Finite Fields and Their Applications 52 (2018) 1–9

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Bol loops and Bruck loops of order pq up to isotopism ☆

Petr Vojtěchovský

Department of Mathematics, University of Denver, South York Street 2390, Denver, CO, 80208, USA

ARTICLE INFO

Article history:
Received 29 September 2017
Received in revised form 16 January 2018
Accepted 26 February 2018
Available online xxxx
Communicated by L. Storme

MSC:
primary 20N05
secondary 12F05, 15B05, 15B33, 20D20

Keywords:
Bol loop
Bruck loop
Quadratic field extension
Enumeration
Isotopism

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,

☆ Research partially supported by the PROF grant of the University of Denver.
E-mail address: petr@math.du.edu.

https://doi.org/10.1016/j.ffa.2018.02.008

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:

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