INVOLUTORY LATIN QUANDLES OF ORDER PQ

PŘEMYSL JEDLIČKA

Abstract. We present a construction of a family of involutory latin quandles, a family that contains all non-Alexander involutory latin quandles of order pq, for $p < q$ odd primes. Such quandles exist if and only if p divides $q^2 - 1$.

1. Introduction

Involutory quandles appear naturally in several areas of mathematics and therefore they were given different names, such as kei, symmetric spaces or right symmetric right distributive idempotent right quasigroups; see [13] for a survey on involutory quandles. Actually, in geometry or in topology, the quandles we study are often latin; we refer to [14] for a guide on latin quandles.

The best understood class of quandles are Alexander quandles and all the smallest examples of quandles are actually Alexander. For instance, the smallest non-Alexander involutory latin quandle is of order 15. It is not difficult to describe this quandle using an ad-hoc formula but what about other involutory latin quandles of a semiprime order?

It is well known, already for a long time [12, 7, 9], that there is a one-to-one correspondence between involutory latin quandles and 2-divisible Bruck loops, see Theorem 3.1. Finite 2-divisible Bruck loops are some generalizations of abelian groups of odd orders and share many properties with groups of odd orders. For instance, they are solvable and, in the case of p-loops, even nilpotent [1]. It is therefore possible to construct all these loops using cohomology, like in [15].

Considering Bruck loops of order pq, the first researchers who constructed some of them were Niederreiter and Robinson [10], using a recursive construction. It has been conjectured for a long time that their loops are the only Bruck loops of order pq but all attempts to prove it failed until the work of Kinyon, Nagy and Vojtěchovský [8]. We summarize here their result as Theorem 4.1 and we easily conclude:

Theorem 1.1. *Let $p < q$ be two odd primes. Then there exists unique, up to isomorphism, involutory latin Alexander quandle of order pq. There exists a non-Alexander involutory latin quandle of order pq if and only if p divides $q^2 - 1$. Such a quandle is unique, up to isomorphism.*

One thing is to know that a quandle exists and another thing is to give a formula how to construct it. To do this, we use yet another algebraic structure – commutative automorphic loops; being commutative and having a nice structural behavior, they seem to be easier to construct than Bruck loops [3]. And it was proved in [2] that, given a commutative automorphic loop of an odd order, we can construct a Bruck loop of it. This is not not a one-to-one correspondence [15] but it does not matter here. Some commutative automorphic loops of order pq were constructed in [5] and they give our Bruck loops of order pq.

This paper contains very few new results, it is rather a synthesis of different results from different papers. In Section 2 we give necessary definitions and fundamental properties of the objects we are working with. In Section 3 we present the correspondence between involutory latin quandles

Date: February 27, 2019.
2000 *Mathematics Subject Classification.* 20N05,57M27.
Key words and phrases. Involutory quandles, quasigroups, Bruck loops, finite fields.

and 2-divisible Bruck loops. And in Section 4 we write down the formula how to construct the involutory latin quandles of order pq.

2. Preliminaries

Definition 2.1. A groupoid $(G,*)$ is *uniquely 2-divisible* if the mapping $x \mapsto x*x$ is a bijection.

Example 2.2. Every idempotent groupoid, that means groupoid satisfying $x*x=x$, is uniquely 2-divisible. A finite group G is uniquely 2-divisible if and only if the order of G is odd.

Definition 2.3. Let G be a groupoid with an operation $*$. We define the *left translation* L_x as the mapping $a \mapsto x*a$ and the *right translation* R_x as the mapping $a \mapsto a*x$. We say that the groupoid G is a *left* (respectively *right*) *quasigroup* if the left translations (respectively right translations) are permutations.

If G is a left (respectively right) quasigroup then we write $x \setminus y$ for $L_x^{-1}(y)$, respectively y/x for $R_x^{-1}(y)$. We define the *left* (respectively *right*) *multiplication group* of G as the permutation group generated by translations, i.e.

$$\mathrm{LMlt}(G) = \langle L_x;\ x \in G\rangle, \qquad \mathrm{RMlt}(G) = \langle R_x;\ x \in G\rangle.$$

Definition 2.4. A *quandle* is a right quasigroup that satisfies

$$x*x = x \quad \text{(idempotency)} \quad \text{and} \quad (x*y)*z = (x*z)*(y*z) \quad \text{(right distributivity)}.$$

A quandle is called *involutory* if it satisfies $(x*y)*y = x$. A quandle is called *latin*, if it is a left quasigroup as well.

Example 2.5. Let A be an abelian group and let f be an automorphism of A. An operation on A defined as

$$x*y = f(x-y)+y$$

forms a quandle. Such a quandle is called an *Alexander* quandle. This quandle is involutory if and only if f is involutory. In particular, if $f=-\mathrm{id}$, that means $x*y = 2y-x$, then such an involutory quandle is called the *core* of the group A.

An Alexander quandle is latin if and only if $\mathrm{id}-f$ is an automorphism. It is not difficult to show that an Alexander quandle is latin and involutory if and only if it is the core of a uniquely 2-divisible abelian group.

Definition 2.6. Let Q be a quandle and let $e \in Q$. The *displacement* group of Q is the group

$$\mathrm{Dis}(Q) = \langle R_x R_y^{-1};\ x,y \in Q\rangle = \langle R_x R_e^{-1};\ x \in Q\rangle.$$

Example 2.7. Let Q be an Alexander quandle obtained from an abelian group A and an automorphism f. Then $R_x R_0^{-1}(z) = R_x(f^{-1}(z)) = z - f(x) + x$. Therefore, as an abstract group, $\mathrm{Dis}(Q) \cong \mathrm{Im}(\mathrm{id}-f)$. If Q is involutory, it is well known that $\mathrm{RMlt}(Q) \cong \mathrm{Dis}(Q) \rtimes \mathbb{Z}_2$.

Definition 2.8. A *loop* is a left and right quasigroup with a neutral element. A loop is called *power associative* if every mono-generated subloop is a group.

If we work in a general loop $(Q,+)$, then $3\cdot x$ is not well defined since $x+(x+x) \neq (x+x)+x$. This is not the case of power associative loops, here $k\cdot x$ is uniquely defined, for every $k \in \mathbb{Z}$. In particular, $-x = x\setminus 0 = x/0$. The mapping $x \mapsto -x$ is then a bijection which is usually denoted by J.

Definition 2.9. A power associative loop $(Q,+)$ is called a *right Bruck* loop, if it satisfies

- $-(x+y) = (-x)+(-y)$, or equivalently $JR_y = R_{J(y)}J$, for all $x,y \in Q$,
- $((z+x)+y)+x = z+((x+y)+x)$, or equivalently $R_xR_yR_x = R_{R_xR_y(x)}$, for all $x,y,z \in Q$.

Right Bruck loops are generalizations of abelian groups. They can be found mainly in non-euclidean geometry, often under different names as *K-loops* [6] or *gyrocommutative gyrogroups* [16]. In a euclidean space the sum of two vectors forms an abelian group, whereas in a non-euclidean space the addition is neither commutative nor associative. But it satisfies both identities shown above an hence it forms (at least locally) a 2-divisible Bruck loop, see e.g. [17].

Among well-known properties [11] of right Bruck loops we shall benefit of $R_{i\cdot u} = R_u^i$, in particular $R_{J(x)} = R_{-x} = R_x^{-1}$. And of a characterization of finite 2-divisible Bruck loops.

Proposition 2.10. [1] *A finite right Bruck loop Q is uniquely 2-divisible if and only if $|Q|$ is odd.*

3. Correspondence between involutory latin quandles and 2-divisible right Bruck loops

The well-known correspondence between abelian groups and their cores has its origins in geometry. Suppose that we work on a manifold with following properties: there exists a unique geodesic between each pair of points and we can measure its length. We can then define "the reflection of x through y", denoted by $x * y$, as the point on the geodesic from to x via y such that y is the midpoint between x and $x*y$. It is easy to see that a groupoid so defined is an involutory quandle. Moreover, if every line from x to y has a midpoint, this midpoint is $x \setminus y$ since $x * (x \setminus y) = y$ and therefore the quandle is latin.

Now, if we are in a euclidean space, the operation $x * y$ can be derived using affine coordinates. We choose an origin 0 and then $x * y = 2 \cdot y - x$, independently on the origin. On the other hand, $x + y$ can be derived from the reflection operation: $x + y = (x * 0) * (0 \setminus y)$. If the space is not euclidean then this correspondence works as well, only that the addition is not an abelian group.

Theorem 3.1. [7],[12],[15]

(1) *Let $(Q,*)$ be an involutory latin quandle and let $0 \in Q$. Then $F_{\mathbf{Q}\to\mathbf{B}}(Q,*)$, which is the groupoid $(Q,+,0)$ with the operation $+$ defined by*
$$x + y = (x/0) * (0 \setminus y) = (x * 0) * (0 \setminus y),$$
is a uniquely 2-divisible right Bruck loop.

(2) *Let $(Q,+,0)$ be a uniquely 2-divisible right Bruck loop. Then $F_{\mathbf{B}\to\mathbf{Q}}(Q,+)$, which is the groupoid $(Q,*)$ with the operation $*$ defined by*
$$x * y = (-x) + (y + y) = -x + 2y,$$
is an involutory latin quandle.

(3) *These constructions are mutually inverse, that means $F_{\mathbf{Q}\to\mathbf{B}}(F_{\mathbf{B}\to\mathbf{Q}}(Q,+)) = (Q,+)$ and $F_{\mathbf{B}\to\mathbf{Q}}(F_{\mathbf{Q}\to\mathbf{B}}(Q,*)) = (Q,*)$*

An immediate consequence is due to Proposition 2.10.

Corollary 3.2. *A finite involutory latin quandle is of an odd order.*

Let an involutory latin quandle be $F_{\mathbf{B}\to\mathbf{Q}}$ of a non-associative Bruck loop. Is it possible that the quandle is Alexander? An effective criterion how to recognize an Alexander quandle was described in [4]; nevertheless we do not need that much detail here, we focus on one property only; as we saw in Example 2.7, the displacement group of an Alexander quandle is commutative.

Proposition 3.3. *Let $(Q,*)$ be an involutory latin quandle. Then* $\mathrm{Dis}(Q,*) = \mathrm{RMlt}(F_{\mathbf{Q}\to\mathbf{B}}(Q,*))$ *and* $\mathrm{RMlt}(Q,*) = \mathrm{Dis}(Q,*) \rtimes \langle R_0 \rangle = \mathrm{RMlt}(F_{\mathbf{Q}\to\mathbf{B}}(Q,*)) \rtimes \langle J \rangle$.

Proof. We shall denote by $(Q,+,0)$ the corresponding loop and we shall distinguish right translations of the quandle and of the loop by superscripts.

The group $\mathrm{Dis}(Q,*)$ is generated by the elements $R^*_x(R^*_0)^{-1}$. Now $R^*_x(R^*_0)^{-1} = R^+_{2\cdot x}J(R^+_{2\cdot 0}J)^{-1} = R^+_{2\cdot x}$ and hence $\mathrm{Dis}(Q,*)$ and $\mathrm{RMlt}(Q)$ have the same generators.

Since $R^*_0 = R^+_{2\cdot 0}J = J$, the group $\mathrm{RMlt}(Q,+)$ is generated by $\mathrm{RMlt}(Q,+)\cup\{J\}$. Now $JR^+_x(y) = -(y+x) = -y+(-x) = (R^+_{-x})J(y) = (R^+_x)^{-1}J(y)$ and we see that $\mathrm{RMlt}(Q,*)$ is a semidirect product of $\mathrm{RMlt}(Q,+)$ and $\langle J\rangle$ determined by the homomorphism $J \mapsto (\alpha \mapsto \alpha^{-1})$. $\square$

Lemma 3.4. *Let Q be a loop. Then $\mathrm{RMlt}(Q)$ is commutative if and only if Q is an abelian group.*

Proof. Let $\mathrm{RMlt}(Q)$ be commutative. Then, for all $x, y \in Q$, $R_xR_y = R_yR_x$ implies $(0+x)+y = (0+y)+x$ and therefore Q is commutative. Furthermore,

$$x+(y+z) = (y+z)+x = (y+x)+z = (x+y)+z.$$

The other direction is evident. $\square$

Combining the previous two results we immediately obtain

Corollary 3.5. *An involutory latin quandle $(Q,*)$ is Alexander if and only if $F_{\mathbf{Q}\to\mathbf{B}}(Q,*)$ is an abelian group.*

4. Construction of right Bruck loops of order pq

In this section we finally describe all involutory latin quandles of order pq. For this we need the classification of right Bruck loops of order pq.

Theorem 4.1. [8, Theorem 1.1, Proposition 4.7] *Let $p < q$ be two odd primes.*

(1) *There exists a non-associative right Bruck loop of order pq if and only if p divides q^2-1 and such a loop is unique up to isomorphism.*
(2) *If p divides q^2-1 then a non-associative right Bruck loop of order pq can be constructed on a set $\mathbb{F}_q \times \mathbb{F}_p$ with the multiplication*
$$(a,i)*(b,j) = (b\cdot(1+\theta_j)^{-1} + (a+b\cdot(1+\theta_j)^{-1})\cdot\theta_i^{-1}\theta_{i+j}, i+j),$$
where $\theta_0,\dots,\theta_{p-1}$ are defined as $\theta_i = 2\cdot(\zeta^i+\zeta^{-i})^{-1}$, where $\zeta \in \mathbb{F}_{q^2}$ is a primitive p-th root of unity.
(3) *If p divides q and Q is a non-associative right Bruck loop of order pq then $\mathrm{RMlt}(Q) \cong (\mathbb{Z}_q \times \mathbb{Z}_q) \rtimes \mathbb{Z}_p$.*

From this theorem we immediately obtain Theorem 1.1.

Proof of Theorem 1.1. There exists only one abelian group of order pq, namely the cyclic one. This group has only one involutory automorphism, namely the inversion. Hence there exists a unique, up to isomorphism, involutory Alexander quandle of order pq and this quandle is latin, since $1-(-1)$ is an invertible element in a cyclic group of order pq.

According to Theorem 3.1 and Corollary 3.5, there is a 1-1 correspondence between involutory non-Alexander latin quandles of order pq and non-associative right Bruck loops of order pq. And, according to Theorem 4.1, such a loop exists if and only if p divides q^2-1 and it is unique. $\square$

Theorem 4.1 reveals how to construct the right Bruck loop of order pq. We shall, however, use a different construction because it is arguably more transparent and it is more general. In this construction we obtain a right Bruck loop of order pq if we set $M = R = \mathbb{F}_q$, $S = \mathbb{F}_{q^2}$ and $k = p$.

Theorem 4.2. [5, Theorem 28] *Let M be a faithful module over a ring R, which is either a field or the ring $\mathbb{Z}_n$. Suppose that, for some odd number k, there exists ζ, an element lying in a quadratic extension S of R, that satisfies:*

- *ζ is of order k in S^*,*

- *ζ is a root of a polynomial x^2+cx+1, for some $c \in R$.*

Then we can define a loop on the set $M \times \mathbb{Z}_k$ as follows:

$$(a,i)*(b,j) = \left(a \cdot \frac{\zeta^j \cdot (\zeta^i+1)^2}{(\zeta^{i+j}+1)^2} + b \cdot \frac{(\zeta^{2i+j}+1)\cdot(\zeta^j+1)}{(\zeta^{i+j}+1)^2} \;,\; i+j \right). \tag{4.1}$$

This loop is a non-associative right Bruck loop.

The property that $\zeta^2+1=-c\zeta$ ensures that the expression is well defined, i.e. that both the fractions lie in the ring R, although the numerators and the denominators may lie in $S \setminus R$.

For each k, there may exist several elements ζ. It was shown in [5] that the choice of ζ is irrelevant when R is a field since we always obtain isomorphic loops. We may, on the other hand, obtain non-isomorphic loops if the ring is not a field. Another interesting question is the sole existence of such a ζ. We give several examples.

Example 4.3. Let $R=\mathbb{R}$ and $k>2$ an arbitrary odd number. Then such ζ always exists, namely $\zeta = \cos\frac{2\pi}{k} + i \cdot \sin\frac{2\pi}{k}$, since this number lies in $\mathbb{C}$ which is a quadratic extension of $\mathbb{R}$ and ζ is a root of $x^2 - 2\cos\frac{2\pi}{k}x + 1$.

Example 4.4. If $R=\mathbb{Q}$ then such ζ exists for $k=3$ only. The number $-\frac{1}{2}+i\cdot\frac{\sqrt{3}}{2}$ is a root of x^2+x+1, whereas $x^{k-1}+x^{k-2}+\cdots+x+1$ does not split as a product of quadratic polynomials with rational coefficients, for $k>3$ and k odd.

Example 4.5. Let $R=\mathbb{F}_q$. There are two possibilities: every $\zeta \in R^*$ is a root of $x^2-(\zeta+\zeta^{-1})x+1$ and it satisfies $\zeta^{q-1}=1$. Therefore k may be any odd divisor of $q-1$. The other possibility is $\zeta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. It is then not difficult to prove [5, Proposition 9] that k may be any odd divisor of $q+1$.

Theorem 4.6. *Let M be a faithful module over a ring R, which is either a field or the ring $\mathbb{Z}_n$. Suppose that, for some odd number k, there exists ζ, an element lying in a quadratic extension S of R, that satisfies:*

- *ζ is of order k in S^*,*
- *ζ is a root of a polynomial x^2+cx+1, for some $c \in R$.*

Then we can define a quasigroup on the set $M \times \mathbb{Z}_k$ as follows:

$$(a,i)*(b,j) = \left(b \cdot \frac{(\zeta^j+1)^2 \cdot (\zeta^{2j-2i}+1)}{(\zeta^{2j-i}+1)^2} - a \cdot \frac{(\zeta^{j-i}+\zeta^j)^2}{(\zeta^{2j-i}+1)^2} \;,\; 2j-i \right). \tag{4.2}$$

This quasigroup is an involutory latin quandle which is not Alexander.

Proof. Let us construct a Bruck loop $(Q,+,0)$ on the set $M \times \mathbb{Z}_k$ using Theorem 4.2 and we shall compute the operation $*$ of $F_{\mathbf{B}\to\mathbf{Q}}(Q,+)$, following Theorem 3.1. We first compute

$$2\cdot(b,j) = \left(\frac{b\cdot\zeta^j\cdot(\zeta^j+1)^2 + b\cdot(\zeta^{3j}+1)\cdot(\zeta^j+1)}{(\zeta^{2j}+1)^2}, 2j \right) =$$
$$= \left(\frac{b\cdot(\zeta^j+1)\cdot(\zeta^{2j}+\zeta^j+\zeta^{3j}+1)}{(\zeta^{2j}+1)^2}, 2j \right) = \left(\frac{b\cdot(\zeta^j+1)^2\cdot(\zeta^{2j}+1)}{(\zeta^{2j}+1)^2}, 2j \right) = \left(b\cdot\frac{(\zeta^j+1)^2}{\zeta^{2j}+1}, 2j \right)$$

and we prove that $-(a,i)=(-a,-i)$:

$$(a,i)*(-a,-i) = \left(\frac{a\cdot\zeta^{-i}\cdot(\zeta^i+1)^2 - a\cdot(\zeta^i+1)\cdot(\zeta^{-i}+1)}{(1+1)^2}, 0 \right) = (0,0)$$

Finally

$$(-a,-i)+2\cdot(b,j)=\left(\frac{-a\cdot\zeta^{2j}\cdot(\zeta^{-i}+1)^2+b\cdot\frac{(\zeta^j+1)^2}{\zeta^{2j}+1}\cdot(\zeta^{-2i+2j}+1)\cdot(\zeta^{2j}+1)}{(\zeta^{-i+2j}+1)^2},-i+2j\right)$$
$$=\left(\frac{-a\cdot(\zeta^{j-i}+\zeta^j)^2+b\cdot(\zeta^j+1)^2\cdot(\zeta^{2j-2i}+1)}{(\zeta^{2j-i}+1)^2},2j-i\right)\quad\square$$

There are two things worth noting. There is a natural projection $(a,i)\mapsto i$ of $M\times\mathbb{Z}_k$ onto the core of $\mathbb{Z}_k$ which is evidently a homomorphism. On the other hand, by setting $i=j$ we obtain $(a,i)*(b,i)=(2b-a,i)$ and therefore each kernel class of the natural projection is itself isomorphic to the core of M. We can hence view this quandle as a sort of a semidirect extension of the core of M by the core of $\mathbb{Z}_k$.

Remark 4.7. It is straightforward (but tedious) to check that the operation defined in (4.2) is always right distributive and idempotent, if it is well-defined, that means if the denominator is never 0, that means if k is not even. In other words, the construction works for $k=\infty$ too.

References

[1] Glauberman G.: *On loops of odd order I,* J. Algebra **1** (1964), 374–396.
[2] Jedlička P., Kinyon M. K., Vojtěchovský P.: *The structure of commutative automorphic loops*, Trans. Amer. Math. Soc. **363**,1 (2011), 365–384
[3] Jedlička P., Kinyon M. K., Vojtěchovský P.: *Constructions of commutative automorphic loops*, Comm. Algebra **38**,9 (2010), 3243–3267.
[4] Jedlička P., Pilitowska A., Stanovský D., Zamojska-Dzienio A.: *Subquandles of affine quandles,* J. Algebra 510,15 (2018), 259–288
[5] Jedlička P., Simon D.: *On commutative A-loops of order pq* J. Algebra Appl. **14**,3 (2014), 20 pages
[6] Kiechle H.: Theory of K-loops, Lecture Notes in Mathematics **1778**, (2002), Springer-Verlag, Berlin
[7] Kikkawa M.: *On some quasigroups of algebraic models of symmetric spaces,* Mem. Fac. Lit. Sci. Shimane Univ. Natur. Sci. No. 6 (1973), 9–13.
[8] Kinyon M. K., Nagy G. P., Vojtěchovský P.: *Bol loops and Bruck loops of order pq,* J. Algebra **473**,1 (2017) 481–512
[9] Nagy P., Strambach K.: *Loops, their cores and symmetric spaces*, Israel J. Math. **105** (1998), 285–322
[10] Niederreiter H., Robinson K. H.: *Bol loops of order pq,* Math. Proc. Cambridge Philos. Soc. **89**,2 (1981), 241–256
[11] Robinson, D. A.: *Bol loops*, Trans. Amer. Math. Soc. **123** (1966), 341–354
[12] Robinson, D. A.: *A loop-theoretic study of right-sided quasigroups,* Ann. Soc. Sci. Bruxelles Sr. I 93 (1979), no. 1, 7–16.
[13] Stanovský D.: *Origins of involutory quandles*, arXiv:1506.02389
[14] Stanovský D.: *A guide to self-distributive quasigroups, or latin quandles,* Quasigroups and Related Systems **23**,1 (2015), 91–128
[15] Stuhl I., Vojtěchovský P.: *Enumeration of involutory latin quandles, Bruck loops and commutative automorphic loops of odd prime power order,* to appear in Contemporary Mathematics
[16] Ungar A. A.: Beyond the Einstein addition law and its gyroscopic Thomas precession. The theory of gyrogroups and gyrovector spaces., Fundam. Theor. of Physics **117**, Kluwer Academic Publishers Group, (2001), Dordrecht.
[17] Ungar A. A.: *Gyrogroups, the Grouplike Loops in the Service of Hyperbolic Geometry and Einstein's Special Theory of Relativity*, Quasigroups and Related Systems **15** (2007), 141–168
[18] Vojtěchovský P.: *Bol loops and Bruck loops of order pq up to isotopism,* Finite Fields and Their Applications **52** (2018), 1–9

Department of Mathematics, Faculty of Engineering, Czech University of Life Sciences, Kamýcká 129, 165 00, Prague, Czech Republic

E-mail address: `jedlickap@tf.czu.cz`