigroup  $Q$ , such that the association  $Q \mapsto S_Q$  is functorial (Theorem 2.3). In §3 we endow the surface with the structure of a CW-complex. This clarifies and extends a construction of Norton and Stein [6] that was limited to the case of idempotent quasigroups.

Using our construction, we present a somewhat simplified proof of a result of Stein [7, Th. 1.1]:

**Corollary 3.4.** *Let  $Q$  be a finite quasigroup, with  $|Q| \equiv 2 \pmod{4}$ . Then the automorphism group of  $Q$  does not act transitively.*

In §4, we state and prove our main result, which depends on a lemma established in §5. The proof of the lemma uses a monodromy technique dating back to Nielsen [5]. The main result is as follows:

---

Received by the editors November 11, 2009.

2010 *Mathematics Subject Classification.* Primary 20N05, 05B15.

*Key words and phrases.* Latin square, quasigroup, surface, monodromy.

**Theorem 4.2.** *If  $2^l$  (with  $l > 0$ ) is the largest power of two dividing the order of a finite quasigroup  $Q$ , then the disjoint cycle decomposition of each automorphism of  $Q$  must contain a cycle whose length is not divisible by  $2^l$ .*

Some indication of the scope of this result is obtained by considering Falcón’s description [2] of the possible cycle structures of autotopies of quasigroups  $Q$  with  $|Q| \leq 11$ . In that work, three potential cycle structures of automorphisms could only be ruled out by an exhaustive computer search. These were  $2^3$  (i.e., a cycle structure consisting of three disjoint transpositions) for quasigroups of order 6, and  $6^1 4^1$  and  $2^5$  for quasigroups of order 10. All these cases are now forbidden by Theorem 4.2 (with  $l = 1$ ).

2. CONSTRUCTION OF THE NORTON-STEIN SURFACE

Let  $Q$  be a quasigroup of order  $n$ . Then  $Q$  is determined by its (*ternary*) multiplication table

$$T_Q = \{(a, b, c) \in Q^3 \mid ab = c\}.$$

For each triple  $t = (a, b, c)$  in  $T_Q$ , construct an equilateral triangle whose vertices will be labeled  $a$ ,  $b$ , and  $c$ , circumnavigating the triangle in the counter-clockwise direction, and whose edges will be labeled  $(a, b)_0$ ,  $(b, c)_1$ ,  $(c, a)_2$ , as shown in Figure 1.

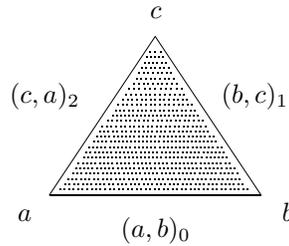


FIGURE 1. A basic triangle.

The disjoint union of these  $n^2$  triangles forms a topological space, a subspace of the Euclidean plane, which we will denote by  $P_Q$ . Note that by definition, each triangle contains three distinct edges, even though the vertex labels  $a$ ,  $b$ , and  $c$  may not all be distinct. An edge with a label of the form  $(a, a)_i$  will be called a *degenerate edge*, while the triangle corresponding to a triple of the form  $(a, a, a)$  will be called a *degenerate triangle*.

**Example 2.1.** Consider the cyclic group  $Q$  of order 3. Write its usual multiplication table as

$Q$		e	a	b
e		e	a	b
a		a	b	e
b		b	e	a

The corresponding space  $P_Q$  is shown in Figure 2.

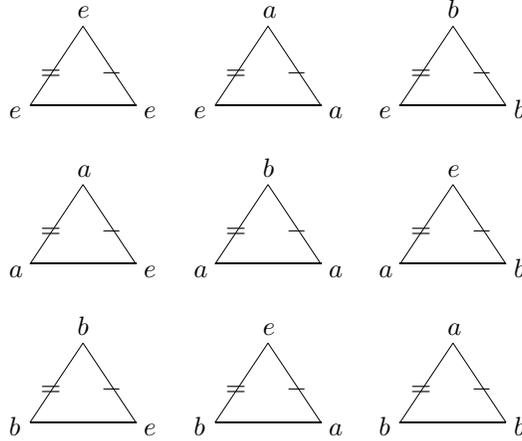


FIGURE 2. The space  $P_Q$  for the cyclic group  $Q$  of order 3.

For convenience, we have omitted the full edge labels  $(a, b)_i$ , instead marking each edge  $(a, b)_i$  with 0, 1, or 2 slashes according as  $i = 0, 1, \text{ or } 2$ , respectively.

If  $n > 0$  there will be many vertices of  $P_Q$  with the same label. However, the quasigroup condition ensures that for each  $a, b \in Q$  and  $i \in \{0, 1, 2\}$  there is a unique edge with the label  $(a, b)_i$ . Likewise, there is a unique edge with the label  $(b, a)_i$ . Thus for each  $a, b$ , and  $i$  we may define a function (the so-called *pasting map*) which maps the edge  $(a, b)_i$  isometrically onto the edge  $(b, a)_i$ , the image proceeding clockwise as we proceed counter-clockwise in the domain, so that the vertex labeled  $a$  is mapped onto the other vertex labeled  $a$ , and the vertex labeled  $b$  is mapped onto the other vertex labeled  $b$ . If we identify points which correspond under the pasting map, then we obtain a topological quotient space of  $P_Q$  which we call the *Norton-Stein surface* of  $Q$  and denote by  $S_Q$ .

We will omit the proof that  $S_Q$  is a (usually disconnected) surface, since this fact is well known for spaces constructed by pasting polygons together in such a manner (see, e.g., [4]). The only issue here is that, in the case of a degenerate edge  $(a, a)_i$ , the edge is pasted onto itself with opposite orientation. Topologically, this simply collapses a triangle into a digon formed by the two remaining edges (see Figure 3).

A degenerate triangle  $(a, a, a)$  collapses further from a digon into a sphere. (See Figure 4, where the process is broken down into two steps.) The resulting quotient space will still be a surface.

Since the edges come in pairs which have opposite orientation under the pasting maps, it follows that the Norton-Stein surface is orientable (again see, e.g., [4] for details).

**Example 2.2.** For  $Q$  the cyclic group of order 3, Figure 5 shows the space resulting from  $P_Q$  after applying enough pasting maps so that the space falls into 3 closed

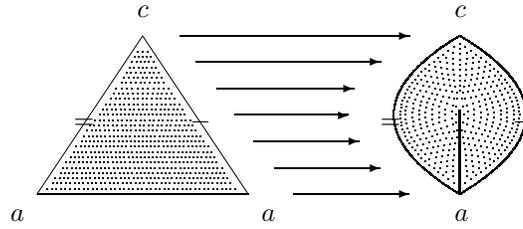


FIGURE 3. Collapse to a digon.

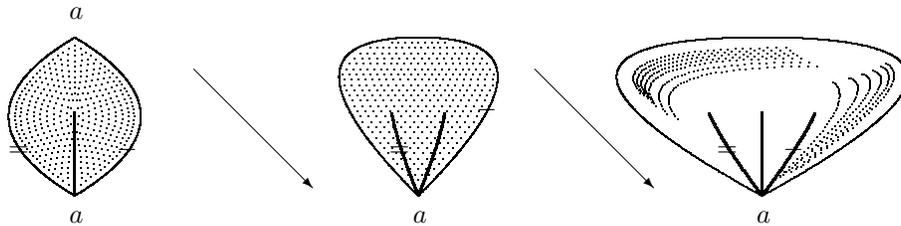


FIGURE 4. Collapse from a digon to a topological sphere.

polygons, each edge of which is paired with another edge (possibly itself) on the same polygon. From this it is evident that  $S_Q$  consists of 3 disconnected spheres.

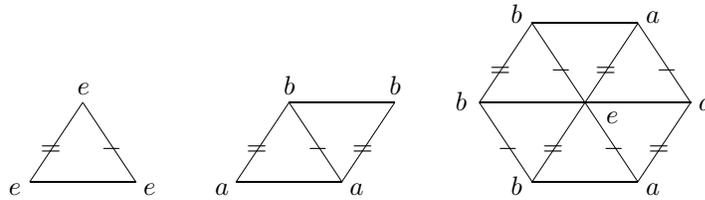


FIGURE 5. The space  $S_Q$  for the cyclic group  $Q$  of order 3.

The functorial nature of this construction of the Norton-Stein surface may be described as follows:

**Theorem 2.3.** *A homomorphism  $\psi : Q_1 \rightarrow Q_2$  of quasigroups induces a continuous map  $\psi_* : S_{Q_1} \rightarrow S_{Q_2}$  on the corresponding Norton-Stein surfaces. This correspondence determines a functor from the category of finite quasigroups and homomorphisms to the category of surfaces and continuous maps.*

*Proof.* First,  $\psi$  determines a map  $\bar{\psi} : P_{Q_1} \rightarrow P_{Q_2}$  by sending each triangle  $(a, b, c)$  of  $P_{Q_1}$  isometrically onto the corresponding triangle  $(\psi(a), \psi(b), \psi(c))$  of  $P_{Q_2}$ , such

that the vertices labeled  $a$ ,  $b$ , and  $c$  map to the vertices labeled  $\psi(a)$ ,  $\psi(b)$ , and  $\psi(c)$ , respectively. Then  $\bar{\psi}$  maps each edge  $(a, b)_i$  isometrically onto the edge  $(\psi(a), \psi(b))_i$ . It follows that if  $f_1$  is the pasting map between two edges  $(a, b)_i$  and  $(b, a)_i$  of  $P_{Q_1}$ , and  $x, y \in P_{Q_1}$  are such that  $f_1(x) = f_1(y)$ , then we also have  $f_2(\bar{\psi}(x)) = f_2(\bar{\psi}(y))$ , where  $f_2$  is the pasting map between the edges  $(\psi(a), \psi(b))_i$  and  $(\psi(b), \psi(a))_i$  of  $P_{Q_2}$ . Thus  $\bar{\psi}$  induces a well-defined continuous map  $\psi_*$  from the quotient space  $S_{Q_1}$  to the quotient space  $S_{Q_2}$ . That this correspondence determines a functor is straightforward to verify.  $\square$

**Corollary 2.4.** *For an automorphism  $\psi$  of a finite quasigroup  $Q$ , the orders of  $\psi_*$  and  $\psi$  are equal.*

*Proof.* Suppose that  $\psi$  and  $\psi_*$  have respective orders  $n$  and  $m$ . Then since  $\psi^n = 1$ , Theorem 2.3 implies  $\psi_*^n = 1$ . Hence  $m \leq n$ , and in particular  $m < \infty$ .

On the other hand, for each element  $q$  of  $Q$ , choose a vertex  $x_q$  in  $S_Q$  with label  $q$ . Now  $\psi_*^m(x_q) = x_q$ , so  $\psi^m(q) = q$ . Since the equality  $\psi^m(q) = q$  holds for each element  $q$  of  $Q$ , we have  $\psi^m = 1$  and thus  $n \leq m$ .  $\square$

### 3. THE NORTON-STEIN COMPLEX AND SOME APPLICATIONS

We now give  $S_Q$  the structure of a CW-complex. The 0-cells are defined to be the images of the vertices of  $P_Q$ . The 1-cells are the images of the nondegenerate edges, and a 2-cell is given by the image of the interior of a triangle of  $P_Q$  together with any degenerate edges of the triangle. With this added structure, we call  $S_Q$  the *Norton-Stein complex* of  $Q$ .

We assign the same labels to the 0-cells of  $S_Q$  as the corresponding vertices of  $P_Q$ . This is well-defined since only vertices with the same label are identified by the pasting maps. Given a nondegenerate edge  $(a, b)_i$  of  $P_Q$ , we assign the label  $\{a, b\}_i$  to the corresponding 1-cell in  $S_Q$ . Note that if  $n > 0$ ,  $S_Q$  will not be a simplicial complex, since it is possible that two distinct 2-cells may be incident with the same three 0-cells, and some 2-cells will be incident with only two 0-cells and 1-cells (if the corresponding triangle contains a degenerate edge). In the case of a degenerate triangle  $(a, a, a)$ , the corresponding 2-cell is incident with only one 0-cell and no 1-cells.

Although only vertices of  $P_Q$  with the same labels are identified in  $S_Q$ , it is not necessarily the case that *all* vertices with the same labels are identified. The number of distinct vertices of  $S_Q$  with the label  $q$  is denoted by  $\Phi(q)$ . It is clear that  $\Phi$  is invariant under isomorphisms. Thus if  $\psi : Q_1 \rightarrow Q_2$  is an isomorphism of quasigroups, then  $\Phi(\psi(q)) = \Phi(q)$ . The number

$$Z_Q = \sum_{q \in Q} \Phi(q)$$

is then an invariant of the quasigroup  $Q$ . We see that  $Z_Q$  is simply the number of vertices in the Norton-Stein complex of  $Q$ . The following result is then immediate.

**Theorem 3.1.** *For a finite quasigroup  $Q$ , the Euler characteristic of  $S_Q$  is*

$$\chi = Z_Q - 3n(n - 1)/2 + n^2.$$

This leads us to the following theorem, proved by Norton and Stein [6] in the special case of idempotent quasigroups.

**Theorem 3.2.** *For a quasigroup  $Q$  of order  $n$ ,*

$$(3.1) \quad Z_Q \equiv n(n+1)/2 \pmod{2}.$$

*Proof.* We have  $Z_Q \equiv 3n(n-1)/2 + n^2 \equiv n(n-1)/2 + n \equiv n(n+1)/2 \pmod{2}$  by Theorem 3.1, since the Euler characteristic of the orientable surface  $S_Q$  is even.  $\square$

*Remark 3.3.* The formula (3.1) differs from that of [6, Th. II], because our definition of  $Z_Q$  includes the vertices which are associated with the degenerate triangles  $(a, a, a)$ .

As shown by the following corollary, even the seemingly miniscule information about the Norton-Stein complex provided by Theorem 3.2 can lead to powerful conclusions about the associated quasigroup.

**Corollary 3.4** ([7]). *Let  $Q$  be a finite quasigroup, with  $|Q| \equiv 2 \pmod{4}$ . Then the automorphism group of  $Q$  does not act transitively.*

*Proof.* Suppose that  $Q$  had a transitive automorphism group. Then there would be a constant  $c$  such that  $\Phi(q) = c$  for all  $q \in Q$ . Hence

$$Z_Q = \sum_{q \in Q} \Phi(q) = c|Q| \equiv 0 \pmod{2}.$$

However, if  $|Q| = 4k + 2$  for some natural number  $k$ , Theorem 3.2 implies  $Z_Q \equiv (2k+1)(4k+3) \equiv 1 \pmod{2}$ .  $\square$

*Remark 3.5.* (a) Stein's original proof of Corollary 3.4 required an initial reduction to the case of idempotent quasigroups.

(b) Stein [8, Th. 9.9] observed that for each positive integer  $n$  not congruent to 2 modulo 4, there is a distributive quasigroup of order  $n$  with a transitive automorphism group (compare Feit's review of [3]): If  $n$  factors into powers of distinct primes  $p_1, p_2, \dots, p_k$  as  $p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ , an example is given by the direct product quasigroup  $\prod_{j=1}^k (\text{GF}(p_j^{e_j}), \circ_j)$  with  $x \circ_j y = \alpha_j x + (1 - \alpha_j)y$ , where  $\alpha_j$  is a constant arbitrarily chosen from  $\text{GF}(p_j^{e_j}) \setminus \{0, 1\}$ .

The same technique as in the proof of Corollary 3.4 serves to give the following special case of our main result.

**Corollary 3.6.** *Let  $\psi$  be an automorphism of a quasigroup  $Q$ , where  $|Q| \equiv 2 \pmod{4}$ . Then the disjoint cycle decomposition of  $\psi$  contains a cycle of odd length.*

*Proof.* If all the cycles of  $\psi$  have even length, then the elements of  $Q$  fall into orbits of even length under  $\langle \psi \rangle$ . The function  $\Phi$  is constant on each orbit. This implies that

$$Z_Q = \sum_{q \in Q} \Phi(q) \equiv 0 \pmod{2},$$

again contrary to the implication  $Z_Q \equiv 1 \pmod{2}$  of Theorem 3.2.  $\square$

As mentioned in the introduction, there are three impossible cycle structures of automorphisms which had to be ruled out by exhaustive computer search in [2]:  $2^3$ ,  $6^1 4^1$ , and  $2^5$ . All three of these cases are now forbidden by Corollary 3.6. However, the more elementary techniques of this section are not capable of eliminating such cycle structures as  $4^3$  (for quasigroups of order 12) or  $4^5$  (for quasigroups of order 20). Further progress requires the full generality of our main result, described in

the next section. This entails a considerably deeper application of the Norton-Stein complex.

4. THE MAIN RESULT

Given an automorphism  $\psi$  of a finite quasigroup  $Q$ , Theorem 2.3 yields a continuous automorphism  $\psi_*$  of the Norton-Stein surface  $S_Q$ . The group  $\langle \psi_* \rangle$  generated by  $\psi_*$  then acts by permuting the connected components of the surface  $S_Q$ . We may thus state the following lemma.

**Lemma 4.1.** *Let  $\psi$  be an automorphism of a finite quasigroup  $Q$ , and suppose that the disjoint cycle decomposition of  $\psi$  consists entirely of cycles of length  $2^a$ . Suppose that a connected component  $W$  of the Norton-Stein surface  $S_Q$  is fixed setwise by  $\psi_*$ . The Euler characteristic of  $W$  is then divisible by  $2^a$ .*

The proof of Lemma 4.1, given in the next section, is at the core of our main result. Here, we state the main result and show how it follows from Lemma 4.1.

**Theorem 4.2.** *If  $2^l$  (with  $l > 0$ ) is the largest power of two dividing the order of a finite quasigroup  $Q$ , then the disjoint cycle decomposition of each automorphism of  $Q$  must contain a cycle whose length is not divisible by  $2^l$ .*

*Proof.* Suppose that all the cycles of an automorphism  $\psi$  have length divisible by  $2^l$ . First, we claim that it suffices to restrict attention to the case where  $\psi$  consists of cycles all of length precisely  $2^l$ .

Let  $c_1, \dots, c_r$  be the cycle lengths of  $\psi$ , and set  $c = \text{lcm}(c_1, \dots, c_r)$ . Write  $c = 2^a k$  with  $k$  odd. By replacing  $\psi$  with its power  $\psi^k$ , we may assume that each cycle of  $\psi$  has length a power of two, each cycle having length at least  $2^l$ . Since  $2^l$  is the largest power of two dividing  $|Q|$  and the cycle lengths add to  $|Q|$ , it follows that  $\psi$  must have an odd number of cycles of length  $2^l$ . The set of fixed points of  $\psi^{2^l}$  forms a subquasigroup  $H$  of  $Q$ , on which  $\psi$  acts as an automorphism consisting of an odd number of cycles all of length precisely  $2^l$ , so that  $2^l$  is the largest power of two dividing the order of  $H$ . Replacing  $Q$  by  $H$  and  $\psi$  by  $\psi|_H$ , this proves the claim.

Since the orbits of  $\langle \psi \rangle$  partition  $Q$  into orbits of length  $2^l$ , it follows that  $Z_Q = \sum_{q \in Q} \Phi(q)$  is divisible by  $2^l$ . Hence by Theorem 3.1 the largest power of 2 dividing the Euler characteristic of  $S_Q$  is  $2^{l-1}$ . We will obtain a contradiction by showing that the Euler characteristic of  $S_Q$  is actually divisible by  $2^l$ . As we have seen,  $\langle \psi_* \rangle$  acts by permuting the connected components of  $S_Q$ . Let  $W$  be such a component of  $S_Q$ . Its stabilizer in  $\langle \psi_* \rangle$  is generated by  $\psi_*^{2^b}$  for some  $b \leq l$ . So the orbit of  $W$  under  $\langle \psi_* \rangle$  consists of  $2^b$  components, each with identical Euler characteristic. Since  $\psi^{2^b}$  is an automorphism of  $Q$  consisting of cycles of length  $2^{l-b}$ , Lemma 4.1 implies that  $W$  has Euler characteristic divisible by  $2^{l-b}$ . It follows that the union of the components in the orbit of  $W$  has Euler characteristic divisible by  $2^l$ . Hence  $S_Q$  itself has Euler characteristic divisible by  $2^l$ , the desired contradiction.  $\square$

5. PROOF OF THE LEMMA

In the proof of Lemma 4.1, we specialize techniques used by Nielsen in [5, §1–§4]. Let  $\psi$  be an automorphism of a finite quasigroup  $Q$ , and suppose that the disjoint cycle decomposition of  $\psi$  consists entirely of cycles of length  $2^a$ . Further, suppose that  $W$  is a connected component of  $S_Q$  which is invariant under  $\psi_*$ . Set

$G = \langle \psi_* \rangle$ . Note that  $G$  acts on  $W$  by permuting its points. By Corollary 2.4, we have  $|G| = |\psi_*| = |\psi| = 2^a$ , so that each  $G$ -orbit on  $W$  is finite, of length dividing  $2^a$ . More precise information on the orbit lengths is given by the following:

**Lemma 5.1.** *Consider the action of  $G$  on the surface  $W$ .*

- (a) *Each interior point of a 2-cell lies in a  $G$ -orbit of length  $2^a$ .*
- (b) *Each 0-cell lies in a  $G$ -orbit of length  $2^a$ .*
- (c) *Each point  $x$  on a 1-cell lies in a  $G$ -orbit of size  $2^b$ , with*

$$(5.1) \quad a - 1 \leq b \leq a.$$

*The lower bound  $b = a - 1$  in (5.1) can only be attained if  $x$  is the midpoint of a 1-cell.*

*Proof.* (a): Suppose that some power  $\psi_*^k$  fixes an interior point  $x$  of some 2-cell  $(u, v, w)$ . Since  $\psi_*$  maps 2-cells to 2-cells,  $\psi_*^k$  must fix the 2-cell  $(u, v, w)$  setwise. By the construction of  $\psi_*^k$  from Theorem 2.3, it follows that  $(\psi^k(u), \psi^k(v), \psi^k(w)) = (u, v, w)$ . In particular  $\psi^k(u) = u$ , which implies  $2^a \mid k$ .

(b): If  $\psi_*^k$  maps a 0-cell  $u$  to itself, then in particular  $\psi_*^k$  maps  $x$  to a vertex with the same label as  $x$ . If  $x$  has label  $q$ , then we must have  $\psi^k(q) = q$ , and so  $2^a \mid k$ .

(c): Suppose  $x$  is a point on a 1-cell  $\{u, v\}_i$ , and that  $\psi_*^k(x) = x$ . Then since  $\psi_*$  maps 1-cells to 1-cells,  $\psi_*^k$  must map the edge  $\{u, v\}_i$  to itself:  $\{\psi^k(u), \psi^k(v)\}_i = \{u, v\}_i$ . Hence  $\psi^k$  either fixes  $u$  and  $v$ , or swaps them. In either case, we have  $\psi^{2k}(u) = u$ , so  $2^{a-1} \mid k$ . If the fixed point  $x$  of  $\psi_*^k$  is not the midpoint of the edge  $\{u, v\}_i$ , then  $\psi^k$  cannot swap  $u$  and  $v$ . Thus  $\psi^k(u) = u$  and  $2^a \mid k$  in this case.  $\square$

**Definition 5.2.** When the midpoint  $x$  of a 1-cell lies on a  $G$ -orbit of minimal length  $2^{a-1}$ , the point  $x$  is described as a *branch point*.

Under the action of  $G$ , the branch points fall into orbits of size  $2^{a-1}$ . Let  $s$  be the (possibly zero) number of such orbits, so that there are  $2^{a-1}s$  branch points altogether. Choose representative branch points  $x_1, \dots, x_s$ , one from each orbit. Now, select disjoint open discs  $U_1, \dots, U_s$  containing  $x_1, \dots, x_s$  respectively, choosing the  $U_i$  sufficiently small so that the  $2^{a-1}s$  images  $\psi_*^k(U_i)$  are all disjoint for  $0 \leq k < 2^{a-1}$  and  $1 \leq i \leq s$ . We remove all of these  $2^{a-1}s$  discs from  $W$  and call the resulting space  $W_0$ . Thus  $W_0$  is an orientable surface with boundary, having  $2^{a-1}s$  boundary curves. Let  $M$  be the quotient space  $W/G$  of  $W$  determined by identifying points which lie in the same  $G$ -orbit. Let  $\pi : W \rightarrow M$  be the quotient map. The images of the discs  $U_1, \dots, U_s$  under  $\pi$  are removed from  $M$ , and we call the resulting space  $M_0$ . This space  $M_0$  is also an orientable surface with boundary having  $s$  boundary curves.

The space  $W_0$  is a  $2^a$ -fold covering space of  $M_0$ , the restriction of  $\pi$  to  $W_0$  being a covering map. If  $f : [0, 1] \rightarrow M_0$  is any closed loop in  $M_0$  based at some point  $m$  of  $M_0$ , and  $u$  is a point of  $W_0$  such that  $\pi(u) = m$ , then  $f$  lifts to a unique path  $\tilde{f} : [0, 1] \rightarrow W_0$  in  $W_0$  with  $\tilde{f}(0) = u$ . Since the endpoint of this path satisfies  $\pi(\tilde{f}(1)) = m$ , it follows that  $\tilde{f}(1) = \psi_*^{\mu(f,u)}(u)$  for some integer  $\mu(f, u)$  modulo  $2^a$ .

**Lemma 5.3.** *There is a unique integer  $\mu(f)$  modulo  $2^a$  such that  $\mu(f) = \mu(f, v)$  for all  $v \in \pi^{-1}\{m\}$ .*

*Proof.* Suppose  $v \in \pi^{-1}\{m\}$ , say  $v = \psi_*^l(u)$ . Since  $\psi_*^l \circ \tilde{f}$  is the lift of  $f$  to a path in  $W_0$  starting from  $v$ , we have

$$\begin{aligned} \psi_*^{\mu(f,v)}(v) &= \left(\psi_*^l \circ \tilde{f}\right)(1) = \psi_*^l\left(\tilde{f}(1)\right) \\ &= \psi_*^l\left(\psi_*^{\mu(f,u)}(u)\right) = \psi_*^{\mu(f,u)}\left(\psi_*^l(u)\right) = \psi_*^{\mu(f,u)}(v), \end{aligned}$$

whence  $\mu(f, v) = \mu(f, u)$  by Lemma 5.1(b). □

**Definition 5.4.** The integer  $\mu(f)$  modulo  $2^a$  of Lemma 5.3 is called the *monodromy number* of the loop  $f$  in  $M_0$ .

The monodromy number  $\mu(f)$  depends only on the homotopy class of the loop  $f$ . Furthermore, for the concatenation  $f * g$  of two loops  $f, g$  based at  $m$  in  $M$ , we have  $\mu(f * g) = \mu(f) + \mu(g)$ . Hence we may consider  $\mu$  as a homomorphism from the fundamental group  $\pi_1(M_0, m)$  of  $M_0$  into  $\mathbb{Z}/2^a\mathbb{Z}$ .

Consider a point  $m$  on one of the  $s$  boundary curves of  $M_0$ . Let  $\gamma$  be a loop starting from  $m$  that follows once around the boundary curve in the positive direction. There are  $2^a$  points of  $W_0$  which map to  $m$ . On the other hand,  $\pi^{-1}(\gamma([0, 1]))$  is the disjoint union of  $2^{a-1}$  boundary curves of  $W_0$ , which are permuted transitively by  $G$ . Thus each such boundary curve must contain precisely two points mapping to  $m$ , and these two points are interchanged by  $\psi_*^{2^{a-1}}$ . This implies  $\mu(\gamma) = 2^{a-1}$ .

Now fix an arbitrary point  $m$  of  $M_0$ . Let  $\gamma_1, \dots, \gamma_s$  denote loops that respectively follow once around each of the  $s$  boundary curves of  $M_0$  in the positive direction. Let  $\delta_1, \dots, \delta_s$  be paths from  $m$  to  $\gamma_1(0), \dots, \gamma_s(0)$ , respectively. Set  $\gamma'_i = \delta_i^{-1} * \gamma_i * \delta_i$  for  $1 \leq i \leq s$ . Then  $\mu(\gamma'_i) = \mu(\gamma) = 2^{a-1}$  for  $1 \leq i \leq s$ , since the loops  $\gamma_i$  and  $\gamma'_i$  are homotopic.

Let  $g$  be the genus of  $M_0$ . Then the fundamental group  $\pi_1(M_0, m)$  is generated by certain loops  $\alpha_1, \beta_1, \dots, \alpha_g, \beta_g$ , together with the loops  $\gamma'_1, \dots, \gamma'_s$ , subject only to the relation

$$(5.2) \quad t_1 t_2 \cdots t_g \gamma'_1 \gamma'_2 \cdots \gamma'_s = 1$$

with commutators

$$t_i = \alpha_i \beta_i \alpha_i^{-1} \beta_i^{-1}.$$

If we apply  $\mu$  to (5.2), we obtain

$$\sum_{i=1}^g \mu(t_i) + \sum_{j=1}^s \mu(\gamma'_j) \equiv 0 \pmod{2^a}.$$

Now  $\mu(t_i) = \mu(\alpha_i) + \mu(\beta_i) - \mu(\alpha_i) - \mu(\beta_i) = 0$  for  $1 \leq i \leq g$ , and  $\mu(\gamma'_i) = 2^{a-1}$  for  $1 \leq j \leq s$ . Thus

$$2^{a-1}s \equiv 0 \pmod{2^a},$$

and so  $s$  is even. The Euler characteristics of  $W$ ,  $W_0$ , and  $M_0$  are related as follows:

$$\chi(W) - 2^{a-1}s = \chi(W_0) = 2^a\chi(M_0).$$

Since  $s$  is even, this implies that  $2^a \mid \chi(W)$ , as desired.

ACKNOWLEDGEMENTS

The first author would like to thank Brian Rushton and Stephen P. Humphries for useful conversations on the topic of this paper.

## REFERENCES

- [1] D. Bryant, M. Buchanan and I.M. Wanless, *The spectrum for quasigroups with cyclic automorphisms and additional symmetries*, Discrete Math. **309** (2009), 821–833. MR2502191 (2010b:20122)
- [2] R.M. Falcón, *Cycle structures of autotopisms of the Latin squares of order up to 11*, to appear in Ars Combinatoria. [arXiv:0709.2973v2](https://arxiv.org/abs/0709.2973v2) [math.CO], 2009.
- [3] B. Fischer, *Distributive Quasigruppen endlicher Ordnung*, Math. Z. **83** (1964), 267–303. MR0160845 (28:4055)
- [4] J.R. Munkres, *Topology*, Prentice-Hall, Englewood Cliffs, NJ, 2000.
- [5] J. Nielsen, *Die Struktur periodischer Transformationen von Flächen*, Kgl. Danske Videnskabernes Selskab., Math.-fys. Meddelelser **15** (1937), 1–77, translated as *The structure of periodic surface transformations*, pp. 65–102 in “Jakob Nielsen: Collected Mathematical Papers, Vol. 2,” Birkhäuser, Boston, MA, 1986. MR0865336 (88a:01070b)
- [6] D.A. Norton and S.K. Stein, *An integer associated with Latin squares*, Proc. Amer. Math. Soc. **7** (1956), 331–334. MR0077486 (17:1043f)
- [7] S.K. Stein, *Homogeneous quasigroups*, Pac. J. Math. **14** (1964), 1091–1102. MR0170972 (30:1206)
- [8] S.K. Stein, *On the foundations of quasigroups*, Trans. Amer. Math. Soc. **85** (1957), 228–256. MR0094404 (20:922)

DEPARTMENT OF MATHEMATICS, BRIGHAM YOUNG UNIVERSITY, PROVO, UTAH 84602

*E-mail address:* [bkerby@math.byu.edu](mailto:bkerby@math.byu.edu)

*Current address:* Department of Mathematics, University of Utah, Salt Lake City, Utah 84112

*E-mail address:* [kerby@math.utah.edu](mailto:kerby@math.utah.edu)

DEPARTMENT OF MATHEMATICS, IOWA STATE UNIVERSITY, AMES, IOWA 50011

*E-mail address:* [jdsmith@iastate.edu](mailto:jdsmith@iastate.edu)

*URL:* <http://www.orion.math.iastate.edu/jdsmith/>