Bol loops of order pq

Gábor Péter Nagy

joint work with M. Kinyon and P. Vojtěchovský (Denver)

University of Szeged (Hungary)
and
Budapest University of Technology (Hungary)

Fourth Mile High Conference on Nonassociative Mathematics
Denver, July 29 – August 5, 2017

Overview

1. Bol loops and Bruck loops
2. The Eighties: Niederreiter, Robinson, Sharma, Solarin, Burn
3. The main theorems

(Remark: We only consider finite loops.)

Overview

1. Bol loops and Bruck loops
2. The Eighties: Niederreiter, Robinson, Sharma, Solarin, Burn
3. The main theorems

(Remark: We only consider finite loops.)

Dedication

Karl Strambach

1939–2016

Loops are "non-associative groups"

1. $(Q, \cdot, /, \backslash, 1)$, where

$$x \cdot y = z$$

has **unique solutions**

$$x = z/y, \qquad y = x \backslash z.$$

2. Powers x^n are **not well defined** in general.
3. Right and left **multiplication maps**

$$R_a : x \to xa, \qquad L_a : x \to ax$$

are bijections.

4. The **right multiplication group**

$$G = \langle R_x \mid x \in Q \rangle$$

is a transitive permutation group on Q.

Loops are "non-associative groups"

1. $(Q, \cdot, /, \backslash, 1)$, where

$$x \cdot y = z$$

has **unique solutions**

$$x = z/y, \qquad y = x\backslash z.$$

2. Powers x^n are **not well defined** in general.
3. Right and left **multiplication maps**

$$R_a : x \to xa, \qquad L_a : x \to ax$$

are bijections.

4. The **right multiplication group**

$$G = \langle R_x \mid x \in Q \rangle$$

is a transitive permutation group on Q.

Loops are "non-associative groups"

1. $(Q, \cdot, /, \backslash, 1)$, where
$$x \cdot y = z$$
has **unique solutions**
$$x = z/y, \qquad y = x\backslash z.$$
2. Powers x^n are **not well defined** in general.
3. Right and left **multiplication maps**
$$R_a : x \to xa, \qquad L_a : x \to ax$$
are bijections.
4. The **right multiplication group**
$$G = \langle R_x \mid x \in Q \rangle$$
is a transitive permutation group on Q.

Loops are “non-associative groups”

1. $(Q, \cdot, /, \backslash, 1)$, where
$$x \cdot y = z$$
has **unique solutions**
$$x = z/y, \qquad y = x\backslash z.$$
2. Powers x^n are **not well defined** in general.
3. Right and left **multiplication maps**
$$R_a : x \to xa, \qquad L_a : x \to ax$$
are bijections.
4. The **right multiplication group**
$$G = \langle R_x \mid x \in Q\rangle$$
is a transitive permutation group on Q.

Right Bol loops

1. **Right Bol** identity: $((xy)z)y = x((yz)y)$.
2. **Automorph inverse** property: $(xy)^{-1} = x^{-1}y^{-1}$.
3. **Bruck** = right Bol + AIP.
4. **Uniquely** 2-**divisible:** $x \mapsto x^2$ is invertible.

Examples

- **Non-zero octonions** are both left and right Bol.
- Elements of norm 1 of the **split octonion algebra** $\mathbb{O}(F)$.
- The set of $n \times n$ **positive definite symmetric matrices** with respect to the multiplication

$$A \circ B = (BA^2B)^{\frac{1}{2}}$$

is a uniquely 2-divisible Bruck loop.

Right Bol loops

1. **Right Bol** identity: $((xy)z)y = x((yz)y)$.
2. **Automorph inverse** property: $(xy)^{-1} = x^{-1}y^{-1}$.
3. **Bruck** = right Bol + AIP.
4. **Uniquely** 2-**divisible:** $x \mapsto x^2$ is invertible.

Examples

- **Non-zero octonions** are both left and right Bol.
- Elements of norm 1 of the **split octonion algebra** $\mathbb{O}(F)$.
- The set of $n \times n$ **positive definite symmetric matrices** with respect to the multiplication

$$A \circ B = (BA^2B)^{\frac{1}{2}}$$

is a uniquely 2-divisible Bruck loop.

Right Bol loops

1. **Right Bol** identity: $((xy)z)y = x((yz)y)$.
2. **Automorph inverse** property: $(xy)^{-1} = x^{-1}y^{-1}$.
3. **Bruck** $=$ right Bol $+$ AIP.
4. **Uniquely** 2-**divisible:** $x \mapsto x^2$ is invertible.

Examples

- **Non-zero octonions** are both left and right Bol.
- Elements of norm 1 of the **split octonion algebra** $\mathbb{O}(F)$.
- The set of $n \times n$ **positive definite symmetric matrices** with respect to the multiplication

$$A \circ B = (BA^2B)^{\frac{1}{2}}$$

is a uniquely 2-divisible Bruck loop.

Right Bol loops

1. **Right Bol** identity: $((xy)z)y = x((yz)y)$.
2. **Automorph inverse** property: $(xy)^{-1} = x^{-1}y^{-1}$.
3. **Bruck** = right Bol + AIP.
4. **Uniquely** 2-**divisible:** $x \mapsto x^2$ is invertible.

Examples

- **Non-zero octonions** are both left and right Bol.
- Elements of norm 1 of the **split octonion algebra** $\mathbb{O}(F)$.
- The set of $n \times n$ **positive definite symmetric matrices** with respect to the multiplication

$$A \circ B = (BA^2B)^{\frac{1}{2}}$$

  is a uniquely 2-divisible Bruck loop.

Right Bol loops

1. **Right Bol** identity: $((xy)z)y = x((yz)y)$.
2. **Automorph inverse** property: $(xy)^{-1} = x^{-1}y^{-1}$.
3. **Bruck** $=$ right Bol $+$ AIP.
4. **Uniquely** 2-**divisible:** $x \mapsto x^2$ is invertible.

Examples

- **Non-zero octonions** are both left and right Bol.
- Elements of norm 1 of the **split octonion algebra** $\mathbb{O}(F)$.
- The set of $n \times n$ **positive definite symmetric matrices** with respect to the multiplication
$$A \circ B = (BA^2B)^{\frac{1}{2}}$$
is a uniquely 2-divisible Bruck loop.

Right Bol loops

1. **Right Bol** identity: $((xy)z)y = x((yz)y)$.
2. **Automorph inverse** property: $(xy)^{-1} = x^{-1}y^{-1}$.
3. **Bruck** $=$ right Bol $+$ AIP.
4. **Uniquely** 2-**divisible:** $x \mapsto x^2$ is invertible.

Examples

- **Non-zero octonions** are both left and right Bol.
- Elements of norm 1 of the **split octonion algebra** $\mathbb{O}(F)$.
- The set of $n \times n$ **positive definite symmetric matrices** with respect to the multiplication

$$A \circ B = (BA^2B)^{\frac{1}{2}}$$

is a uniquely 2-divisible Bruck loop.

Right Bol loops

1. **Right Bol** identity: $((xy)z)y = x((yz)y)$.
2. **Automorph inverse** property: $(xy)^{-1} = x^{-1}y^{-1}$.
3. **Bruck** $=$ right Bol $+$ AIP.
4. **Uniquely** 2**-divisible:** $x \mapsto x^2$ is invertible.

Examples

- **Non-zero octonions** are both left and right Bol.
- Elements of norm 1 of the **split octonion algebra** $\mathbb{O}(F)$.
- The set of $n \times n$ **positive definite symmetric matrices** with respect to the multiplication

$$A \circ B = (BA^2B)^{\frac{1}{2}}$$

is a uniquely 2-divisible Bruck loop.

Right Bol loops

1. **Right Bol** identity: $((xy)z)y = x((yz)y)$.
2. **Automorph inverse** property: $(xy)^{-1} = x^{-1}y^{-1}$.
3. **Bruck** $=$ right Bol $+$ AIP.
4. **Uniquely** 2-**divisible:** $x \mapsto x^2$ is invertible.

Examples

- **Non-zero octonions** are both left and right Bol.
- Elements of norm 1 of the **split octonion algebra** $\mathbb{O}(F)$.
- The set of $n \times n$ **positive definite symmetric matrices** with respect to the multiplication

$$A \circ B = (BA^2B)^{\frac{1}{2}}$$

is a uniquely 2-divisible Bruck loop.

Elementary properties

1. **Power-associativity:** x^n is well-defined for all $n \in \mathbb{Z}$.
2. Bol loops are power-associative and

$$\underbrace{(((x\,y)y)\cdots)y}_{n} = x \cdot y^n$$

holds for all n. That is,

$$R_y^n = R_{y^n}.$$

3. $\Rightarrow$ All cycles of R_y have the **same length** $o(y)$.
4. $\Rightarrow$ $o(y)$ divides $|Q|$.
5. $\Rightarrow$ Bol loops of **prime order** are cyclic groups.

Theorem (Burn 1978-1981)

- Bol loops of order $2p$, p^2 are groups.
- There are non-associative Bol loops of order $4p$, $2p^2$ and p^3.

Elementary properties

1. **Power-associativity:** x^n is well-defined for all $n \in \mathbb{Z}$.
2. Bol loops are power-associative and

$$(((x\,\underbrace{y)y)\cdots)y}_{n} = x \cdot y^n$$

holds for all n. That is,

$$R_y^n = R_{y^n}.$$

3. $\Rightarrow$ All cycles of R_y have the **same length** $o(y)$.
4. $\Rightarrow$ $o(y)$ divides $|Q|$.
5. $\Rightarrow$ Bol loops of **prime order** are cyclic groups.

Theorem (Burn 1978-1981)

- Bol loops of order $2p$, p^2 are groups.
- There are non-associative Bol loops of order $4p$, $2p^2$ and p^3.

Elementary properties

1. **Power-associativity:** x^n is well-defined for all $n \in \mathbb{Z}$.
2. Bol loops are power-associative and

$$(((x\underbrace{y)y)\cdots)y}_{n} = x \cdot y^n$$

holds for all n. That is,

$$R_y^n = R_{y^n}.$$

3. $\Rightarrow$ All cycles of R_y have the **same length** $o(y)$.
4. $\Rightarrow$ $o(y)$ divides $|Q|$.
5. $\Rightarrow$ Bol loops of **prime order** are cyclic groups.

Theorem (Burn 1978-1981)

- Bol loops of order $2p$, p^2 are groups.
- There are non-associative Bol loops of order $4p$, $2p^2$ and p^3.

Elementary properties

1. **Power-associativity:** x^n is well-defined for all $n \in \mathbb{Z}$.
2. Bol loops are power-associative and

$$(((x\,\underbrace{y)y)\cdots)y}_{n} = x \cdot y^n$$

holds for all n. That is,

$$R_y^n = R_{y^n}.$$

3. $\Rightarrow$ All cycles of R_y have the **same length** $o(y)$.
4. $\Rightarrow$ $o(y)$ divides $|Q|$.
5. $\Rightarrow$ Bol loops of **prime order** are cyclic groups.

Theorem (Burn 1978-1981)

- Bol loops of order $2p$, p^2 are groups.
- There are non-associative Bol loops of order $4p$, $2p^2$ and p^3.

Elementary properties

1. **Power-associativity:** x^n is well-defined for all $n \in \mathbb{Z}$.
2. Bol loops are power-associative and
$$(((x\underbrace{y)y)\cdots)y}_{n} = x \cdot y^n$$
holds for all n. That is,
$$R_y^n = R_{y^n}.$$
3. $\Rightarrow$ All cycles of R_y have the **same length** $o(y)$.
4. $\Rightarrow$ $o(y)$ divides $|Q|$.
5. $\Rightarrow$ Bol loops of **prime order** are cyclic groups.

Theorem (Burn 1978-1981)

- Bol loops of order $2p$, p^2 are groups.
- There are non-associative Bol loops of order $4p$, $2p^2$ and p^3.

Elementary properties

1. **Power-associativity:** x^n is well-defined for all $n \in \mathbb{Z}$.
2. Bol loops are power-associative and

$$(((x\,\underbrace{y)y)\cdots)y}_{n} = x \cdot y^n$$

   holds for all n. That is,

$$R_y^n = R_{y^n}.$$

3. $\Rightarrow$ All cycles of R_y have the **same length** $o(y)$.
4. $\Rightarrow$ $o(y)$ divides $|Q|$.
5. $\Rightarrow$ Bol loops of **prime order** are cyclic groups.

Theorem (Burn 1978-1981)

- Bol loops of order $2p$, p^2 are groups.
- There are non-associative Bol loops of order $4p$, $2p^2$ and p^3.

Elementary properties

1. **Power-associativity:** x^n is well-defined for all $n \in \mathbb{Z}$.
2. Bol loops are power-associative and
$$((\underbrace{(x\,y)y)\cdots)y}_{n} = x \cdot y^n$$
holds for all n. That is,
$$R_y^n = R_{y^n}.$$
3. $\Rightarrow$ All cycles of R_y have the **same length** $o(y)$.
4. $\Rightarrow$ $o(y)$ divides $|Q|$.
5. $\Rightarrow$ Bol loops of **prime order** are cyclic groups.

Theorem (Burn 1978-1981)

- Bol loops of order $2p$, p^2 are groups.
- There are non-associative Bol loops of order $4p$, $2p^2$ and p^3.

Elementary properties

1. **Power-associativity:** x^n is well-defined for all $n \in \mathbb{Z}$.
2. Bol loops are power-associative and

$$(((x\,\underbrace{y)y)\cdots)y}_{n} = x \cdot y^n$$

   holds for all n. That is,

$$R_y^n = R_{y^n}.$$

3. $\Rightarrow$ All cycles of R_y have the **same length** $o(y)$.
4. $\Rightarrow$ $o(y)$ divides $|Q|$.
5. $\Rightarrow$ Bol loops of **prime order** are cyclic groups.

Theorem (Burn 1978-1981)

- Bol loops of order $2p$, p^2 are groups.
- There are non-associative Bol loops of order $4p$, $2p^2$ and p^3.

Properties related to Glauberman's Z^*-theorem (1968)

Property	**for Bol loops**	**for Bruck loops**
$\lvert Q\rvert$ odd	$\lvert G\rvert$ odd with the same prime factors as $\lvert Q\rvert$	Q is solvable
$\lvert Q\rvert = p^n$	G is a p-group and Q is solvable	Q is nilpotent
$\forall x : o(x) = p^k$ (p odd)	$\lvert Q\rvert$ is a p-power and Q is solvable	Q is nilpotent

Examples

Properties related to Glauberman's Z^*-theorem (1968)

Property	for Bol loops	for Bruck loops
$\lvert Q\rvert$ odd	$\lvert G\rvert$ odd with the same prime factors as $\lvert Q\rvert$	Q is solvable
$\lvert Q\rvert = p^n$	G is a p-group and Q is solvable	Q is nilpotent
$\forall x : o(x) = p^k$ (p odd)	$\lvert Q\rvert$ is a p-power and Q is solvable	Q is nilpotent

Examples

- **Non-nilpotent** Bol p-loops: GN, Kiechle (2002), Kinyon, Phillips, Foguel (2006).
- **Simple** (non-solvable) Bol loops of odd order and Bol loops of exponent 2: GN (2007).

Properties related to Glauberman's Z^*-theorem (1968)

Property	**for Bol loops**	**for Bruck loops**
$\lvert Q\rvert$ odd	$\lvert G\rvert$ odd with the same prime factors as $\lvert Q\rvert$	Q is solvable
$\lvert Q\rvert = p^n$	G is a p-group and Q is solvable	Q is nilpotent
$\forall x : o(x) = p^k$ (p odd)	$\lvert Q\rvert$ is a p-power and Q is solvable	Q is nilpotent

Examples

- **Non-nilpotent** Bol p-loops: GN, Kiechle (2002), Kinyon, Phillips, Foguel (2006).
- **Simple** (non-solvable) Bol loops of odd order and Bol loops of exponent 2: GN (2007).

Properties related to Glauberman's Z^*-theorem (1968)

Property	for Bol loops	for Bruck loops
$\lvert Q\rvert$ odd	$\lvert G\rvert$ odd with the same prime factors as $\lvert Q\rvert$	Q is solvable
$\lvert Q\rvert = p^n$	G is a p-group and Q is solvable	Q is nilpotent
$\forall x : o(x) = p^k$ (p odd)	$\lvert Q\rvert$ is a p-power and Q is solvable	Q is nilpotent

Examples

- **Non-nilpotent** Bol p-loops: GN, Kiechle (2002), Kinyon, Phillips, Foguel (2006).
- **Simple** (non-solvable) Bol loops of odd order and Bol loops of exponent 2: GN (2007).

The associated Bruck loop of 2-divisible Bol loops

Let Q be a Bol loop of odd order. Then

1. Q is **uniquely** 2-**divisible;** we denote the inverse of $x \to x^2$ by $x \to x^{\frac{1}{2}}$.
2. We define the **associated Bruck loop** $Q(\circ)$ by
$$x \circ y = ((yx^2)y)^{\frac{1}{2}}.$$
3. Inverse and powers of elements coincide in Q and $Q(\circ)$.
4. G is a **central extension** of $G(\circ)$.
5. $|G(\circ)|$, $|G|$ and $|Q|$ have the **same prime factors.**

The associated Bruck loop of 2-divisible Bol loops

Let Q be a Bol loop of odd order. Then

1. Q is **uniquely** 2-**divisible;** we denote the inverse of $x \to x^2$ by $x \to x^{\frac{1}{2}}$.
2. We define the **associated Bruck loop** $Q(\circ)$ by
$$x \circ y = ((yx^2)y)^{\frac{1}{2}}.$$
3. Inverse and powers of elements coincide in Q and $Q(\circ)$.
4. G is a **central extension** of $G(\circ)$.
5. $|G(\circ)|$, $|G|$ and $|Q|$ have the **same prime factors.**

The associated Bruck loop of 2-divisible Bol loops

Let Q be a Bol loop of odd order. Then

1. Q is **uniquely** 2-**divisible;** we denote the inverse of $x \to x^2$ by $x \to x^{\frac{1}{2}}$.
2. We define the **associated Bruck loop** $Q(\circ)$ by
$$x \circ y = ((yx^2)y)^{\frac{1}{2}}.$$
3. Inverse and powers of elements coincide in Q and $Q(\circ)$.
4. G is a **central extension** of $G(\circ)$.
5. $|G(\circ)|$, $|G|$ and $|Q|$ have the **same prime factors.**

The associated Bruck loop of 2-divisible Bol loops

Let Q be a Bol loop of odd order. Then

1. Q is **uniquely** 2-**divisible;** we denote the inverse of $x \to x^2$ by $x \to x^{\frac{1}{2}}$.
2. We define the **associated Bruck loop** $Q(\circ)$ by

$$x \circ y = ((yx^2)y)^{\frac{1}{2}}.$$

3. Inverse and powers of elements coincide in Q and $Q(\circ)$.
4. G is a **central extension** of $G(\circ)$.
5. $|G(\circ)|$, $|G|$ and $|Q|$ have the **same prime factors.**

The associated Bruck loop of 2-divisible Bol loops

Let Q be a Bol loop of odd order. Then

1. Q is **uniquely** 2-**divisible;** we denote the inverse of $x \to x^2$ by $x \to x^{\frac{1}{2}}$.
2. We define the **associated Bruck loop** $Q(\circ)$ by

$$x \circ y = ((yx^2)y)^{\frac{1}{2}}.$$

3. Inverse and powers of elements coincide in Q and $Q(\circ)$.
4. G is a **central extension** of $G(\circ)$.
5. $|G(\circ)|$, $|G|$ and $|Q|$ have the **same prime factors.**

Results by Niederreiter, Robinson (1981)

Theorem (Niederreiter, Robinson 1981)

Let $p > q$ be odd primes.

1. If q divides $p^2 - 1$ then there exists a **nonassociative right Bruck loop** $B_{p,q}$ of order pq, and a **non-Bruck right Bol loop** of order pq.
2. A right Bol loop of order pq contains a **unique subloop of order** p, and when $q = 3$ then the unique subloop of order p is normal.
3. There are at least $(p+1)/2$ right Bol loops of order $3p$ up to isomorphism, and at least $(p+5)/6$ right Bol loops of order $3p$ up to isotopism.

Results by Niederreiter, Robinson (1981)

Theorem (Niederreiter, Robinson 1981)

Let $p > q$ be odd primes.

1. If q divides $p^2 - 1$ then there exists a **nonassociative right Bruck loop** $B_{p,q}$ of order pq, and a **non-Bruck right Bol loop** of order pq.
2. A right Bol loop of order pq contains a **unique subloop of order** p, and when $q = 3$ then the unique subloop of order p is normal.
3. There are at least $(p+1)/2$ right Bol loops of order $3p$ up to isomorphism, and at least $(p+5)/6$ right Bol loops of order $3p$ up to isotopism.

Results by Niederreiter, Robinson (1981)

Theorem (Niederreiter, Robinson 1981)

Let $p > q$ be odd primes.

1. If q divides $p^2 - 1$ then there exists a **nonassociative right Bruck loop** $B_{p,q}$ of order pq, and a **non-Bruck right Bol loop** of order pq.
2. A right Bol loop of order pq contains a **unique subloop of order** p**,** and when $q = 3$ then the unique subloop of order p is normal.
3. There are at least $(p+1)/2$ right Bol loops of order $3p$ up to isomorphism, and at least $(p+5)/6$ right Bol loops of order $3p$ up to isotopism.

Results by Niederreiter, Robinson (1981)

Theorem (Niederreiter, Robinson 1981)

Let $p > q$ be odd primes.

1. If q divides $p^2 - 1$ then there exists a **nonassociative right Bruck loop** $B_{p,q}$ of order pq, and a **non-Bruck right Bol loop** of order pq.
2. A right Bol loop of order pq contains a **unique subloop of order** p, and when $q = 3$ then the unique subloop of order p is normal.
3. There are at least $(p+1)/2$ right Bol loops of order $3p$ up to isomorphism, and at least $(p+5)/6$ right Bol loops of order $3p$ up to isotopism.

Multiplication formula by Niederreiter, Robinson (1981)

- Let Q be right Bol loop of order pq, $p > q$ odd primes.
- Put $Q = \mathbb{F}_q \times \mathbb{F}_p$ as underlying set.

Consider the following properties

(P1) The unique subloop of order p is normal.

(P2) The multiplication of Q is given by the formula

$$(x_1, y_1)(x_2, y_2) = (x_1 + x_2, z + (y_1 + z)\vartheta_{x_1}^{-1}\vartheta_{x_1+x_2}) \qquad (*)$$

where for $x \in \mathbb{F}_q$, $\vartheta_x : \mathbb{F}_p \to \mathbb{F}_p$ are certain **complete mappings** and $z + z\vartheta_{x_2} = y_2$.

(P3) The multiplication of Q is given by (*) with ***linear* complete mappings** $\vartheta_x \in \mathbb{F}_p \setminus \{0, -1\}$.

- Clearly, (P3)⇒(P2)⇒(P1).
- [NR81] had (P1)⇒(P2) + complete classification for loops with (P3).

Multiplication formula by Niederreiter, Robinson (1981)

- Let Q be right Bol loop of order pq, $p > q$ odd primes.
- Put $Q = \mathbb{F}_q \times \mathbb{F}_p$ as underlying set.

Consider the following properties

(P1) The unique subloop of order p is normal.

(P2) The multiplication of Q is given by the formula

$$(x_1, y_1)(x_2, y_2) = (x_1 + x_2, z + (y_1 + z)\vartheta_{x_1}^{-1}\vartheta_{x_1+x_2}) \qquad (*)$$

where for $x \in \mathbb{F}_q$, $\vartheta_x : \mathbb{F}_p \to \mathbb{F}_p$ are certain **complete mappings** and $z + z\vartheta_{x_2} = y_2$.

(P3) The multiplication of Q is given by (*) with ***linear* complete mappings** $\vartheta_x \in \mathbb{F}_p \setminus \{0, -1\}$.

- Clearly, (P3)$\Rightarrow$(P2)$\Rightarrow$(P1).
- [NR81] had (P1)$\Rightarrow$(P2) + complete classification for loops with (P3).

Multiplication formula by Niederreiter, Robinson (1981)

- Let Q be right Bol loop of order pq, $p > q$ odd primes.
- Put $Q = \mathbb{F}_q \times \mathbb{F}_p$ as underlying set.

Consider the following properties

(P1) The unique subloop of order p is normal.

(P2) The multiplication of Q is given by the formula

$$(x_1, y_1)(x_2, y_2) = (x_1 + x_2, z + (y_1 + z)\vartheta_{x_1}^{-1}\vartheta_{x_1+x_2}) \qquad (*)$$

where for $x \in \mathbb{F}_q$, $\vartheta_x : \mathbb{F}_p \to \mathbb{F}_p$ are certain **complete mappings** and $z + z\vartheta_{x_2} = y_2$.

(P3) The multiplication of Q is given by (*) with ***linear* complete mappings** $\vartheta_x \in \mathbb{F}_p \setminus \{0, -1\}$.

- Clearly, (P3)⇒(P2)⇒(P1).
- [NR81] had (P1)⇒(P2) + complete classification for loops with (P3).

Multiplication formula by Niederreiter, Robinson (1981)

- Let Q be right Bol loop of order pq, $p > q$ odd primes.
- Put $Q = \mathbb{F}_q \times \mathbb{F}_p$ as underlying set.

Consider the following properties

(P1) The unique subloop of order p is normal.

(P2) The multiplication of Q is given by the formula

$$(x_1, y_1)(x_2, y_2) = (x_1 + x_2, z + (y_1 + z)\vartheta_{x_1}^{-1}\vartheta_{x_1+x_2}) \qquad (*)$$

where for $x \in \mathbb{F}_q$, $\vartheta_x : \mathbb{F}_p \to \mathbb{F}_p$ are certain **complete mappings** and $z + z\vartheta_{x_2} = y_2$.

(P3) The multiplication of Q is given by (*) with ***linear* complete mappings** $\vartheta_x \in \mathbb{F}_p \setminus \{0, -1\}$.

- Clearly, (P3)⇒(P2)⇒(P1).
- [NR81] had (P1)⇒(P2) + complete classification for loops with (P3).

Multiplication formula by Niederreiter, Robinson (1981)

- Let Q be right Bol loop of order pq, $p > q$ odd primes.
- Put $Q = \mathbb{F}_q \times \mathbb{F}_p$ as underlying set.

Consider the following properties

(P1) The unique subloop of order p is normal.

(P2) The multiplication of Q is given by the formula

$$(x_1, y_1)(x_2, y_2) = (x_1 + x_2, z + (y_1 + z)\vartheta_{x_1}^{-1}\vartheta_{x_1+x_2}) \qquad (*)$$

where for $x \in \mathbb{F}_q$, $\vartheta_x : \mathbb{F}_p \to \mathbb{F}_p$ are certain **complete mappings** and $z + z\vartheta_{x_2} = y_2$.

(P3) The multiplication of Q is given by (*) with ***linear* complete mappings** $\vartheta_x \in \mathbb{F}_p \setminus \{0, -1\}$.

- Clearly, (P3)⇒(P2)⇒(P1).
- [NR81] had (P1)⇒(P2) + complete classification for loops with (P3).

Multiplication formula by Niederreiter, Robinson (1981)

- Let Q be right Bol loop of order pq, $p > q$ odd primes.
- Put $Q = \mathbb{F}_q \times \mathbb{F}_p$ as underlying set.

Consider the following properties

(P1) The unique subloop of order p is normal.

(P2) The multiplication of Q is given by the formula

$$(x_1, y_1)(x_2, y_2) = (x_1 + x_2, z + (y_1 + z)\vartheta_{x_1}^{-1}\vartheta_{x_1+x_2}) \qquad (*)$$

where for $x \in \mathbb{F}_q$, $\vartheta_x : \mathbb{F}_p \to \mathbb{F}_p$ are certain **complete mappings** and $z + z\vartheta_{x_2} = y_2$.

(P3) The multiplication of Q is given by (*) with ***linear* complete mappings** $\vartheta_x \in \mathbb{F}_p \setminus \{0, -1\}$.

- Clearly, (P3)⇒(P2)⇒(P1).
- [NR81] had (P1)⇒(P2) + complete classification for loops with (P3).

Multiplication formula by Niederreiter, Robinson (1981)

- Let Q be right Bol loop of order pq, $p > q$ odd primes.
- Put $Q = \mathbb{F}_q \times \mathbb{F}_p$ as underlying set.

Consider the following properties

(P1) The unique subloop of order p is normal.

(P2) The multiplication of Q is given by the formula

$$(x_1, y_1)(x_2, y_2) = (x_1 + x_2, z + (y_1 + z)\vartheta_{x_1}^{-1}\vartheta_{x_1+x_2}) \qquad (*)$$

where for $x \in \mathbb{F}_q$, $\vartheta_x : \mathbb{F}_p \to \mathbb{F}_p$ are certain **complete mappings** and $z + z\vartheta_{x_2} = y_2$.

(P3) The multiplication of Q is given by (*) with ***linear* complete mappings** $\vartheta_x \in \mathbb{F}_p \setminus \{0, -1\}$.

- Clearly, (P3)⇒(P2)⇒(P1).
- [NR81] had (P1)⇒(P2) + complete classification for loops with (P3).

Multiplication formula by Niederreiter, Robinson (1981)

- Let Q be right Bol loop of order pq, $p > q$ odd primes.
- Put $Q = \mathbb{F}_q \times \mathbb{F}_p$ as underlying set.

Consider the following properties

(P1) The unique subloop of order p is normal.

(P2) The multiplication of Q is given by the formula

$$(x_1, y_1)(x_2, y_2) = (x_1 + x_2, z + (y_1 + z)\vartheta_{x_1}^{-1}\vartheta_{x_1+x_2}) \qquad (*)$$

where for $x \in \mathbb{F}_q$, $\vartheta_x : \mathbb{F}_p \to \mathbb{F}_p$ are certain **complete mappings** and $z + z\vartheta_{x_2} = y_2$.

(P3) The multiplication of Q is given by (*) with ***linear* complete mappings** $\vartheta_x \in \mathbb{F}_p \setminus \{0, -1\}$.

- Clearly, (P3)$\Rightarrow$(P2)$\Rightarrow$(P1).
- [NR81] had (P1)$\Rightarrow$(P2) + complete classification for loops with (P3).

The impact of [NR81]

1. Burn (1985) claimed that there is a unique nonassociative right Bol loop of order $2p^2$.
2. Sharma (1984) constructed two examples of order 18, Burn accounted for the second class of examples in a correction, and Sharma, Solarin (1986) gave an independent proof.
3. Sharma, Solarin (1988) came up with a conflicting estimate on the number of right Bol loops of order $3p$.
4. A problem with their proof was pointed out in Niederreiter, Robinson (1994).
5. Sharma (1987) also attempted to prove that the unique subloop of order p is normal, and that a right Bol loop of order pq must be associative when q does not divide $p^2 - 1$.
6. Both of these results turn out to be true but the proofs are incorrect (there are counterexamples to some intermediate claims made in the proofs).

The impact of [NR81]

1. Burn (1985) claimed that there is a unique nonassociative right Bol loop of order $2p^2$.
2. Sharma (1984) constructed two examples of order 18, Burn accounted for the second class of examples in a correction, and Sharma, Solarin (1986) gave an independent proof.
3. Sharma, Solarin (1988) came up with a conflicting estimate on the number of right Bol loops of order $3p$.
4. A problem with their proof was pointed out in Niederreiter, Robinson (1994).
5. Sharma (1987) also attempted to prove that the unique subloop of order p is normal, and that a right Bol loop of order pq must be associative when q does not divide $p^2 - 1$.
6. Both of these results turn out to be true but the proofs are incorrect (there are counterexamples to some intermediate claims made in the proofs).

The impact of [NR81]

1. Burn (1985) claimed that there is a unique nonassociative right Bol loop of order $2p^2$.
2. Sharma (1984) constructed two examples of order 18, Burn accounted for the second class of examples in a correction, and Sharma, Solarin (1986) gave an independent proof.
3. Sharma, Solarin (1988) came up with a conflicting estimate on the number of right Bol loops of order $3p$.
4. A problem with their proof was pointed out in Niederreiter, Robinson (1994).
5. Sharma (1987) also attempted to prove that the unique subloop of order p is normal, and that a right Bol loop of order pq must be associative when q does not divide $p^2 - 1$.
6. Both of these results turn out to be true but the proofs are incorrect (there are counterexamples to some intermediate claims made in the proofs).

The impact of [NR81]

1. Burn (1985) claimed that there is a unique nonassociative right Bol loop of order $2p^2$.
2. Sharma (1984) constructed two examples of order 18, Burn accounted for the second class of examples in a correction, and Sharma, Solarin (1986) gave an independent proof.
3. Sharma, Solarin (1988) came up with a conflicting estimate on the number of right Bol loops of order $3p$.
4. A problem with their proof was pointed out in Niederreiter, Robinson (1994).
5. Sharma (1987) also attempted to prove that the unique subloop of order p is normal, and that a right Bol loop of order pq must be associative when q does not divide $p^2 - 1$.
6. Both of these results turn out to be true but the proofs are incorrect (there are counterexamples to some intermediate claims made in the proofs).

The impact of [NR81]

1. Burn (1985) claimed that there is a unique nonassociative right Bol loop of order $2p^2$.
2. Sharma (1984) constructed two examples of order 18, Burn accounted for the second class of examples in a correction, and Sharma, Solarin (1986) gave an independent proof.
3. Sharma, Solarin (1988) came up with a conflicting estimate on the number of right Bol loops of order $3p$.
4. A problem with their proof was pointed out in Niederreiter, Robinson (1994).
5. Sharma (1987) also attempted to prove that the unique subloop of order p is normal, and that a right Bol loop of order pq must be associative when q does not divide $p^2 - 1$.
6. Both of these results turn out to be true but the proofs are incorrect (there are counterexamples to some intermediate claims made in the proofs).

The impact of [NR81]

1. Burn (1985) claimed that there is a unique nonassociative right Bol loop of order $2p^2$.
2. Sharma (1984) constructed two examples of order 18, Burn accounted for the second class of examples in a correction, and Sharma, Solarin (1986) gave an independent proof.
3. Sharma, Solarin (1988) came up with a conflicting estimate on the number of right Bol loops of order $3p$.
4. A problem with their proof was pointed out in Niederreiter, Robinson (1994).
5. Sharma (1987) also attempted to prove that the unique subloop of order p is normal, and that a right Bol loop of order pq must be associative when q does not divide $p^2 - 1$.
6. Both of these results turn out to be true but the proofs are incorrect (there are counterexamples to some intermediate claims made in the proofs).

Results on Bruck loops of order pq

Theorem 1 (Kinyon, N, Vojtěchovský 2017)

Let $p > q$ be odd primes.

1. A nonassociative right Bol loop Q of order pq exists if and only if q divides $p^2 - 1$.
2. If q divides $p^2 - 1$, there exists a unique nonassociative right Bruck loop $B_{p,q}$ of order pq up to isomorphism.
3. The right multiplication group of $B_{p,q}$ is isomorphic to $C_p^2 \rtimes C_q$.
4. The right multiplication group of Q has order p^2q or p^3q.
5. Q contains a unique subloop of order p and this subloop is normal.
6. This subloop of order p equals the left nucleus of Q.

Results on Bruck loops of order pq

Theorem 1 (Kinyon, N, Vojtěchovský 2017)

Let $p > q$ be odd primes.

1. A nonassociative right Bol loop Q of order pq exists if and only if q divides $p^2 - 1$.
2. If q divides $p^2 - 1$, there exists a unique nonassociative right Bruck loop $B_{p,q}$ of order pq up to isomorphism.
3. The right multiplication group of $B_{p,q}$ is isomorphic to $C_p^2 \rtimes C_q$.
4. The right multiplication group of Q has order p^2q or p^3q.
5. Q contains a unique subloop of order p and this subloop is normal.
6. This subloop of order p equals the left nucleus of Q.

Results on Bruck loops of order pq

Theorem 1 (Kinyon, N, Vojtěchovský 2017)

Let $p > q$ be odd primes.

1. A nonassociative right Bol loop Q of order pq exists if and only if q divides $p^2 - 1$.
2. If q divides $p^2 - 1$, there exists a unique nonassociative right Bruck loop $B_{p,q}$ of order pq up to isomorphism.
3. The right multiplication group of $B_{p,q}$ is isomorphic to $C_p^2 \rtimes C_q$.
4. The right multiplication group of Q has order p^2q or p^3q.
5. Q contains a unique subloop of order p and this subloop is normal.
6. This subloop of order p equals the left nucleus of Q.

Results on Bruck loops of order pq

Theorem 1 (Kinyon, N, Vojtěchovský 2017)

Let $p > q$ be odd primes.

1. A nonassociative right Bol loop Q of order pq exists if and only if q divides $p^2 - 1$.
2. If q divides $p^2 - 1$, there exists a unique nonassociative right Bruck loop $B_{p,q}$ of order pq up to isomorphism.
3. The right multiplication group of $B_{p,q}$ is isomorphic to $C_p^2 \rtimes C_q$.
4. The right multiplication group of Q has order p^2q or p^3q.
5. Q contains a unique subloop of order p and this subloop is normal.
6. This subloop of order p equals the left nucleus of Q.

Results on Bruck loops of order pq

Theorem 1 (Kinyon, N, Vojtěchovský 2017)

Let $p > q$ be odd primes.

1. A nonassociative right Bol loop Q of order pq exists if and only if q divides $p^2 - 1$.
2. If q divides $p^2 - 1$, there exists a unique nonassociative right Bruck loop $B_{p,q}$ of order pq up to isomorphism.
3. The right multiplication group of $B_{p,q}$ is isomorphic to $C_p^2 \rtimes C_q$.
4. The right multiplication group of Q has order p^2q or p^3q.
5. Q contains a unique subloop of order p and this subloop is normal.
6. This subloop of order p equals the left nucleus of Q.

Results on Bruck loops of order pq

Theorem 1 (Kinyon, N, Vojtěchovský 2017)

Let $p > q$ be odd primes.

1. A nonassociative right Bol loop Q of order pq exists if and only if q divides $p^2 - 1$.
2. If q divides $p^2 - 1$, there exists a unique nonassociative right Bruck loop $B_{p,q}$ of order pq up to isomorphism.
3. The right multiplication group of $B_{p,q}$ is isomorphic to $C_p^2 \rtimes C_q$.
4. The right multiplication group of Q has order p^2q or p^3q.
5. Q contains a unique subloop of order p and this subloop is normal.
6. This subloop of order p equals the left nucleus of Q.

Results on Bruck loops of order pq

Theorem 1 (Kinyon, N, Vojtěchovský 2017)

Let $p > q$ be odd primes.

1. A nonassociative right Bol loop Q of order pq exists if and only if q divides $p^2 - 1$.
2. If q divides $p^2 - 1$, there exists a unique nonassociative right Bruck loop $B_{p,q}$ of order pq up to isomorphism.
3. The right multiplication group of $B_{p,q}$ is isomorphic to $C_p^2 \rtimes C_q$.
4. The right multiplication group of Q has order p^2q or p^3q.
5. Q contains a unique subloop of order p and this subloop is normal.
6. This subloop of order p equals the left nucleus of Q.

Concerning the proof of Theorem 1

1. Let Q be a non-cyclic Bol loop of order pq, and let $Q(\circ)$ be its associated Bruck loop.
2. We know that $Q(\circ)$ is solvable and non-associative.
3. We show that $q \mid p^2 - 1$ and $G(\circ) \cong C_p^2 \rtimes C_q$.
4. By Glauberman, the class of Bruck loops of odd order is ***essentially equivalent*** with the class of pairs (T, τ) where T is a group of odd order and τ is an involutory automorphism of T.
5. This implies the uniqueness for $Q(\circ)$
6. and $|G| = p^2q$ or $|G| = p^3q$.
7. The latter implies that the unique subloop of order p is normal.
8. Further elementary study of G implies (6).

Concerning the proof of Theorem 1

1. Let Q be a non-cyclic Bol loop of order pq, and let $Q(\circ)$ be its associated Bruck loop.
2. We know that $Q(\circ)$ is solvable and non-associative.
3. We show that $q \mid p^2 - 1$ and $G(\circ) \cong C_p^2 \rtimes C_q$.
4. By Glauberman, the class of Bruck loops of odd order is ***essentially equivalent*** with the class of pairs (T, τ) where T is a group of odd order and τ is an involutory automorphism of T.
5. This implies the uniqueness for $Q(\circ)$
6. and $|G| = p^2q$ or $|G| = p^3q$.
7. The latter implies that the unique subloop of order p is normal.
8. Further elementary study of G implies (6).

Concerning the proof of Theorem 1

1. Let Q be a non-cyclic Bol loop of order pq, and let $Q(\circ)$ be its associated Bruck loop.
2. We know that $Q(\circ)$ is solvable and non-associative.
3. We show that $q \mid p^2 - 1$ and $G(\circ) \cong C_p^2 \rtimes C_q$.
4. By Glauberman, the class of Bruck loops of odd order is ***essentially equivalent*** with the class of pairs (T, τ) where T is a group of odd order and τ is an involutory automorphism of T.
5. This implies the uniqueness for $Q(\circ)$
6. and $|G| = p^2 q$ or $|G| = p^3 q$.
7. The latter implies that the unique subloop of order p is normal.
8. Further elementary study of G implies (6).

Concerning the proof of Theorem 1

1. Let Q be a non-cyclic Bol loop of order pq, and let $Q(\circ)$ be its associated Bruck loop.
2. We know that $Q(\circ)$ is solvable and non-associative.
3. We show that $q \mid p^2 - 1$ and $G(\circ) \cong C_p^2 \rtimes C_q$.
4. By Glauberman, the class of Bruck loops of odd order is ***essentially equivalent*** with the class of pairs (T, τ) where T is a group of odd order and τ is an involutory automorphism of T.
5. This implies the uniqueness for $Q(\circ)$
6. and $|G| = p^2 q$ or $|G| = p^3 q$.
7. The latter implies that the unique subloop of order p is normal.
8. Further elementary study of G implies (6).

Concerning the proof of Theorem 1

1. Let Q be a non-cyclic Bol loop of order pq, and let $Q(\circ)$ be its associated Bruck loop.
2. We know that $Q(\circ)$ is solvable and non-associative.
3. We show that $q \mid p^2 - 1$ and $G(\circ) \cong C_p^2 \rtimes C_q$.
4. By Glauberman, the class of Bruck loops of odd order is ***essentially equivalent*** with the class of pairs (T, τ) where T is a group of odd order and τ is an involutory automorphism of T.
5. This implies the uniqueness for $Q(\circ)$
6. and $|G| = p^2 q$ or $|G| = p^3 q$.
7. The latter implies that the unique subloop of order p is normal.
8. Further elementary study of G implies (6).

Concerning the proof of Theorem 1

1. Let Q be a non-cyclic Bol loop of order pq, and let $Q(\circ)$ be its associated Bruck loop.
2. We know that $Q(\circ)$ is solvable and non-associative.
3. We show that $q \mid p^2 - 1$ and $G(\circ) \cong C_p^2 \rtimes C_q$.
4. By Glauberman, the class of Bruck loops of odd order is ***essentially equivalent*** with the class of pairs (T, τ) where T is a group of odd order and τ is an involutory automorphism of T.
5. This implies the uniqueness for $Q(\circ)$
6. and $|G| = p^2 q$ or $|G| = p^3 q$.
7. The latter implies that the unique subloop of order p is normal.
8. Further elementary study of G implies (6).

Concerning the proof of Theorem 1

1. Let Q be a non-cyclic Bol loop of order pq, and let $Q(\circ)$ be its associated Bruck loop.
2. We know that $Q(\circ)$ is solvable and non-associative.
3. We show that $q \mid p^2 - 1$ and $G(\circ) \cong C_p^2 \rtimes C_q$.
4. By Glauberman, the class of Bruck loops of odd order is ***essentially equivalent*** with the class of pairs (T, τ) where T is a group of odd order and τ is an involutory automorphism of T.
5. This implies the uniqueness for $Q(\circ)$
6. and $|G| = p^2q$ or $|G| = p^3q$.
7. The latter implies that the unique subloop of order p is normal.
8. Further elementary study of G implies (6).

Concerning the proof of Theorem 1

1. Let Q be a non-cyclic Bol loop of order pq, and let $Q(\circ)$ be its associated Bruck loop.
2. We know that $Q(\circ)$ is solvable and non-associative.
3. We show that $q \mid p^2 - 1$ and $G(\circ) \cong C_p^2 \rtimes C_q$.
4. By Glauberman, the class of Bruck loops of odd order is ***essentially equivalent*** with the class of pairs (T, τ) where T is a group of odd order and τ is an involutory automorphism of T.
5. This implies the uniqueness for $Q(\circ)$
6. and $|G| = p^2 q$ or $|G| = p^3 q$.
7. The latter implies that the unique subloop of order p is normal.
8. Further elementary study of G implies (6).

Results on non-Bruck Bol loops of order pq

Theorem 2 (Kinyon, N, Vojtěchovský 2017)

A right Bol loop Q can be constructed on $\mathbb{F}_q \times \mathbb{F}_p$ by formula (*)

$$(x_1, y_1)(x_2, y_2) = (x_1 + x_2, y_2(\mathrm{id} + \vartheta_{x_2})^{-1} + (y_1 + y_2(\mathrm{id} + \vartheta_{x_2})^{-1})\vartheta_{x_1}^{-1}\vartheta_{x_1+x_2})$$

where the linear complete mappings $\vartheta_x \in \mathbb{F}_p$ are chosen as follows.

1. Either $\vartheta_x = 1$ for every $x \in \mathbb{F}_q$,
2. or
$$\vartheta_x = (\gamma\omega^x + (1-\gamma)\omega^{-x})^{-1}$$
for every $x \in \mathbb{F}_q$, where ω is a fixed primitive qth root of unity in $\mathbb{F}_{p^2}$, $\gamma \in \Gamma$ and Γ is a fixed subset of $\mathbb{F}_{p^2}$ of cardinality $(p-q+2)/2$.
3. $\vartheta_x \equiv 1$ results in the cyclic group of order pq.
4. $\gamma = 1/2$ results in the Bruck loop $B_{p,q}$.
5. If $q \mid p-1$, then $\gamma = 1$ results in the nonabelian group of order pq.

Results on non-Bruck Bol loops of order pq

Theorem 2 (Kinyon, N, Vojtěchovský 2017)

A right Bol loop Q can be constructed on $\mathbb{F}_q \times \mathbb{F}_p$ by formula (*)

$$(x_1, y_1)(x_2, y_2) = (x_1 + x_2, y_2(\mathrm{id} + \vartheta_{x_2})^{-1} + (y_1 + y_2(\mathrm{id} + \vartheta_{x_2})^{-1})\vartheta_{x_1}^{-1}\vartheta_{x_1+x_2})$$

where the linear complete mappings $\vartheta_x \in \mathbb{F}_p$ are chosen as follows.

1. Either $\vartheta_x = 1$ for every $x \in \mathbb{F}_q$,
2. or
$$\vartheta_x = (\gamma\omega^x + (1-\gamma)\omega^{-x})^{-1}$$
for every $x \in \mathbb{F}_q$, where ω is a fixed primitive qth root of unity in $\mathbb{F}_{p^2}$, $\gamma \in \Gamma$ and Γ is a fixed subset of $\mathbb{F}_{p^2}$ of cardinality $(p-q+2)/2$.
3. $\vartheta_x \equiv 1$ results in the cyclic group of order pq.
4. $\gamma = 1/2$ results in the Bruck loop $B_{p,q}$.
5. If $q \mid p-1$, then $\gamma = 1$ results in the nonabelian group of order pq.

Results on non-Bruck Bol loops of order pq

Theorem 2 (Kinyon, N, Vojtěchovský 2017)

A right Bol loop Q can be constructed on $\mathbb{F}_q \times \mathbb{F}_p$ by formula (*)

$$(x_1, y_1)(x_2, y_2) = (x_1 + x_2, y_2(\mathrm{id} + \vartheta_{x_2})^{-1} + (y_1 + y_2(\mathrm{id} + \vartheta_{x_2})^{-1})\vartheta_{x_1}^{-1}\vartheta_{x_1+x_2})$$

where the linear complete mappings $\vartheta_x \in \mathbb{F}_p$ are chosen as follows.

1. Either $\vartheta_x = 1$ for every $x \in \mathbb{F}_q$,
2. or
$$\vartheta_x = (\gamma\omega^x + (1-\gamma)\omega^{-x})^{-1}$$
for every $x \in \mathbb{F}_q$, where ω is a fixed primitive qth root of unity in $\mathbb{F}_{p^2}$, $\gamma \in \Gamma$ and Γ is a fixed subset of $\mathbb{F}_{p^2}$ of cardinality $(p-q+2)/2$.
3. $\vartheta_x \equiv 1$ results in the cyclic group of order pq.
4. $\gamma = 1/2$ results in the Bruck loop $B_{p,q}$.
5. If $q \mid p-1$, then $\gamma = 1$ results in the nonabelian group of order pq.

Theorem 2 (Kinyon, N, Vojtěchovský 2017)

A right Bol loop Q can be constructed on $\mathbb{F}_q \times \mathbb{F}_p$ by formula (*)

$$(x_1, y_1)(x_2, y_2) = (x_1 + x_2, y_2(\mathrm{id} + \vartheta_{x_2})^{-1} + (y_1 + y_2(\mathrm{id} + \vartheta_{x_2})^{-1})\vartheta_{x_1}^{-1}\vartheta_{x_1+x_2})$$

where the linear complete mappings $\vartheta_x \in \mathbb{F}_p$ are chosen as follows.

1. Either $\vartheta_x = 1$ for every $x \in \mathbb{F}_q$,
2. or
$$\vartheta_x = (\gamma\omega^x + (1-\gamma)\omega^{-x})^{-1}$$
for every $x \in \mathbb{F}_q$, where ω is a fixed primitive qth root of unity in $\mathbb{F}_{p^2}$, $\gamma \in \Gamma$ and Γ is a fixed subset of $\mathbb{F}_{p^2}$ of cardinality $(p - q + 2)/2$.
3. $\vartheta_x \equiv 1$ results in the cyclic group of order pq.
4. $\gamma = 1/2$ results in the Bruck loop $B_{p,q}$.
5. If $q \mid p - 1$, then $\gamma = 1$ results in the nonabelian group of order pq.

Results on non-Bruck Bol loops of order pq

Theorem 2 (Kinyon, N, Vojtěchovský 2017)

A right Bol loop Q can be constructed on $\mathbb{F}_q \times \mathbb{F}_p$ by formula (*)

$$(x_1, y_1)(x_2, y_2) = (x_1 + x_2, y_2(\mathrm{id} + \vartheta_{x_2})^{-1} + (y_1 + y_2(\mathrm{id} + \vartheta_{x_2})^{-1})\vartheta_{x_1}^{-1}\vartheta_{x_1+x_2})$$

where the linear complete mappings $\vartheta_x \in \mathbb{F}_p$ are chosen as follows.

1. Either $\vartheta_x = 1$ for every $x \in \mathbb{F}_q$,
2. or
$$\vartheta_x = (\gamma\omega^x + (1-\gamma)\omega^{-x})^{-1}$$
for every $x \in \mathbb{F}_q$, where ω is a fixed primitive qth root of unity in $\mathbb{F}_{p^2}$, $\gamma \in \Gamma$ and Γ is a fixed subset of $\mathbb{F}_{p^2}$ of cardinality $(p-q+2)/2$.
3. $\vartheta_x \equiv 1$ results in the cyclic group of order pq.
4. $\gamma = 1/2$ results in the Bruck loop $B_{p,q}$.
5. If $q \mid p-1$, then $\gamma = 1$ results in the nonabelian group of order pq.

Results on non-Bruck Bol loops of order pq

Theorem 2 (Kinyon, N, Vojtěchovský 2017)

A right Bol loop Q can be constructed on $\mathbb{F}_q \times \mathbb{F}_p$ by formula (*)

$$(x_1, y_1)(x_2, y_2) = (x_1 + x_2, y_2(\mathrm{id} + \vartheta_{x_2})^{-1} + (y_1 + y_2(\mathrm{id} + \vartheta_{x_2})^{-1})\vartheta_{x_1}^{-1}\vartheta_{x_1+x_2})$$

where the linear complete mappings $\vartheta_x \in \mathbb{F}_p$ are chosen as follows.

1. Either $\vartheta_x = 1$ for every $x \in \mathbb{F}_q$,
2. or
$$\vartheta_x = (\gamma\omega^x + (1-\gamma)\omega^{-x})^{-1}$$
for every $x \in \mathbb{F}_q$, where ω is a fixed primitive qth root of unity in $\mathbb{F}_{p^2}$, $\gamma \in \Gamma$ and Γ is a fixed subset of $\mathbb{F}_{p^2}$ of cardinality $(p-q+2)/2$.
3. $\vartheta_x \equiv 1$ results in the cyclic group of order pq.
4. $\gamma = 1/2$ results in the Bruck loop $B_{p,q}$.
5. If $q \mid p-1$, then $\gamma = 1$ results in the nonabelian group of order pq.

Concerning the proof of Theorem 2

1. By [NR81], the normality of the unique subloop of order p implies (*) with complete mappings ϑ_x.
2. The linearity of ϑ_x follows from the following:

Lemma

Let $p > q$ be odd primes, and let Q be a groupoid defined on $\mathbb{F}_q \times \mathbb{F}_p$ by (*), where every θ_x is a complete mapping of $\mathbb{F}_p$. Write $a = (1,0)$ and $b = (0,1)$. Then $b^j \cdot a^k b^\ell = b^j a^k \cdot b^\ell$ holds for every j, ℓ if and only if θ_k is linear.

3. The formula for ϑ_x follows from the following:

Observation by Niederreiter and Robinson (1981)

The sequence $u_x = \vartheta_x^{-1}$ of period q satisfies the **linear recurrence relation**

$$u_0 = 1, \qquad u_{x+2} = \lambda u_{x+1} - u_x \qquad \text{for some } \lambda \in \mathbb{F}_p.$$

Concerning the proof of Theorem 2

1. By [NR81], the normality of the unique subloop of order p implies (*) with complete mappings ϑ_x.
2. The linearity of ϑ_x follows from the following:

Lemma

Let $p > q$ be odd primes, and let Q be a groupoid defined on $\mathbb{F}_q \times \mathbb{F}_p$ by (*), where every θ_x is a complete mapping of $\mathbb{F}_p$. Write $a = (1,0)$ and $b = (0,1)$. Then $b^j \cdot a^k b^\ell = b^j a^k \cdot b^\ell$ holds for every j, ℓ if and only if θ_k is linear.

3. The formula for ϑ_x follows from the following:

Observation by Niederreiter and Robinson (1981)

The sequence $u_x = \vartheta_x^{-1}$ of period q satisfies the **linear recurrence relation**

$$u_0 = 1, \qquad u_{x+2} = \lambda u_{x+1} - u_x \qquad \text{for some } \lambda \in \mathbb{F}_p.$$

Concerning the proof of Theorem 2

1. By [NR81], the normality of the unique subloop of order p implies (*) with complete mappings ϑ_x.
2. The linearity of ϑ_x follows from the following:

Lemma

Let $p > q$ be odd primes, and let Q be a groupoid defined on $\mathbb{F}_q \times \mathbb{F}_p$ by (*), where every θ_x is a complete mapping of $\mathbb{F}_p$. Write $a = (1,0)$ and $b = (0,1)$. Then $b^j \cdot a^k b^\ell = b^j a^k \cdot b^\ell$ holds for every j, ℓ if and only if θ_k is linear.

3. The formula for ϑ_x follows from the following:

Observation by Niederreiter and Robinson (1981)

The sequence $u_x = \vartheta_x^{-1}$ of period q satisfies the **linear recurrence relation**

$$u_0 = 1, \qquad u_{x+2} = \lambda u_{x+1} - u_x \qquad \text{for some } \lambda \in \mathbb{F}_p.$$

Concerning the proof of Theorem 2

1. By [NR81], the normality of the unique subloop of order p implies (*) with complete mappings ϑ_x.
2. The linearity of ϑ_x follows from the following:

Lemma

Let $p > q$ be odd primes, and let Q be a groupoid defined on $\mathbb{F}_q \times \mathbb{F}_p$ by (*), where every θ_x is a complete mapping of $\mathbb{F}_p$. Write $a = (1, 0)$ and $b = (0, 1)$. Then $b^j \cdot a^k b^\ell = b^j a^k \cdot b^\ell$ holds for every j, ℓ if and only if θ_k is linear.

3. The formula for ϑ_x follows from the following:

Observation by Niederreiter and Robinson (1981)

The sequence $u_x = \vartheta_x^{-1}$ of period q satisfies the **linear recurrence relation**

$$u_0 = 1, \qquad u_{x+2} = \lambda u_{x+1} - u_x \qquad \text{for some } \lambda \in \mathbb{F}_p.$$

Concerning the proof of Theorem 2

1. By [NR81], the normality of the unique subloop of order p implies (*) with complete mappings ϑ_x.
2. The linearity of ϑ_x follows from the following:

Lemma

Let $p > q$ be odd primes, and let Q be a groupoid defined on $\mathbb{F}_q \times \mathbb{F}_p$ by (*), where every θ_x is a complete mapping of $\mathbb{F}_p$. Write $a = (1,0)$ and $b = (0,1)$. Then $b^j \cdot a^k b^\ell = b^j a^k \cdot b^\ell$ holds for every j, ℓ if and only if θ_k is linear.

3. The formula for ϑ_x follows from the following:

Observation by Niederreiter and Robinson (1981)

The sequence $u_x = \vartheta_x^{-1}$ of period q satisfies the **linear recurrence relation**

$$u_0 = 1, \qquad u_{x+2} = \lambda u_{x+1} - u_x \qquad \text{for some } \lambda \in \mathbb{F}_p.$$

The number of Bol loops of order pq

1. We also have complete control on the **isomorphism problem** of Bol loops given by (*)
2. Hence, we know the **number of isomorphism classes** of Bol loops of order pq.

Corollary

There are precisely $(p - q + 4)/2$ right Bol loops of order pq up to isomorphism.

3. For the **number of isotopy classes** we had a conjecture when $q = 3$.
4. This was proved in full generality

Theorem (Stuhl, Vojtěchovský)

With primes $2 < q < p$, the number of right Bol loops of order pq up to isotopism is equal to $\left\lfloor \frac{p - 1 + 4q}{2q} \right\rfloor$.

The number of Bol loops of order pq

1. We also have complete control on the **isomorphism problem** of Bol loops given by (*)
2. Hence, we know the **number of isomorphism classes** of Bol loops of order pq.

Corollary

There are precisely $(p-q+4)/2$ right Bol loops of order pq up to isomorphism.

3. For the **number of isotopy classes** we had a conjecture when $q=3$.
4. This was proved in full generality

Theorem (Stuhl, Vojtěchovský)

With primes $2<q<p$, the number of right Bol loops of order pq up to isotopism is equal to $\left\lfloor \frac{p-1+4q}{2q} \right\rfloor$.

The number of Bol loops of order pq

1. We also have complete control on the **isomorphism problem** of Bol loops given by (*)
2. Hence, we know the **number of isomorphism classes** of Bol loops of order pq.

Corollary

There are precisely $(p - q + 4)/2$ right Bol loops of order pq up to isomorphism.

3. For the **number of isotopy classes** we had a conjecture when $q = 3$.
4. This was proved in full generality

Theorem (Stuhl, Vojtěchovský)

With primes $2 < q < p$, the number of right Bol loops of order pq up to isotopism is equal to $\left\lfloor \frac{p-1+4q}{2q} \right\rfloor$.

The number of Bol loops of order pq

1. We also have complete control on the **isomorphism problem** of Bol loops given by (*)
2. Hence, we know the **number of isomorphism classes** of Bol loops of order pq.

Corollary

There are precisely $(p - q + 4)/2$ right Bol loops of order pq up to isomorphism.

3. For the **number of isotopy classes** we had a conjecture when $q = 3$.
4. This was proved in full generality

Theorem (Stuhl, Vojtěchovský)

With primes $2 < q < p$, the number of right Bol loops of order pq up to isotopism is equal to $\left\lfloor \frac{p - 1 + 4q}{2q} \right\rfloor$.

The number of Bol loops of order pq

1. We also have complete control on the **isomorphism problem** of Bol loops given by (*)
2. Hence, we know the **number of isomorphism classes** of Bol loops of order pq.

Corollary

There are precisely $(p - q + 4)/2$ right Bol loops of order pq up to isomorphism.

3. For the **number of isotopy classes** we had a conjecture when $q = 3$.
4. This was proved in full generality

Theorem (Stuhl, Vojtěchovský)

With primes $2 < q < p$, the number of right Bol loops of order pq up to isotopism is equal to $\left\lfloor \dfrac{p - 1 + 4q}{2q} \right\rfloor$.

The number of Bol loops of order pq

1. We also have complete control on the **isomorphism problem** of Bol loops given by (*)
2. Hence, we know the **number of isomorphism classes** of Bol loops of order pq.

Corollary

There are precisely $(p-q+4)/2$ right Bol loops of order pq up to isomorphism.

3. For the **number of isotopy classes** we had a conjecture when $q=3$.
4. This was proved in full generality

Theorem (Stuhl, Vojtěchovský)

With primes $2 < q < p$, the number of right Bol loops of order pq up to isotopism is equal to $\left\lfloor \dfrac{p-1+4q}{2q} \right\rfloor$.

Further project: Bol loops of order $p^a q$

1. I would like to start a

Project

Investigate right Bol loops of order $p^a q$, with primes p, q and $q > 2$.

2. If p, q are primes such that $q > 2$ and $q \mid p^p - 1$ then there is a **simple** right Bol loop of order $p^{p+1} q$.
3. There are infinitely many simple Bol loops of **exponent** 2 of order $3 \cdot 2^a$.
4. Not much known on Bol loops of order $p^2 q$.
5. Work in progress on Bol loops of order 24...

Further project: Bol loops of order $p^a q$

1. I would like to start a

Project

Investigate right Bol loops of order $p^a q$, with primes p, q and $q > 2$.

2. If p, q are primes such that $q > 2$ and $q \mid p^p - 1$ then there is a **simple** right Bol loop of order $p^{p+1} q$.
3. There are infinitely many simple Bol loops of **exponent** 2 of order $3 \cdot 2^a$.
4. Not much known on Bol loops of order $p^2 q$.
5. Work in progress on Bol loops of order 24...

Further project: Bol loops of order $p^a q$

1. I would like to start a

Project

Investigate right Bol loops of order $p^a q$, with primes p, q and $q > 2$.

2. If p, q are primes such that $q > 2$ and $q \mid p^p - 1$ then there is a **simple** right Bol loop of order $p^{p+1} q$.
3. There are infinitely many simple Bol loops of **exponent** 2 of order $3 \cdot 2^a$.
4. Not much known on Bol loops of order $p^2 q$.
5. Work in progress on Bol loops of order 24...

Further project: Bol loops of order $p^a q$

1. I would like to start a

Project

Investigate right Bol loops of order $p^a q$, with primes p, q and $q > 2$.

2. If p, q are primes such that $q > 2$ and $q \mid p^p - 1$ then there is a **simple** right Bol loop of order $p^{p+1} q$.
3. There are infinitely many simple Bol loops of **exponent** 2 of order $3 \cdot 2^a$.
4. Not much known on Bol loops of order $p^2 q$.
5. Work in progress on Bol loops of order 24...

Further project: Bol loops of order $p^a q$

1. I would like to start a

Project

Investigate right Bol loops of order $p^a q$, with primes p, q and $q > 2$.

2. If p, q are primes such that $q > 2$ and $q \mid p^p - 1$ then there is a **simple** right Bol loop of order $p^{p+1} q$.
3. There are infinitely many simple Bol loops of **exponent** 2 of order $3 \cdot 2^a$.
4. Not much known on Bol loops of order $p^2 q$.
5. Work in progress on Bol loops of order 24...

Further project: Bol loops of order $p^a q$

1. I would like to start a

Project

Investigate right Bol loops of order $p^a q$, with primes p, q and $q > 2$.

2. If p, q are primes such that $q > 2$ and $q \mid p^p - 1$ then there is a **simple** right Bol loop of order $p^{p+1} q$.
3. There are infinitely many simple Bol loops of **exponent** 2 of order $3 \cdot 2^a$.
4. Not much known on Bol loops of order $p^2 q$.
5. Work in progress on Bol loops of order 24...

Acknowledgement

THANK YOU FOR YOUR ATTENTION!