BOL LOOPS AND BRUCK LOOPS OF ORDER pq UP TO ISOTOPISM

PETR VOJTĚCHOVSKÝ

Abstract. Let $p > q$ be odd primes. We classify Bol loops and Bruck loops of order pq up to isotopism. When q does not divide $p^2 - 1$, the only Bol loop (and hence the only Bruck loop) of order pq is the cyclic group of order pq. When q divides $p^2 - 1$, there are precisely $\lfloor (p-1+4q)(2q)^{-1} \rfloor$ Bol loops of order pq up to isotopism, including a unique nonassociative Bruck loop of order pq.

1. Introduction

Let $p > q$ be odd primes. In this short note we classify Bol loops of order pq up to isotopism, building upon the work of Niederreiter and Robinson [18, 19], and Kinyon, Nagy and Vojtěchovský [12]. The classification turns out to be a nice application of group actions on finite fields.

A *quasigroup* is a groupoid $(Q, \cdot)$ in which all left translations $yL_x = xy$ and all right translations $yR_x = yx$ are bijections. A *loop* is a quasigroup Q with identity element 1. A (right) *Bol loop* is a loop satisfying the identity $((zx)y)x = z((xy)x)$, and a (right) *Bruck loop* is a Bol loop satisfying the identity $(xy)^{-1} = x^{-1}y^{-1}$.

Two loops Q_1, Q_2 are said to be *isotopic* if there are bijections f, g, $h : Q_1 \to Q_2$ such that $(xf)(yg) = (xy)h$ for every x, $y \in Q_1$. If $f = g = h$, the loops are said to be *isomorphic*. Since an isotopism corresponds to an independent renaming of rows, columns and symbols in a multiplication table, it is customary to classify loops (quasigroups and latin squares [5, 14, 15]) not only up to isomorphism but also up to isotopism.

Alongside Moufang loops [3, 16], automorphic loops [4, 11] and conjugacy closed loops [6, 9, 13], Bol loops and Bruck loops are among the most studied varieties of loops [2, 7, 8, 10, 17, 20]. We refer the reader to [1, 3] for an introduction to loop theory and to [12] for an introduction to the convoluted history of the classification of Bol loops whose order is a factor of only a few primes.

The following construction is of key importance for Bol loops of order pq. Let

$$\Theta = \{\theta_i \mid i \in \mathbb{F}_q\} \subseteq \mathbb{F}_p$$

be such that $\theta_0 = 1$ and $\theta_i^{-1}\theta_j \in \mathbb{F}_p^* \setminus \{-1\}$ for every i, $j \in \mathbb{F}_q$. Define $\mathcal{Q}(\Theta)$ on $\mathbb{F}_q \times \mathbb{F}_p$ by

$$(i,j)(k,\ell) = (i+k,\ \ell(1+\theta_k)^{-1} + (j + \ell(1+\theta_k)^{-1})\theta_i^{-1}\theta_{i+k}). \tag{1.1}$$

Then $\mathcal{Q}(\Theta)$ is always a loop.

This construction was introduced and carefully analyzed by Niederreiter and Robinson in [18]. We can restate some of their results as follows:

2010 *Mathematics Subject Classification.* Primary: 20N05; Secondary: 12F05, 15B05, 15B33, 20D20.

Key words and phrases. Bol loop, Bruck loop, quadratic field extension, enumeration, isotopism.

Research partially supported by the PROF grant of the University of Denver.

Theorem 1.1. [18] *Let $p > q$ be odd primes. Then $\mathcal{Q}(\Theta)$ is a Bol loop if and only if there exists a bi-infinite q-periodic sequence (u_i) solving the recurrence relation*

$$u_{n+2} = \lambda u_{n+1} - u_n \tag{1.2}$$

for some $\lambda \in \mathbb{F}_p^*$ such that $u_0 = 1$ and $u_i^{-1}u_j \in \mathbb{F}_p^* \setminus \{-1\}$ for every i, j. (Then $\theta_i = u_i^{-1}$ for every $i \in \mathbb{F}_q$.)

If $\mathcal{Q}(\Theta)$ is a Bol loop then it is a Bruck loop if and only if $u_i = u_{-i}$ for every $i \in \mathbb{F}_q$.

Suppose that two Bol loops correspond to the sequences (u_i) and (v_i), respectively. Then the loops are isomorphic if and only if there is $s \in \mathbb{F}_q^*$ such that $u_i = v_{si}$ for every $i \in \mathbb{F}_q$, and the loops are isotopic if and only if there are $s \in \mathbb{F}_q^*$ and $r \in \mathbb{F}_q$ such that $u_i = v_r^{-1}v_{si+r}$ for every $i \in \mathbb{F}_q$.

It is not at all obvious that every Bol loop of order pq is of the form $\mathcal{Q}(\Theta)$. This was proved in [12], where the isomorphism problem was resolved as follows:

Theorem 1.2. [12] *Let $p > q$ be odd primes. A nonassociative Bol loop of order pq exists if and only if q divides $p^2 - 1$. If q divides $p^2 - 1$ then there is a unique nonassociative Bruck loop $B_{p,q}$ of order pq up to isomorphism and there are precisely*

$$\frac{p - q + 4}{2}$$

Bol loops of order pq up to isomorphism. All these loops are of the form $\mathcal{Q}(\{\theta_i \mid i \in \mathbb{F}_q\})$ with multiplication (1.1) and are obtained as follows:

Set $\theta_i = 1$ for every $i \in \mathbb{F}_q$ for the cyclic group of order pq. For the non-cyclic loops, fix a non-square t of $\mathbb{F}_p$, write $\mathbb{F}_{p^2} = \{u + v\sqrt{t} \mid u, v \in \mathbb{F}_p\}$, and let $\omega \in \mathbb{F}_{p^2}$ be a primitive qth root of unity. Let

$$\Gamma_{p,q} = \begin{cases} \{\gamma \in \mathbb{F}_p \mid \gamma = 0 \text{ or } 1 - \gamma^{-1} \notin \langle\omega\rangle\}, & \text{if } q \text{ divides } p - 1, \\ \{\gamma \in 1/2 + \mathbb{F}_p\sqrt{t} \mid 1 - \gamma^{-1} \notin \langle\omega\rangle\}, & \text{if } q \text{ divides } p + 1. \end{cases}$$

Let f be the bijection on $\Gamma_{p,q}$ defined by

$$\gamma \mapsto 1 - \gamma.$$

The non-cyclic Bol loops of order pq up to isomorphism correspond to the orbits of the group $\langle f \rangle$ acting on $\Gamma_{p,q}$. For every orbit representative γ let

$$\theta_i = \theta(\gamma)_i = \frac{1}{\gamma\omega^i + (1 - \gamma)\omega^{-i}}.$$

The choice $\gamma = 1/2$ results in the nonassociative Bruck loop $B_{p,q}$. If q divides $p - 1$, the choice $\gamma = 1$ results in the nonabelian group of order pq.

Since a loop isotopic to a group is already isomorphic to it, Theorem 1.2 contains the classification of Bruck loops of order pq up to isotopism. In this paper we finish the classification of Bol loops of order pq up to isotopism by proving:

Theorem 1.3. *Let $p > q$ be odd primes such that q divides $p^2 - 1$. Then there are precisely*

$$\left\lfloor \frac{p - 1 + 4q}{2q} \right\rfloor$$

Bol loops of order pq up to isotopism. With the notation of Theorem 1.2, these loops are obtained as follows:

Set $\theta_i = 1$ for every $i \in \mathbb{F}_q$ for the cyclic group of order pq. The non-cyclic loops correspond to orbit representatives of the group $\langle f, g\rangle$ acting on $\Gamma_{p,q}$, where g is given by

$$\gamma \mapsto \frac{\gamma\omega}{\gamma\omega + (1-\gamma)\omega^{-1}}.$$

Remark 1.4. Let $p > 3$ be a prime. By Theorem 1.3, the number N_{3p} of Bol loops of order $3p$ up to isotopism is equal to $\lfloor (p + 11)/6\rfloor$, confirming [12, Conjecture 7.3]. It was shown already in [18, p. 255] that $N_{3p} \geq \lceil (p + 5)/6\rceil$, a remarkably good estimate. Note that

$$\left\lfloor \frac{p+11}{6} \right\rfloor - \left\lceil \frac{p+5}{6} \right\rceil = \begin{cases} 0, & \text{if } p = 6k+5, \\ 1, & \text{if } p = 6k+1. \end{cases}$$

2. Proof of the main result

For the rest of the paper assume that $p > q$ are odd primes, q divides $p^2 - 1$, ω is a primitive qth root of unity in $\mathbb{F}_{p^2}$ and write $\mathbb{F}_{p^2} = \{u + v\sqrt{t} \mid u, v \in \mathbb{F}_p\}$ for some non-square $t \in \mathbb{F}_p$.

Let $\mathcal{X}_{p,q}$ be the set of all bi-infinite q-periodic sequences with entries in $\mathbb{F}_{p^2}$. As explained in [12], $u \in \mathcal{X}_{p,q}$ solves the recurrence relation (1.2) if and only if $Au = \lambda u$, where A is the $q \times q$ circulant matrix whose first row is equal to $(0, 1, 0, \dots, 0, 1)$ and where we identify u with the vector $(u_0, \dots, u_{q-1})^T$. General theory of circulant matrices applies and yields:

Lemma 2.1. [12] *Let A be the $q\times q$ circulant matrix whose first row is equal to $(0, 1, 0, \dots, 0, 1)$. For $0 \leq j < q$, let*

$$\lambda_j = \omega^j + \omega^{-j} \quad \textit{and} \quad e_j = (1, \omega^j, \omega^{2j}, \dots, \omega^{(q-1)j})^T. \tag{2.1}$$

Then:

(i) *For every $0 \leq j < q$, λ_j is an element of the prime field of $\mathbb{F}_{p^2}$.*
(ii) *For every $0 \leq j < q$, λ_j is an eigenvalue of A over $\mathbb{F}_{p^2}$ with eigenvector e_j.*
(iii) *For $0 < j \leq (q-1)/2$, the eigenvectors e_j, e_{-j} are linearly independent.*
(iv) *For $0 \leq j < k < q$, $\lambda_j = \lambda_k$ if and only if $j + k \equiv 0 \pmod q$. In particular, $\lambda_0 = 2$ has multiplicity 1, and every λ_j with $1 \leq j \leq (q-1)/2$ has multiplicity 2.*

Let λ_j and e_j be as in (2.1). In order to better understand which elements of $\mathcal{X}_{p,q}$ yield Bol loops, let us define the following subsets:

$$\mathcal{X}^*_{p,q} = \{u \in \mathcal{X}_{p,q} \mid u_0 = 1\},$$

$$\mathcal{A}^j_{p,q} = \{u \in \mathcal{X}^*_{p,q} \mid Au = \lambda_j u\}, \qquad \mathcal{A}_{p,q} = \bigcup_{0\leq j<q} \mathcal{A}^j_{p,q},$$

$$\mathcal{B}^j_{p,q} = \{u \in \mathcal{A}^j_{p,q} \mid u_i^{-1}u_k \in \mathbb{F}_p^* \setminus \{-1\} \text{ for every } i, k\}, \qquad \mathcal{B}_{p,q} = \bigcup_{0\leq j<q} \mathcal{B}^j_{p,q}.$$

By Theorem 1.1, the elements of $\mathcal{B}_{p,q}$ are precisely the sequences that yield Bol loops.

Lemma 2.2. *For every $j \in \mathbb{F}_q$, $\mathcal{A}^j_{p,q} = \{\gamma e_j + (1-\gamma)e_{-j} \mid \gamma \in \mathbb{F}_{p^2}\}$. In particular, the only element of $\mathcal{A}^0_{p,q} = \mathcal{B}^0_{p,q}$ is the all-1 sequence.*

Proof. Let $u \in \mathcal{A}^j_{p,q}$. By Lemma 2.1, $u = \gamma e_j + \delta e_{-j}$ for some $\gamma, \delta \in \mathbb{F}_{p^2}$. The condition $u_0 = 1$ forces $\gamma + \delta = 1$. □

Let u be the unique element of $\mathcal{B}^0_{p,q}$, the all-1 sequence. Then $\theta_i = u_i^{-1} = 1$ for every i, and the multiplication formula (1.1) becomes $(i,j)(k,\ell) = (i+k, j+\ell)$, the direct product $\mathbb{Z}_q \times \mathbb{Z}_p \cong \mathbb{Z}_{pq}$.

Consider the following binary relations on $\mathcal{X}^*_{p,q}$:

- $u \sim v$ if there is $s \in \mathbb{F}_q^*$ such that $u_i = v_{si}$ for every i,
- $u \approx v$ if there is $r \in \mathbb{F}_q$ such that $u_i = v_r^{-1} v_{i+r}$ for every i, and
- $u \equiv v$ if there are $s \in \mathbb{F}_q^*$ and $r \in \mathbb{F}_q$ such that $u_i = v_r^{-1} v_{si+r}$ for every i.

We recognize $\sim$ as the isomorphism relation and $\equiv$ as the isotopism relation from Theorem 1.1.

Lemma 2.3. *If $u \in \mathcal{A}^j_{p,q}$ and $v \equiv u$ via $v_i = u_r^{-1} u_{si+r}$ then $v \in \mathcal{A}^{sj}_{p,q}$. Conversely, if $u \in \mathcal{A}^j_{p,q}$ for some $j \in \mathbb{F}_q^*$ then for every $k \in \mathbb{F}_q^*$ there is $v \in \mathcal{A}^k_{p,q}$ such that $v \equiv u$.*

Proof. Suppose that $u \in \mathcal{A}^j_{p,q}$ and $v_i = u_r^{-1} u_{si+r}$. Note that $v_0 = u_r^{-1} u_r = 1$. By Lemmas 2.1 and 2.2, we have $u = \gamma e_j + (1-\gamma) e_{-j}$ for some $\gamma \in \mathbb{F}_{p^2}$. Let $f_i = e_{j,r}^{-1} e_{j,si+r}$. Then $f_i = \omega^{-jr} \omega^{j(si+r)} = \omega^{jsi} = e_{sj,i}$. By linearity, $v = \gamma e_{sj} + (1-\gamma) e_{-sj}$. By Lemma 2.1, $v \in \mathcal{A}^{sj}_{p,q}$.

For the converse, suppose that $j \in \mathbb{F}_q^*$ and let $s \in \mathbb{F}_q^*$ be such that $sj = k$. Set $v_i = u_r^{-1} u_{si+r}$ for some $r \in \mathbb{F}_q$. Then certainly $v \equiv u$ and we have $v \in \mathcal{A}^k_{p,q}$ by the first part. □

Lemma 2.4. *The following statements hold:*

(i) *$\sim$, $\approx$ and $\equiv$ are equivalence relations on $\mathcal{X}^*_{p,q}$, and $\equiv$ is the transitive closure of $\sim$ and $\approx$.*
(ii) *$\mathcal{B}_{p,q}$ is the union of some equivalence classes of each of $\sim$, $\approx$ and $\equiv$.*
(iii) *If $u \in \mathcal{B}^1_{p,q}$ and $v_i = u_r^{-1} u_{si+r}$ then $v \in \mathcal{B}^1_{p,q}$ if and only if $s = \pm 1$.*
(iv) *$\mathcal{B}^1_{p,q}$ is the union of some equivalence classes of $\approx$.*

Proof. (i) Note that $\sim$ is contained in $\equiv$ (set $r = 0$ and use $v_0 = 1$) and $\approx$ is contained in $\equiv$ (set $s = 1$). We show that $\equiv$ is an equivalence relation, the other two cases being similar. We have $u \equiv u$ with $r = 0$, $s = 1$. If $u_i = v_r^{-1} v_{si+r}$ then $u^{-1}_{-s^{-1}r} u_{s^{-1}i - s^{-1}r} = (v_r^{-1} v_{s(-s^{-1}r)+r})^{-1} v_r^{-1} v_{s(s^{-1}i - s^{-1}r)+r} = v_i$, proving symmetry. If $u_i = v_r^{-1} v_{si+r}$ and $v_i = w_a^{-1} w_{bi+a}$ then $u_i = (w_a^{-1} w_{br+a})^{-1} w_a^{-1} w_{b(si+r)+a} = w^{-1}_{br+a} w_{(bs)i+(br+a)}$, proving transitivity. For the transitive closure, if $u_i = w_r^{-1} w_{si+r}$, set $v_i = w_r^{-1} w_{i+r}$ and note that $u_i = v_{si}$.

(ii) Suppose that $u \equiv v$, $u_i = v_r^{-1} v_{si+r}$. By Lemma 2.3, if $u \in \mathcal{A}_{p,q}$ then $v \in \mathcal{A}_{p,q}$. If $u_i^{-1} u_j \in \mathbb{F}_p^* \setminus \{-1\}$ for every i, j, then $v^{-1}_{si+r} v_{sj+r} = (v_r^{-1} v_{si+r})^{-1} v_r^{-1} v_{sj+r} = u_i^{-1} u_j \in \mathbb{F}_p^* \setminus \{-1\}$ for every i, j, and we are done since $(i,j) \mapsto (si+r, sj+r)$ is a bijection of $\mathbb{F}_q \times \mathbb{F}_q$.

Part (iii) follows from (ii) and Lemma 2.3. Part (iv) is then immediate. □

Let $j \in \mathbb{F}_q^*$. By Lemmas 2.3 and 2.4, for any $u \in \mathcal{B}^j_{p,q}$ there is $v \in \mathcal{B}^1_{p,q}$ such that $u \equiv v$, and there is no $w \in \mathcal{B}^0_{p,q}$ such that $u \equiv w$. For the isotopism problem, it therefore remains to study the restriction of $\equiv$ onto $\mathcal{B}^1_{p,q}$, taking parts (iii) and (iv) of Lemma 2.4 into account.

Every element of $\mathcal{B}^1_{p,q}$ is by definition an element of $\mathcal{A}^1_{p,q}$ and hence is of the form

$$u(\gamma) = \gamma e_1 + (1-\gamma) e_{-1}$$

for some $\gamma \in \mathbb{F}_{p^2}$, by Lemma 2.2. The mapping $\gamma \mapsto u(\gamma)$ is a bijection. Indeed, if $u(\gamma) = u(\delta)$ then $\gamma\omega + (1-\gamma)\omega^{-1} = u(\gamma)_1 = u(\delta)_1 = \delta\omega + (1-\delta)\omega^{-1}$, hence $(\gamma-\delta)\omega = (\gamma-\delta)\omega^{-1}$ and $\gamma = \delta$ follows. It was shown in [12, Section 6] that

$$\mathcal{B}^1_{p,q} = \{u(\gamma) \mid \gamma \in \Gamma_{p,q}\},$$

where $\Gamma_{p,q}$ is as in Theorem 1.2. Moreover, by [12, Lemma 6.8], $\Gamma_{p,q}$ is a set of cardinality $p-q+1$, it is closed under the map $\gamma \mapsto 1-\gamma$, and it always contains $1/2$.

Let $u = u(\gamma) \in \mathcal{B}^1_{p,q}$ and consider $v_i = u_{-i}$. Since $u(\gamma)_i = u(1-\gamma)_{-i}$, we have $v = u(1-\gamma) \in \mathcal{B}^1_{p,q}$. The non-cyclic Bol loops of order pq up to isomorphism therefore correspond to the orbits of the group $\langle f \rangle$ acting on $\Gamma_{p,q}$, where

$$\gamma f = 1-\gamma.$$

At this point we can recover Theorem 1.2. The cyclic group of order pq corresponds to the unique sequence of $\mathcal{B}^0_{p,q}$. The above action has a unique fixed point on $\Gamma_{p,q}$, namely $\gamma = 1/2$, and all other orbits have size 2. The fixed point $\gamma = 1/2$ yields a Bruck loop by Theorem 1.1. Since $|\Gamma_{p,q}| = p-q+1$, there are additional $(p-q)/2$ Bol loops, for the total of $1+1+(p-q)/2 = (p-q+4)/2$ Bol loops of order pq. If q divides $p-1$, the nonabelian group of order pq must be among these pq loops. It is easy to check that it is the loop corresponding to $\gamma = 1$.

To further classify Bol loops of order pq up to isotopism, we must now also consider the equivalence classes of $\approx$ on $\mathcal{B}^1_{p,q}$.

Lemma 2.5. *Let γ, $\delta \in \Gamma_{p,q}$. Then $u(\gamma) \approx u(\delta)$ if and only if*

$$\gamma = \frac{\delta\omega^r}{\delta\omega^r + (1-\delta)\omega^{-r}} \tag{2.2}$$

for some $r \in \mathbb{F}_q$.

Proof. By definition, $u(\gamma) \approx u(\delta)$ if an only if there is $r \in \mathbb{F}_q$ such that

$$\gamma\omega^i + (1-\gamma)\omega^{-i} = u(\gamma)_i = u(\delta)_r^{-1} u(\delta)_{i+r} = \frac{\delta\omega^{i+r} + (1-\delta)\omega^{-i-r}}{\delta\omega^r + (1-\delta)\omega^{-r}} \tag{2.3}$$

for every $i \in \mathbb{F}_q$.

Suppose that (2.3) holds. If $r = 0$ then $u(\gamma) = u(\delta)$ and hence $\gamma = \delta$, which agrees with (2.2). Suppose that $r \neq 0$. Substituting $i = r$ into (2.3) yields

$$\gamma\omega^r + (1-\gamma)\omega^{-r} = \frac{\delta\omega^{2r} + (1-\delta)\omega^{-2r}}{\delta\omega^r + (1-\delta)\omega^{-r}},$$

and therefore

$$\gamma = \frac{(\delta\omega^{2r} + (1-\delta)\omega^{-2r})(\delta\omega^r + (1-\delta)\omega^{-r})^{-1} - \omega^{-r}}{\omega^r - \omega^{-r}}.$$

A straightforward computation now shows that γ is as in (2.2).

Conversely, suppose that γ is as in (2.2). Then another straightforward calculation shows that (2.3) holds for every i, and thus $u(\gamma) \approx u(\delta)$. $\square$

For $r \in \mathbb{F}_q$, consider the mapping $g_r : \Gamma_{p,q} \to \Gamma_{p,q}$ defined by

$$\gamma g_r = \frac{\gamma\omega^r}{\gamma\omega^r + (1-\gamma)\omega^{-r}}.$$

We note that g_r is well-defined since $\gamma\omega^r + (1-\gamma)\omega^{-r} = u(\gamma)_r \neq 0$. By Lemma 2.5, if $\gamma = \delta g_r$ then $u(\gamma) \approx u(\delta)$, so $u(\delta) \in \mathcal{B}^1_{p,q}$ by Lemma 2.4(iv), which in turn implies $\delta \in \Gamma_{p,q}$. Altogether, g_r is a bijection on $\Gamma_{p,q}$.

Yet another straightforward calculation shows that $\gamma g_r g_s = \gamma g_{r+s}$ for every r, $s \in \mathbb{F}_q$. Let $g = g_1$, that is,

$$\gamma g = \frac{\gamma\omega}{\gamma\omega + (1-\gamma)\omega^{-1}}.$$

Combining our results obtained so far, we see that $u(\gamma) \approx u(\delta)$ if and only if γ, δ are in the same orbit of the group $\langle g\rangle$ acting on $\Gamma_{p,q}$, and $u(\gamma) \equiv u(\delta)$ if and only if γ, δ are in the same orbit of the group $G = \langle f, g\rangle$ acting on $\Gamma_{p,q}$.

Proposition 2.6. *The group $G = \langle f, g\rangle$ is isomorphic to the dihedral group D_{2q} of order $2q$. Moreover:*

(i) *The only fixed point of f is $1/2$. If q divides $p-1$ then $f(0) = 1$ and $f(1) = 0$.*
(ii) *If $0 < i < q$ and q divides $p-1$ then the only fixed points of g^i are 0 and 1.*
(iii) *If $0 < i < q$ and q divides $p+1$ then g^i has no fixed points.*
(iv) *If $0 < i < q$ then the only fixed point of fg^i is $(1+\omega^i)^{-1}$.*

Proof. Part (i) is obvious. For the rest of the proof, let $0 < i < q$. We have $\gamma g^i = \gamma$ if and only if $\gamma\omega^i = \gamma(\gamma\omega^i + (1-\gamma)\omega^{-i})$, which is equivalent to $\gamma(1-\gamma)\omega^i = \gamma(1-\gamma)\omega^{-i}$. Clearly, $\gamma = 0$, $\gamma = 1$ are fixed points as long as they lie in $\Gamma_{p,q}$, which happens if and only if q divides $p-1$. If $\gamma \notin \{0, 1\}$ and $\gamma g^i = \gamma$ then $\omega^i = \omega^{-i}$, a contradiction.

Suppose now that $\gamma f g^i = \gamma$. Then $(1-\gamma)g^i = \gamma$, $(1-\gamma)\omega^i = \gamma((1-\gamma)\omega^i + \gamma\omega^{-i})$, and $(1-\gamma)^2\omega^i = \gamma^2\omega^{-i}$. We certainly have $\gamma \neq 0$ and thus $((1-\gamma)/\gamma)^2 = \omega^{2i}$, which we rewrite as $(1-\gamma^{-1})^2 = \omega^{2i}$. Then either $1-\gamma^{-1} = \omega^i$ (which implies $1-\gamma^{-1} \in \langle\omega\rangle$, a contradiction with $\gamma \in \Gamma_{p,q}$), or $1-\gamma^{-1} = -\omega^i$, which implies $\gamma = (1+\omega^i)^{-1}$, the only candidate for a fixed point of fg^i.

Now, $|f| = 2$ since $f^2 = 1$ and $\gamma f \neq \gamma$ if $\gamma \neq 1/2$. Also $|g| = q$ since $g^q = 1$ and $\gamma g \neq \gamma$ whenever $\gamma \notin \{0, 1\}$. Finally,

$$\gamma g f = 1 - \frac{\gamma\omega}{\gamma\omega + (1-\gamma)\omega^{-1}} = \frac{(1-\gamma)\omega^{-1}}{\gamma\omega + (1-\gamma)\omega^{-1}},$$

while

$$\gamma f g^{-1} = (1-\gamma)g^{-1} = \frac{(1-\gamma)\omega^{-1}}{(1-\gamma)\omega^{-1} + \gamma\omega}.$$

Thus $gf = fg^{-1}$ and $G \cong D_{2q}$ follows.

Since $1/2$ is fixed by f but not by g, the orbit-stabilizer theorem implies that the orbit of $1/2$ contains q elements. In turn, each of these q elements has a stabilizer of size 2, so it must be stabilized by some fg^i of G. We conclude that the purported fixed points $(1+\omega^i)^{-1}$ of fg^i are indeed fixed points. $\square$

We are ready to prove the main result, Theorem 1.3:

Let us count the orbits of $G = \langle f, g\rangle$ on the set $\Gamma_{p,q}$ or cardinality $p - q + 1$. We will use Proposition 2.6 without reference. For $\gamma \in \Gamma_{p,q}$, let $O(\gamma)$ be the orbit of γ.

First suppose that q divides $p-1$. Let $p - 1 = kq$ and note that $|\Gamma_{p,q}| = (k-1)q + 2$. We have 0, $1 \in \Gamma_{p,q}$ and $O(0) = \{0, 1\}$, leaving $(k-1)q$ elements. The orbit $O(1/2)$ accounts for the remaining q points fixed by some element of G. All the other $(k-2)q$ elements lie in orbits of size $2q$, so there must be $(k-2)/2$ such orbits. Altogether, we have counted $1 + 1 + 1 + (k-2)/2 = (p - 1 + 4q)/(2q)$ Bol loops of order pq up to isotopism, including the cyclic group.

Now suppose that q divides $p+1$. Let $p+1 = \ell q$ and note that $|\Gamma_{p,q}| = (\ell-1)q$. Also note that $0, 1 \not\in \Gamma_{p,q}$. The orbit $O(1/2)$ again accounts for q elements, and these are the only elements with nontrivial stabilizers. The remaining $(\ell-2)q$ elements lie in $(\ell-2)/2$ orbits of size $2q$. Altogether, we have counted $1+1+(\ell-2)/2 = (p+1+2q)/(2q)$ Bol loops up to isotopism. We note that ℓ must be even and therefore

$$\left\lfloor \frac{p-1+4q}{2q} \right\rfloor = \left\lfloor \frac{p+1+4q-2}{2q} \right\rfloor = \left\lfloor \frac{\ell q+4q-2}{2q} \right\rfloor = \left\lfloor \frac{\ell}{2} + 2 - \frac{2}{2q} \right\rfloor = \frac{\ell}{2} + 1 = \frac{p+1+2q}{2q},$$

finishing the proof of Theorem 1.3.

ACKNOWLEDGMENT

We thank Izabella Stuhl for several discussions on the topic of this paper.

References

[1] V.D. Belousov, Основы теории квазигрупп и луп, Izdat. "Nauka", Moscow 1967.
[2] G. Bol, *Gewebe und gruppen*, Math. Ann. **114** (1937), no. **1**, 414–431.
[3] Richard Hubert Bruck, *A survey of binary systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Heft **20**, Springer Verlag, Berlin-Göttingen-Heidelberg 1958.
[4] R.H. Bruck and Lowell J. Paige, *Loops whose inner mappings are automorphisms*, Ann. of Math. (**2**) **63** (1956), 308–323.
[5] J. Dénes and A.D. Keedwell, *Latin squares and their applications*, Academic Press, New York-London, 1974.
[6] Aleš Drápal, *Structural interactions of conjugacy closed loops*, Trans. Amer. Math. Soc. **360** (2008), no. **2**, 671–689.
[7] George Glauberman, *On loops of odd order*, J. Algebra **1** (1964), 374–396.
[8] George Glauberman, *On loops of odd order II*, J. Algebra **8** (1968), 393–414.
[9] Edgar G. Goodaire and D.A. Robinson, *A class of loops which are isomorphic to all loop isotopes*, Canad. J. Math. **34** (1982), no. **3**, 662–672.
[10] Hubert Kiechle, *Theory of K-loops*, Lecture Notes in Mathematics **1778**, Springer-Verlag, Berlin, 2002.
[11] Michael K. Kinyon, Kenneth Kunen, J.D. Phillips and Petr Vojtěchovský, *The structure of automorphic loops*, Trans. Amer. Math. Soc. **368** (2016), no. **12**, 8901–8927.
[12] Michael K. Kinyon, Gábor P. Nagy and Petr Vojtěchovský, *Bol loops and Bruck loops of order pq*, J. Algebra **473** (2017), 481–512.
[13] Kenneth Kunen, *The structure of conjugacy closed loops*, Trans. Amer. Math. Soc. **352** (2000), no. **6**, 2889–2911.
[14] Charles F. Laywine and Garry L. Mullen, *Discrete mathematics using Latin squares*, Wiley-Interscience Series in Discrete Mathematics and Optimization. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1998.
[15] Brendan D. McKay and Ian M. Wanless, *On the number of Latin squares*, Ann. Comb. **9** (2005), no. **3**, 335–344.
[16] Ruth Moufang, *Zur Struktur von Alternativkörpern*, Math. Ann. **110** (1935), no. **1**, 416–430.
[17] Gábor P. Nagy, *A class of simple proper Bol loops*, Manuscripta Math. **127** (2008), no. **1**, 81–88.
[18] Harald Niederreiter and Karl H. Robinson, *Bol loops of order pq*, Math. Proc. Cambridge Philos. Soc. **89** (1981), no. **2**, 241–256.
[19] Harald Niederreiter and Karl H. Robinson, *On isomorphisms and isotopisms of Bol loops of order* $3p$, Comm. Algebra **22** (1994), no. **1**, 345–347.
[20] D.A. Robinson, *Bol loops*, Trans. Amer. Math. Soc. **123** (1966), 341–354.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF DENVER, SOUTH YORK STREET 2390, DENVER, COLORADO, 80208, U.S.A.
E-mail address: petr@math.du.edu