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 \(\lfloor \frac{(p-1+4q)(2q)^{-1}}{2} \rfloor\) 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 \(Q(\Theta)\) on \(\mathbb{F}_q \times \mathbb{F}_p\) by

\[(i, j)(k, \ell) = (i + k, \ell(1 + \theta_k)^{-1} + (j + \ell(1 + \theta_k)^{-1})\theta_i^{-1}\theta_{i+k}).\]

Then \(Q(\Theta)\) 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:

\begin{itemize}
\item \textbf{2010 Mathematics Subject Classification.} Primary: 20N05; Secondary: 12F05, 15B05, 15B33, 20D20.
\item \textbf{Key words and phrases.} Bol loop, Bruck loop, quadratic field extension, enumeration, isotopism.
\item Research partially supported by the PROF grant of the University of Denver.
\end{itemize}
Theorem 1.1. [18] Let $p > q$ be odd primes. Then $Q(\Theta)$ is a Bol loop if and only if there exists a bi-infinite $q$-periodic sequence $(u_i)$ solving the recurrence relation

\begin{equation}
 u_{n+2} = \lambda u_{n+1} - u_n
\end{equation}

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 $Q(\Theta)$ 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 $Q(\Theta)$. 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 $Q(\{\theta_i | i \in \mathbb{F}_q\})$ 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 $\mathbb{F}_{p^2} = \{u + v\sqrt{t} | u, v \in \mathbb{F}_p\}$, and let $\omega \in \mathbb{F}_{p^2}$ be a primitive $q$th root of unity. Let

$$\Gamma_{p,q} = \\{ \gamma \in \mathbb{F}_{p^2} \mid \gamma = 0 \text{ or } 1 - \gamma^{-1} \not\in \langle \omega \rangle \}, \quad \text{if } q \text{ divides } p - 1,$$

$$\Gamma_{p,q} = \\{ \gamma \in 1/2 + \mathbb{F}_p \sqrt{t} \mid 1 - \gamma^{-1} \not\in \langle \omega \rangle \}, \quad \text{if } q \text{ divides } p + 1.$$ 

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 $\gamma$ 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 isotopy is equal to \( \lfloor (p + 11)/6 \rfloor \), confirming [12, Conjecture 7.3]. It was shown already in [18, p. 255] that \( N_{3p} \geq \lfloor (p + 5)/6 \rfloor \), a remarkably good estimate. Note that

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

2. Proof of the main result

For the rest of the paper assume that \( p > q \) are odd primes, \( q \) divides \( p^2 - 1 \), \( \omega \) is a primitive \( q \)th 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 \( X_{p,q} \) be the set of all bi-infinite \( q \)-periodic sequences with entries in \( \mathbb{F}_{p^2} \). As explained in [12], \( u \in X_{p,q} \) 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 \( (0, 1, 0, \ldots, 0, 1) \) and where we identify \( u \) with the vector \( (u_0, u_1, \ldots, u_{q-1})^T \). 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 \( (0, 1, 0, \ldots, 0, 1) \).

For \( 0 \leq j < q \), let

\[
\lambda_j = \omega^j + \omega^{-j} \quad \text{and} \quad e_j = (1, \omega^j, \omega^{2j}, \ldots, \omega^{(q-1)j})^T.
\]

Then:

(i) For every \( 0 \leq j < q \), \( \lambda_j \) is an element of the prime field of \( \mathbb{F}_{p^2} \).

(ii) For every \( 0 \leq j < q \), \( \lambda_j \) 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 \( \lambda_j \) with \( 1 \leq j \leq (q - 1)/2 \) has multiplicity 2.

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

\[
X_{p,q}^* = \{ u \in X_{p,q} \mid u_0 = 1 \},
\]

\[
A_{p,q} = \bigcup_{0 \leq j < q} A_{p,q}^j,
\]

\[
B_{p,q} = \bigcup_{0 \leq j < q} B_{p,q}^j.
\]

By Theorem 1.1, the elements of \( B_{p,q} \) are precisely the sequences that yield Bol loops.

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

**Proof.** Let \( u \in A_{p,q}^j \). 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 \( \gamma + \delta = 1 \). \( \square \)
Let $u$ be the unique element of $B_{p,q}^0$, the all-1 sequence. Then $\theta_i = u^{-1}i = 1$ 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 $X_{p,q}^*$:

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

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

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

**Proof.** Suppose that $u \in A_{p,q}^j$ and $v = u_i^{r-1}u_{si+r}$. Note that $v_0 = u_i^{r-1}u_{i} = 1$. By Lemmas 2.1 and 2.2, we have $u = \gamma_je_j + (1 - \gamma)e_{-j}$ for some $\gamma \in \mathbb{F}_p^*$. Let $f_i = e_{j,i}^{r-1}e_{si+r}$. Then $f_i = \omega^{jr}j^{(s+i+r)} = \omega^{s+1}$. By linearity, $v = \gamma_je_j + (1 - \gamma)e_{-j}$. By Lemma 2.1, $v \in A_{p,q}^j$.

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

**Lemma 2.4.** The following statements hold:

(i) $\sim$, $\approx$ and $\equiv$ are equivalence relations on $X_{p,q}^*$, and $\equiv$ is the transitive closure of $\sim$ and $\approx$.

(ii) $B_{p,q}$ is the union of some equivalence classes of each of $\sim$, $\approx$ and $\equiv$.

(iii) If $u \in B_{p,q}^1$ and $v_i = u_i^{r-1}u_{si+r}$ then $v \in B_{p,q}^1$ if and only if $s = \pm 1$.

(iv) $B_{p,q}^1$ 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 $\sim$ is contained in $\approx$ (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 $u_i = v_i^{r-1}u_{si+r}$ then $u_i^{r-1}u_{si+1} = (v_i^{r-1}u_{si})^{r-1}v_{si+1} = v_i$, proving symmetry. If $u_i = v_i^{r-1}u_{si+r}$ and $v_i = w_i^{r-1}w_{si+r}$ then $u_i = (w_i^{r-1}w_{br+a})^{r-1}w_i = w_i^{r-1}w_{br+a}w_{br+a} = u_i^{r-1}u_{br+a}$, proving transitivity. For the transitive closure, if $u_i = v_i^{r-1}u_{si+r}$, set $v_i = w_i^{r-1}w_{i+r}$ and note that $u_i = v_i$.

(ii) Suppose that $v \equiv u$, $u_i = v_i^{r-1}v_{si+r}$. By Lemma 2.3, if $u \in A_{p,q}$ then $v \in A_{p,q}$. If $u_i^{-1}v_j \in \mathbb{F}_p^* \setminus \{-1\}$ for every $i, j$, then $v_{si+r} = (u_i^{-1}v_{si+r})^{-1}u_i^{-1}v_{si+r} = u_i^{-1}u_j \in \mathbb{F}_p^* \setminus \{-1\}$ 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. \qed

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

Every element of $B_{p,q}^1$ is by definition an element of $A_{p,q}^1$ and hence is of the form

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

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

$$B_{p,q}^1 = \{u(\gamma) \mid \gamma \in \Gamma_{p,q}\},$$
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 $u = u(\gamma) \in B_{p,q}^1$ and consider $v_i = u_{-i}$. Since $u(\gamma_i) = u(1 - \gamma)_{-i}$, we have $v = u(1 - \gamma) \in B_{p,q}^1$. The non-cyclic Bol loops of order $pq$ up to isomorphism therefore correspond to the orbits of the group $(f)$ 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 $B_{p,q}^0$. 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 $B_{p,q}^1$.

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

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

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

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

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

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

A straightforward computation now shows that $\gamma$ is as in (2.2).

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

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 $u(\delta) \in B_{p,q}^1$ 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 \( \gamma, \delta \) 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 \( \gamma, \delta \) 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 \( \omega^i = \gamma (\omega^i + (1 - \gamma) \omega^{-i}) \), 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 \( \gamma fg^i = \gamma \). 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,
\[
\gamma gf = 1 - \frac{\gamma \omega}{\gamma \omega + (1 - \gamma) \omega^{-1}} = \frac{(1 - \gamma) \omega^{-1}}{\gamma \omega + (1 - \gamma) \omega^{-1}},
\]
while
\[
\gamma fg^{-1} = (1 - \gamma) g^{-1} = \frac{(1 - \gamma) \omega^{-1}}{(1 - \gamma) \omega^{-1} + \gamma \omega}.
\]
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.

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 \( \gamma \).

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 $0, 1 \notin \Gamma_{p,q}$. 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 isomorphism. We note that $\ell$ must be even and therefore

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

finishing the proof of Theorem 1.3.

ACKNOWLEDGMENT

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

REFERENCES


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