Contemporary Mathematics

Enumeration of involutory latin quandles, Bruck loops and commutative automorphic loops of odd prime power order

Izabella Stuhl and Petr Vojtěchovský

Abstract. There is a one-to-one correspondence between involutory latin quandles and uniquely 2-divisible Bruck loops. Bruck loops of odd prime power order are centrally nilpotent. Using linear-algebraic approach to central extensions, we enumerate Bruck loops (and hence involutory latin quandles) of order 3^k for $k \leq 5$, except for those loops that are central extensions of the cyclic group of order 3 by the elementary abelian group of order 3^4.

Among the constructed loops there is a Bruck loop of order 3^5 whose associated Γ-loop is not a commutative automorphic loop. We independently enumerate commutative automorphic loops of order 3^k for $k \leq 5$, with the same omission as in the case of Bruck loops.

1. Introduction

Quandles are self-distributive algebras designed for colorings of arcs of oriented knot diagrams [**9, 23**]. The standard axioms of quandles give sufficient (and in some sense necessary) conditions for the arc colorings to be invariant under Reidemeister moves. Quandles also form a class of set-theoretical solutions of the quantum Yang-Baxter equation [**6, 8**]. Of particular interest in both areas are connected quandles, which are quandles whose left translations generate a permutation group that acts transitively on the underlying set [**16**]. Latin quandles form a proper subset of connected quandles and, being quasigroups, they can be investigated not only by methods of quandle theory but also by methods of quasigroup theory [**10**]. For an introduction to quandles, see [**7**].

Bruck loops (also known as K-loops) form a well-studied variety of loops with properties close to abelian groups [**20**]. In his seminal work [**12, 13**], Glauberman derived many structural results for Bruck loops in which all elements have a finite odd order, and then went on to transfer some of these results to Moufang loops. For instance, he proved that every Bruck loop of odd order and every Moufang loop of odd order are solvable [**13**]. Bruck loops are also important in the study of

2010 *Mathematics Subject Classification.* 57M27, 20N05.

Key words and phrases. Quandle, latin quandle, involutory latin quandle, connected quandle, Bruck loop, Bol loop, Γ-loop, automorphic loop, commutative automorphic loop.

Petr Vojtěchovský partially supported by the University of Denver PROF grant.

neardomains [**20**] and show up as a natural algebraic structure describing relativistic addition of vectors [**29**]. For an introduction to loop theory, see [**1, 26**].

There is a one-to-one correspondence between involutory latin quandles and uniquely 2-divisible Bruck loops (see Theorem 3.1). Therefore, one can construct all involutory latin quandles of a given odd order n by constructing all Bruck loops of order n. This observation is of importance for two reasons:

First, while the theory of extensions is not well developed for involutory latin quandles, Glauberman showed [**12**] that any Bruck loop of odd prime power order p^k is centrally nilpotent and hence is a central extension of the p-element group $\mathbb{Z}_p$ by some Bruck loop of order p^{k-1}. Given a Bruck loop F of order p^{k-1}, the vector space of cocycles that yield all central extensions of $\mathbb{Z}_p$ by F as well as the subspace of coboundaries can be calculated by solving a certain system of linear equations over the p-element field, cf. Corollary 5.3

Second, any enumeration of involutory latin quandles or Bruck loops of order p^k will invariably require explicit isomorphism checks, given that the isomorphism problem for central extensions is not solved. Every latin quandle is homogeneous, that is, its automorphism group acts transitively on the underlying set, while Bruck loops are certainly not homogeneous. It is therefore possible in principle and in practice to partition a given Bruck loop into nontrivial blocks that are preserved under isomorphisms, thus greatly aiding in isomorphism searches.

Since Bruck loops are precisely the Bol loops satisfying the automorphic inverse property, results on Bol loops are relevant here. Let p be a prime. Bol loops are power associative and hence all Bol loops of order p are groups. Burn showed [**3**] that all Bol loops of order p^2 are groups as well. However, there exist nonassociative Bruck loops of order p^3. Using central extensions, we construct here all Bruck loops (and hence all involutory latin quandles) of orders 3^k for $k \leq 4$, and also all Bruck loops of order 3^5 that are not central extensions of $\mathbb{Z}_3$ by the elementary abelian group of order 3^4. The results can be found in Theorem 1.1 and Table 3. Computationally speaking, the task is not difficult for $n = 3^k$ with $k \leq 4$, but it takes several months of computing time for $n = 3^5$, and the excluded case of order 3^5 is out of reach because the corresponding vector space of cocycles modulo coboundaries has dimension 24.

All left translations of quandles are automorphisms, and so are all left inner mappings of left Bruck loops. Automorphic loops [**2**], which are loops whose inner mappings are automorphisms, are therefore of interest here. Like Bruck loops, commutative automorphic loops of odd prime power order are centrally nilpotent [**18**]. Moreover, there is a one-to-one correspondence between Bruck loops of odd order and the so-called Γ-loops of odd order [**14**], a class of loops that contains all commutative automorphic loops of odd order.

It was known that there exist Γ-loops of odd order that are not commutative automorphic loops [**14**], but it was not known until now if there exists a Γ-loop of odd prime power order that is not a commutative automorphic loop. By exhaustively inspecting the Bruck loops obtained in our enumeration, we found several Bruck loops of order 3^5 whose corresponding Γ-loops are not commutative automorphic loops. (At the moment we do not understand the abstract reason for the existence of these examples.)

Finite commutative automorphic loops are solvable; see [**19**] for the odd case and [**15**] for the general case. Automorphic loops of odd order are solvable [**22**].

Let p be a prime. Since automorphic loops are power associative [**2**], automorphic loops of order p are groups. Csörgő showed [**4, 22**] that all automorphic loops of order p^2 are groups as well. There exist commutative automorphic loops of order 8 that are not centrally nilpotent. Not all automorphic loops of odd order p^3 are centrally nilpotent and their classification is open [**22**]. Commutative automorphic loops of order p^3 have been first obtained in [**17**] and classified in [**5**]—there are 7 commutative automorphic loops of order p^3, independent of the prime p.

Due to the newly discovered examples, the enumeration of commutative automorphic loops of odd prime power order does not coincide with the enumeration of Bruck loops of odd prime power order. The former enumeration can either be obtained from the latter by constructing all associated Γ-loops and checking whether their inner mappings are automorphisms, or by using central extensions for commutative automorphic loops, cf. Corollary 5.6. We have opted for the second method and enumerated all commutative automorphic loops of orders 3^k for $k \leq 4$, and also all commutative automorphic loops of order 3^5 that are not central extensions of $\mathbb{Z}_3$ by the elementary abelian group of order 3^4. The results can again be found in Theorem 1.1 and Table 3.

THEOREM 1.1. *Up to isomorphism, there are* 7 *left Bruck loops (equivalently, involutory latin quandles) of order* 3^3*,* 72 *of order* 3^4*, and* 118673 *of order* 3^5*, excluding central extensions of* $\mathbb{Z}_3$ *by* $\mathbb{Z}_3^4$*.*

Up to isomorphism, there are 7 *commutative automorphic loops of order* 3^3*,* 72 *of order* 3^4*, and* 118405 *of order* 3^5*, excluding central extensions of* $\mathbb{Z}_3$ *by* $\mathbb{Z}_3^4$*.*

2. Notation and background material

In this section we gather required definitions and background material. The results presented in this section will be used throughout the paper, often without warning.

Let $(Q, \cdot)$ be a groupoid. For every $x \in Q$, let $L_x : Q \to Q$, $y \mapsto x \cdot y$ be the *left translation by* x, and $R_x : Q \to Q$, $y \mapsto y \cdot x$ the *right translation by* x.

A *left quasigroup* is a groupoid in which all left translations are bijections. In a left quasigroup, we let $x\backslash y = L_x^{-1}(y)$ be the left division operation. Similarly, a *right quasigroup* is a groupoid in which all right translations are bijections, and then we denote by $y/x = R_x^{-1}(y)$ the right division operation. A *quasigroup* is a groupoid in which all translations are bijections.

We will often use juxtaposition in place of the multiplication operation and we introduce the following priority rules for expressions involving multiplications and divisions: juxtaposition is more binding than divisions, which are in turn more binding than multiplication. For instance, $x \cdot yz\backslash u$ means $x((yz)\backslash u)$.

A groupoid Q is *left involutory* if $L_x^2 = 1$ for every $x \in Q$. From the condition $L_x^2 = 1$ we deduce that L_x is a bijection and $L_x^{-1} = L_x$. In other words, every left involutory groupoid is a left quasigroup satisfying $xy = x\backslash y$. If Q is a left involutory quasigroup, then $x = (x/y)y = (x/y)\backslash y$, so $y = (x/y)x$ and $y/x = x/y$.

A *loop* is a quasigroup with an identity element, usually denoted by e. In a loop Q, we say that an element $x \in Q$ has a *two-sided inverse* if there is $x^{-1} \in Q$ such that $xx^{-1} = x^{-1}x = e$. A loop with two-sided inverses has the *left inverse property* if $x^{-1}(xy) = y$ holds, and the *automorphic inverse property* if $(xy)^{-1} = x^{-1}y^{-1}$ holds. A quasigroup is *power associative* if every element generates a group, *flexible*

if $x(yx) = (xy)x$ holds, and *left power alternative* if it is power associative and $x^n(x^m y) = x^{n+m}y$ holds for all integers n, m.

A *left Bol loop* is a loop satisfying the left Bol identity

$$x(y(xz)) = (x(yx))z. \tag{2.1}$$

Left Bol loops are power associative and left power alternative (hence have the left inverse property). A *left Bruck loop* is a left Bol loop with the automorphic inverse property.

In a quasigroup Q with inverses, let $P_x = L_{x^{-1}}^{-1} R_x$. A Γ-*loop* is a commutative loop with automorphic inverse property satisfying $L_x L_{x^{-1}} = L_{x^{-1}} L_x$ and $P_x P_y P_x = P_{P_x(y)}$. Every Γ-loop is power associative.

For a loop Q let $\mathrm{Mlt}(Q) = \langle L_x, R_x \,|\, x \in Q \rangle$ be the *multiplication group* of Q, and $\mathrm{Inn}(Q) = \{\varphi \in \mathrm{Mlt}(Q) \,|\, \varphi(e) = e\}$ the *inner mapping group* of Q. It is well-known that $\mathrm{Inn}(Q) = \langle T_x, L_{x,y}, R_{x,y} \,|\, x, y \in Q \rangle$, where

$$T_x = L_x^{-1} R_x,\ L_{x,y} = L_{yx}^{-1} L_y L_x,\ \text{and}\ R_{x,y} = R_{xy}^{-1} R_y R_x.$$

The *center* $Z(Q)$ is the set of all elements $x \in Q$ such that $\varphi(x) = x$ for all $\varphi \in \mathrm{Inn}(Q)$. A loop Q is *centrally nilpotent* if the sequence

$$Q,\ Q/Z(Q),\ (Q/Z(Q))/Z(Q/Z(Q)),\ \ldots$$

terminates at the trivial loop in finitely many steps.

A loop Q is *automorphic* if $\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q)$. Note that a commutative loop Q is automorphic if and only if $L_{x,y} \in \mathrm{Aut}(Q)$ for every x, $y \in Q$.

A groupoid Q is *uniquely 2-divisible* if the squaring map $x \mapsto x^2$ is a bijection of Q. A finite left Bruck loop is uniquely 2-divisible if and only if it is of odd order. If Q is a left Bruck loop in which every element has finite odd order, then $\mathrm{Mlt}(Q)$ is uniquely 2-divisible. (There are examples of infinite uniquely 2-divisible left Bruck loops Q for which $\mathrm{Mlt}(Q)$ is not uniquely 2-divisible.)

Let $(Q_1, \cdot)$, $(Q_2, \circ)$ be groupoids. A triple (α, β, γ) of bijections $Q_1 \to Q_2$ is an *isotopism* from $(Q_1, \cdot)$ onto $(Q_2, \circ)$ if $\alpha(x) \circ \beta(y) = \gamma(x \cdot y)$ for every x, $y \in Q_1$, in which case we say that the two groupoids are *isotopic*. A groupoid isotopic to a quasigroup is itself a quasigroup. If $Q_1 = Q_2$ and the above isotopism of quasigroups has the form $(R_a, L_b, 1)$ for some a, $b \in Q_1$, then $(Q_2, \circ)$ is a loop with identity element $b \cdot a$.

A *quandle*[1] is a left quasigroup that is left distributive (that is, the identity $x(yz) = (xy)(xz)$ holds) and idempotent (that is, the identity $xx = x$ holds). Equivalently, a quandle is an idempotent groupoid Q such that $L_x \in \mathrm{Aut}(Q)$ for every $x \in Q$. A quandle is *latin* if it is a quasigroup. We say that a quandle is *involutory* if it is left involutory. Every quandle is flexible and, being idempotent, uniquely 2-divisible.

The varieties of commutative automorphic loops, left Bruck loops, Γ-loops and quandles will be denoted by **A**, **B**, **Γ**, **Q**, respectively.

3. Two correspondences

The following correspondence is well known and likely first appeared in D.A. Robinson's 1964 dissertation. Kikkawa [**21**] published it in 1973, with uniquely 2-divisible left Bruck loops replaced by "left diassociative loops satisfying $x(y^2 z) =$

[1]It would make a lot of sense to call quandles *left quandles* but traditionally the chirality of the quandle is suppressed in its name.

$(xy)^2(x^{-1}z)$ in which $x \mapsto x^2$ is a bijection." Robinson eventually published it in 1979 [**27**], using the terminology of Bruck loops and right distributive right symmetric quasigroups. The correspondence is also alluded to in the recent survey of Stanovský [**28**]. We give a short but detailed proof that relies only on standard properties of left Bruck loops, summarized in Section 2.

THEOREM 3.1 (Kikkawa, Robinson). *Let Q be a set and let $e \in Q$. There is a one-to-one correspondence between involutory latin quandles defined on Q and uniquely 2-divisible left Bruck loops defined on Q with identity element e. In more detail:*

(i) *If $(Q, \cdot)$ is an involutory latin quandle then*

$$F_{\mathbf{Q}\to\mathbf{B}}(Q,\cdot) = (Q,+) \text{ defined by } x + y = (x/e)(e\backslash y) = (x/e)(ey)$$

is a uniquely 2-divisible left Bruck loop with identity element e. Moreover, in $(Q,+)$ we have $-x = ex$, $2x = x + x = xe$ and $x/2 = x/e$.

(ii) *If $(Q,+)$ is a uniquely 2-divisible left Bruck loop with identity element e then*

$$F_{\mathbf{B}\to\mathbf{Q}}(Q,+) = (Q,\cdot) \text{ defined by } xy = (x + x) - y = 2x - y$$

is an involutory latin quandle.

(iii) *The mappings of* (i) *and* (ii) *are mutual inverses, that is,*

$$F_{\mathbf{Q}\to\mathbf{B}}(F_{\mathbf{B}\to\mathbf{Q}}(Q,+)) = (Q,+)$$

for any uniquely 2-divisible left Bruck loop $(Q,+)$ with identity element e, and

$$F_{\mathbf{B}\to\mathbf{Q}}(F_{\mathbf{Q}\to\mathbf{B}}(Q,\cdot)) = (Q,\cdot)$$

for any involutory latin quandle $(Q,\cdot)$.

PROOF. (i) Let $(Q,\cdot,\backslash,/)$ be an involutory latin quandle and let $(Q,+) = F_{\mathbf{Q}\to\mathbf{B}}(Q,\cdot)$. Then $(R_e, L_e, 1)$ is an isotopism from $(Q,\cdot)$ onto $(Q,+)$ and hence $(Q,+)$ is a loop with identity element $ee = e$. Since $x + ex = (x/e)x = (e/x)x = e$ and $ex + x = e(x/e)e + x = e(x/e) \cdot ex = e(x/e \cdot x) = ee = e$, the two-sided inverse of x in $(Q,+)$ is $-x = ex$. The automorphic inverse property then follows from $-(x+y) = e(x+y) = e(x/e \cdot e\backslash y) = e(x/e) \cdot y = (ex)/e \cdot y = ex + ey = (-x) + (-y)$. For the left Bol identity, we calculate $xe + (ye + (xe + ez)) = x \cdot e(y \cdot e(xz)) = x(ey \cdot xz) = x(ey) \cdot z = (x(ey) \cdot e)/e \cdot z = (x(ey \cdot xe))/e \cdot z = (x \cdot e(y \cdot e(xe)))/e \cdot z = (xe + (ye + xe)) + ez$. Note that $x + x = (x/e)(ex) = (x/e \cdot e)(x/e \cdot x) = xe$. Since R_e is a bijection of Q, we see that $(Q,+)$ is uniquely 2-divisible and $x/2 = x/e$.

(ii) Let $(Q,+)$ be a uniquely 2-divisible left Bruck loop with identity element e and let $(Q,\cdot) = F_{\mathbf{B}\to\mathbf{Q}}(Q,+)$. Then $(x \mapsto 2x,\ x \mapsto -x,\ 1)$ is an isotopism from $(Q,\cdot)$ onto $(Q,+)$ and hence $(Q,\cdot,\backslash,/)$ is a quasigroup. We have $xx = 2x - x = x$ by power-associativity, and $x(xy) = 2x - (2x - y) = 2x + (-2x + y) = y$ by the automorphic inverse and left inverse properties. The desired identity $x(yz) = (xy)(xz)$ is equivalent to $2x - (2y - z) = 2(2x - y) - (2x - z)$ and hence to $2x + (-2y + z) = 2(2x - y) + (-2x + z)$. Substituting x for $2x$, $-y$ for y, and $x + z$ for z yields $x + (2y + (x + z)) = 2(x + y) + z$, which can be rewritten as $(x + (2y + x)) + z = 2(x + y) + z$ by the left Bol identity. We are done by the key identity $x + (2y + x) = 2(x + y)$ for left Bruck loops. (See [**12**, Lemma 1] or note that the identity follows from $2(x+y) - (x+y) = x+y = x+(2y+(x+(-x-y))) = (x + (2y + x)) + (-x - y) = (x + (2y + x)) - (x + y)$ upon canceling $x + y$.)

(iii) Let $(Q,+)$ be a uniquely 2-divisible left Bruck loop with identity element e, $(Q,\cdot,\backslash,/) = F_{\mathbf{B}\to\mathbf{Q}}(Q,+)$ and $(Q,\circ) = F_{\mathbf{Q}\to\mathbf{B}}(Q,\cdot)$. Note that $-y = (e+e)-y = ey$, so $x\circ y = x/e\cdot ey = (x/e+x/e)-ey = (x/e+x/e)+y$. In particular, $x = x\circ e = (x/e+x/e)+e = x/e+x/e$, and we see that $x\circ y = x+y$.

Conversely, let $(Q,\cdot,\backslash,/)$ be an involutory latin quandle, $(Q,+) = F_{\mathbf{Q}\to\mathbf{B}}(Q,\cdot)$ and $(Q,*) = F_{\mathbf{B}\to\mathbf{Q}}(Q,+)$. In (i) we showed $x+x = xe$ and $-x = ex$, hence $x*y = (x+x)-y = xe-y = (xe)/e\cdot e(-y) = xy$. □

Note that the correspondence of Theorem 3.1 is vacuous when $|Q|$ is even.

The following correspondence was proved in [**14**]:

THEOREM 3.2 (Greer). *There is a one-to-one correspondence between left Bruck loops of odd order n and Γ-loops of odd order n. In more detail:*

(i) *If $(Q,+)$ is a left Bruck loop of odd order n with identity element e then*

$$F_{\mathbf{B}\to\mathbf{\Gamma}}(Q,+) = (Q,\cdot) \text{ defined by } x\cdot y = (L_xL_yL_x^{-1}L_y^{-1})^{1/2}L_yL_x(e)$$

is a Γ-loop of order n. Here, $L_x(y) = x+y$.

(ii) *If $(Q,\cdot)$ is a Γ-loop of odd order n then*

$$F_{\mathbf{\Gamma}\to\mathbf{B}}(Q,\cdot) = (Q,+) \text{ defined by } x+y = (x^{-1}\backslash(y^2x))^{1/2}$$

is a left Bruck loop of order n.

(iii) *The mappings of* (i) *and* (ii) *are mutual inverses, that is,*

$$F_{\mathbf{B}\to\mathbf{\Gamma}}(F_{\mathbf{\Gamma}\to\mathbf{B}}(Q,\cdot)) = (Q,\cdot)$$

for any Γ-loop $(Q,\cdot)$ of odd order, and

$$F_{\mathbf{\Gamma}\to\mathbf{B}}(F_{\mathbf{B}\to\mathbf{\Gamma}}(Q,+)) = (Q,+)$$

for any left Bruck loop $(Q,+)$ of odd order.

4. Central extensions of loops

In this section we briefly review the theory of central extensions for loops. Most of the material is well known. We were not able to find Proposition 4.3 in the literature; it is a very simple and very useful observation.

Throughout this section, let $F = (F,\cdot,\backslash,/,1)$ be a loop and $A = (A,+,0)$ an abelian group.

A loop Q is a *central extension* of A by F if there is a subloop $Z\le Z(Q)$ isomorphic to A such that Q/Z is isomorphic to F.

A mapping $\theta : F\times F\to A$ is called a *cocycle*. Given a cocycle θ, define $Q(F,A,\theta)$ on $F\times A$ by

$$(x,a)(y,b) = (xy,\ a+b+\theta(x,y)). \tag{4.1}$$

The resulting groupoid is a quasigroup with $(x,a)\backslash(y,b) = (x\backslash y, b-a-\theta(x,x\backslash y))$ and $(x,a)/(y,b) = (x/y, a-b-\theta(x/y,y))$.

If a cocycle is of the form $\hat\tau(x,y) = \tau(xy)-\tau(x)-\tau(y)$ for some mapping $\tau : F\to A$, then it is called a *coboundary*.

The quasigroup $Q(F,A,\theta)$ is a loop if and only if there is an $a\in A$ such that $\theta(x,1) = \theta(1,x) = -a$ for every $x\in F$, in which case the identity element of $Q(F,A,\theta)$ is $(1,a)$.

PROPOSITION 4.1. *Suppose that A is an abelian group, F a loop, $\theta : F \times F \to A$ a cocycle and $\hat{\tau} : F \times F \to A$ a coboundary. Then $Q(F, A, \theta)$ is isomorphic to $Q(F, A, \theta + \hat{\tau})$.*

PROOF. Consider the bijection $Q(F, A, \theta) \to Q(F, A, \theta + \hat{\tau})$ given by $(x, a) \mapsto (x, a + \tau(x))$. □

In particular, if $Q(F, A, \theta)$ is a loop with identity element $(1, a)$ and $\tau : F \to A$ is any mapping satisfying $\tau(1) = -a$, then $Q(F, A, \theta)$ is isomorphic to the loop $Q(F, A, \theta + \hat{\tau})$ with identity element $(1, 0)$. We can therefore assume without loss of generality that every cocycle $\theta : F \times F \to A$ satisfies

$$\theta(x, 1) = \theta(1, x) = 0 \tag{4.2}$$

for every $x \in F$, in which case we call θ a *loop cocycle*. We note that a coboundary $\hat{\tau} : F \times F \to A$ is a loop cocycle if and only if it satisfies $\tau(1) = 0$, in which case we call it a *loop coboundary*.

Loop cocycles $F \times F \to A$ form a vector space $C(F, A)$ under pointwise addition, and loop coboundaries form a subspace $B(F, A)$ of $C(F, A)$. We have shown that up to isomorphism it suffices to consider representative loop cocycles from the factor space $H(F, A) = C(F, A)/B(F, A)$. In fact, we obtain precisely all central extensions of A by F in this way (see [**24**, Theorem 6] for a proof):

THEOREM 4.2. *Let F be a loop and A an abelian group. Then a loop is a central extension of A by F if and only if it is isomorphic to $Q(F, A, \theta)$ for some $\theta \in H(F, A)$.*

Let $\mathbf{V}$ be a variety of loops. We now address the question when $Q(F, A, \theta)$ belongs to $\mathbf{V}$. A necessary condition for $Q(F, A, \theta) \in \mathbf{V}$ is that both $A \in \mathbf{V}$ and $F \in \mathbf{V}$, since $A \leq Q(F, A, \theta)$ and F is a factor of $Q(F, A, \theta)$.

Assuming that A, $F \in \mathbf{V}$, we call $\theta \in C(F, A)$ a $\mathbf{V}$-*cocycle* if $Q(F, A, \theta) \in \mathbf{V}$. We denote by $C_{\mathbf{V}}(F, A) \leq C(F, A)$ the set of all $\mathbf{V}$-cocycles.

It is usually straightforward to decide which cocycles are $\mathbf{V}$-cocycles. For instance, if $\mathbf{V}$ is the variety of groups then θ is a $\mathbf{V}$-cocycle if and only if the group cocycle identity $\theta(x, y) + \theta(xy, z) = \theta(y, z) + \theta(x, yz)$ holds.

The notion of $\mathbf{V}$-cocycles is well-defined on the factor space $H(F, A)$, i.e., there is no need to verify the $\mathbf{V}$-cocycle condition for loop coboundaries:

PROPOSITION 4.3. *Let $\mathbf{V}$ be a variety of loops, A an abelian group and F a loop such that A, $F \in \mathbf{V}$. Let $\theta \in C(F, A)$ and $\hat{\tau} \in B(F, A)$. Then θ is a $\mathbf{V}$-cocycle if and only if $\theta + \hat{\tau}$ is a $\mathbf{V}$-cocycle.*

PROOF. The loops $\theta(F, A, \theta)$ and $\theta(F, A, \theta + \hat{\tau})$ are isomorphic by Proposition 4.1. □

Finally, the group $\mathrm{Aut}(F) \times \mathrm{Aut}(A)$ acts on $C(F, A)$ by

$$\theta \mapsto \theta^{(\alpha,\beta)}, \quad \theta^{(\alpha,\beta)}(x, y) = \beta^{-1}(\theta(\alpha(x), \alpha(y))).$$

It also acts on $H(F, A)$ since for any coboundary $\hat{\tau}$ we have $\hat{\tau}^{(\alpha,\beta)} = \widehat{\beta^{-1}\tau\alpha}$. Moreover, this action preserves the isomorphism type of the associated loops and hence also the $\mathbf{V}$-cocycle property:

PROPOSITION 4.4. *Let F be a loop, A an abelian group, $\theta \in C(F, A)$ and $(\alpha, \beta) \in \mathrm{Aut}(F) \times \mathrm{Aut}(A)$. Then $Q(F, A, \theta)$ is isomorphic to $Q(F, A, \theta^{(\alpha,\beta)})$.*

PROOF. Consider the bijection $Q(F, A, \theta^{(\alpha,\beta)}) \to Q(F, A, \theta)$ given by $(x, a) \mapsto (\alpha(x), \beta(a))$. □

Altogether, while classifying central extensions of a given abelian group A by a given loop F up to isomorphism, it suffices to consider representatives from the orbits of the group action of $\mathrm{Aut}(F) \times \mathrm{Aut}(A)$ on $H(F, A)$. It is possible for representatives from distinct orbits to yield isomorphic loops—the isomorphism problem of central extensions is delicate.

5. Central extensions of left Bruck loops and commutative automorphic loops

In this section we work out the cocycle conditions for the variety of left Bruck loops and the variety of commutative automorphic loops. We use the same notational conventions as in Section 4.

LEMMA 5.1. *Let F be a loop, A an abelian group and $\theta \in C(F, A)$. Then $Q(F, A, \theta)$ is a left Bol loop if and only if F is a left Bol loop and*

$$\theta(x, z) + \theta(y, xz) + \theta(x, y(xz)) = \theta(y, x) + \theta(x, yx) + \theta(x(yx), z) \tag{5.1}$$

holds for every x, y, $z \in F$.

PROOF. Straightforward computation shows that $(x, a)((y, b) \cdot (x, a)(z, c))$ is equal to

$$(x(y(xz)), 2a + b + c + \theta(x, z) + \theta(y, xz) + \theta(x, y(xz))),$$

while $((x, a) \cdot (y, b)(x, a))(z, c)$ is equal to

$$((x(yx))z, 2a + b + c + \theta(y, x) + \theta(x, yx) + \theta(x(yx), z)).$$

The claim follows. □

LEMMA 5.2. *Let F be a loop, A an abelian group and $\theta \in C(F, A)$. Then:*

(i) *$Q(F, A, \theta)$ has two-sided inverses if and only if F has two-sided inverses and*

$$\theta(x, x^{-1}) = \theta(x^{-1}, x) \tag{5.2}$$

holds for every $x \in F$. Then $(x, a)^{-1} = (x^{-1}, -a - \theta(x, x^{-1}))$.

(ii) *$Q(F, A, \theta)$ has the automorphic inverse property if and only if F has the automorphic inverse property,* (5.2) *holds, and*

$$\theta(x, x^{-1}) + \theta(y, y^{-1}) = \theta(x, y) + \theta(x^{-1}, y^{-1}) + \theta(xy, (xy)^{-1}) \tag{5.3}$$

holds for every x, $y \in F$.

PROOF. (i) The element (x, a) has a two-sided inverse (y, b) if and only if $(1, 0) = (x, a)(y, b) = (xy, a+b+\theta(x, y))$ and at the same time $(1, 0) = (y, b)(x, a) = (yx, a + b + \theta(y, x))$, that is, if and only if $y = x^{-1}$, $\theta(x, x^{-1}) = \theta(x^{-1}, x)$ and $b = -a - \theta(x, x^{-1})$. In that case, $(x, a)^{-1} = (x^{-1}, -a - \theta(x, x^{-1}))$.

(ii) Suppose that $Q(F, A, \theta)$ has two-sided inverses. Then

$$\begin{aligned}(x, a)^{-1}(y, b)^{-1} &= (x^{-1}, -a - \theta(x, x^{-1}))(y^{-1}, -b - \theta(y, y^{-1})) \\ &= (x^{-1}y^{-1}, -a - b - \theta(x, x^{-1}) - \theta(y, y^{-1}) + \theta(x^{-1}, y^{-1})),\end{aligned}$$

while

$$\begin{aligned}((x,a)(y,b))^{-1} &= (xy, a+b+\theta(x,y))^{-1}\\ &= ((xy)^{-1}, -a-b-\theta(x,y)-\theta(xy,(xy)^{-1})).\end{aligned}$$

The claim follows. □

Corollary 5.3. *Let F be a loop, A an abelian group and $\theta \in C(F,A)$. Then $Q(F,A,\theta)$ is a left Bruck loop if and only if F is a left Bruck loop and the identities* (5.1) *and* (5.3) *hold.*

Proof. By definition, a loop is left Bruck if and only if it is left Bol and satisfies the automorphic inverse property. By Lemmas 5.1 and 5.2, $Q(F,A,\theta)$ is left Bruck if and only if F is left Bruck and (5.1), (5.2), (5.3) hold. Since every left Bol loop has two-sided inverses, the identity (5.2) follows from (5.1) and can be omitted. □

Call a loop Q *left automorphic* if $L_{x,y} \in \mathrm{Aut}(Q)$ for every x, $y \in Q$. As we have already noted in the introduction, a commutative loop is automorphic if and only if it is left automorphic. We obviously have:

Lemma 5.4. *Let F be a loop, A an abelian group and $\theta \in C(F,A)$. Then $Q(F,A,\theta)$ is commutative if and only if F is commutative and*

$$\theta(x,y) = \theta(y,x) \tag{5.4}$$

holds for every x, $y \in F$.

Lemma 5.5. *Let F be a loop, A an abelian group and $\theta \in C(F,A)$. Then $Q(F,A,\theta)$ is a left automorphic loop if and only if F is a left automorphic loop and*

(5.5)
$$\begin{aligned}&\theta(x,z)+\theta(x,u)+\theta(y,xz)+\theta(y,xu)+\theta(yx,L_{x,y}(zu))+\theta(L_{x,y}(z),L_{x,y}(u))\\ &\quad=\theta(z,u)+\theta(y,x)+\theta(x,zu)+\theta(y,x(zu))+\theta(yx,L_{x,y}(z))+\theta(yx,L_{x,y}(u))\end{aligned}$$

holds for every x, y, z, $u \in F$.

Proof. Recall that $L^{-1}_{(x,a)}(y,b) = (x,a)\backslash(y,b) = (x\backslash y, b-a-\theta(x,x\backslash y))$ and thus

$$\begin{aligned}L_{(x,a),(y,b)}(z,c) &= L^{-1}_{(y,b)(x,a)}L_{(y,b)}L_{(x,a)}(z,c)\\ &= L^{-1}_{(yx,a+b+\theta(y,x))}L_{(y,b)}(xz,a+c+\theta(x,z))\\ &= L^{-1}_{(yx,a+b+\theta(y,x))}(y(xz),a+b+c+\theta(x,z)+\theta(y,xz))\\ &= (L_{x,y}(z),c+\theta(x,z)+\theta(y,xz)-\theta(y,x)-\theta(yx,L_{x,y}(z))).\end{aligned}$$

Then $L_{(x,a),(y,b)}(z,c)L_{(x,a),(y,b)}(u,d)$ is equal to $(L_{x,y}(z)L_{x,y}(u),r)$, where r is equal to

$$\begin{aligned}&c+d+\theta(x,z)+\theta(y,xz)-\theta(y,x)-\theta(yx,L_{x,y}(z))\\ &\qquad+\theta(x,u)+\theta(y,xu)-\theta(y,x)-\theta(yx,L_{x,y}(u))+\theta(L_{x,y}(z),L_{x,y}(u)),\end{aligned}$$

while $L_{(x,a),(y,b)}((z,c)(u,d)) = L_{(x,a),(y,b)}(zu, c+d+\theta(z,u))$ is equal to $(L_{x,y}(zu),s)$, where s is equal to

$$c+d+\theta(z,u)+\theta(x,zu)+\theta(y,x(zu))-\theta(y,x)-\theta(yx,L_{x,y}(zu)).$$

The claim follows. □

COROLLARY 5.6. *Let F be a loop, A an abelian group and $\theta \in C(F, A)$. Then $Q(F, A, \theta)$ is a commutative automorphic loop if and only if F is a commutative automorphic loop and* (5.4), (5.5) *hold.*

6. The algorithm

Our approach to enumeration is similar to that of [**24**]. The following algorithm has been implemented in `GAP` [**11**] using the package `LOOPS` [**25**].

Let p be an odd prime and $A = \mathbb{Z}_p$ the cyclic group of order p.

6.1. Central extensions of A by a given factor F. Let F be a loop of order p^k. The vector space $B(F, A)$ of loop coboundaries can be constructed as the linear span over the p-element field $GF(p)$ of the set $\{\widehat{\tau_c} \,|\, 1 \neq c \in F\}$, where $\tau_c : F \to A$ is given by

$$\tau_c(x) = \begin{cases} 1, & \text{if } x = c, \\ 0, & \text{otherwise.} \end{cases}$$

Let now F be a left Bruck loop of order p^k. Consider the $|F|^2 = p^{2k}$ variables $\theta(x, y)$ indexed by x, $y \in F$. By Corollary 5.3, the vector space $C_{\mathbf{B}}(F, A)$ consists of the solutions to the homogeneous system of $2|F| + |F|^2 + |F|^3 = 2p^k + p^{2k} + p^{3k}$ linear equations

$$\begin{aligned} \theta(x, 1) &= 0, && x \in F, \\ \theta(1, x) &= 0, && x \in F, \\ \theta(x, x^{-1}) + \theta(y, y^{-1}) &= \theta(x, y) + \theta(x^{-1}, y^{-1}) + \theta(xy, (xy)^{-1}), && x, y \in F, \\ \theta(x, z) + \theta(y, xz) + \theta(x, y(xz)) &= \theta(y, x) + \theta(x, yx) + \theta(x(yx), z), && x, y, z \in F, \end{aligned}$$

over $GF(p)$. The linear equations forming this system correspond to the identities (4.2), (5.1) and (5.3).

When $|F|$ is large enough (say $|F| = 3^4$), the linear system must be periodically reduced while it is being set up so as to fit into memory.

For $p = 3$ and $k \leq 5$, the dimensions of the vector spaces $C_{\mathbf{B}}(F, A)$ and $B(F, A)$ are recorded in Tables 1 and 2.

The action of $\mathrm{Aut}(F) \times \mathrm{Aut}(A)$ on $H_{\mathbf{B}}(F, A) = C_{\mathbf{B}}(F, A)/B(F, A)$ can be implemented in a straightforward fashion. We were not able to calculate the orbits for the case $F = \mathbb{Z}_3^4$, since $|H_{\mathbf{B}}(\mathbb{Z}_3^4, \mathbb{Z}_3)| = 3^{24}$.

The set

$$\mathcal{Q}_{\mathbf{B}}(F, A) = \{Q(F, A, \theta) \,|\, \theta \in H_{\mathbf{B}}(F, A) \text{ modulo the action of } \mathrm{Aut}(F) \times \mathrm{Aut}(A)\}$$

contains all left Bruck loops of order p^{k+1} that are central extensions of A by F, up to isomorphism. But it can contain duplicate isomorphism types and we must therefore filter $\mathcal{Q}_{\mathbf{B}}(F, A)$ up to isomorphism, resulting in a smaller set $\mathcal{Q}^*_{\mathbf{B}}(F, A)$.

Calculating $\mathcal{Q}^*_{\mathbf{B}}(F, A)$ is a nontrivial task. For instance, there exists a left Bruck loop F of order 3^4 such that $|\mathcal{Q}_{\mathbf{B}}(F, A)| = 29525$, so, in the worst case, filtering $\mathcal{Q}_{\mathbf{B}}(F, A)$ up to isomorphism will require $\binom{29525}{2} = 435848050$ isomorphism checks among loops of order 243, which is intractable. (It turns out that $|\mathcal{Q}^*_{\mathbf{B}}(F, A)| = 26865$ here, so the above upper bound is not far from the actual number of isomorphism checks required.)

However, by precalculating certain isomorphism invariants, the set $\mathcal{Q}_{\mathbf{B}}(F, A)$ can be pre-partitioned without any isomorphism checks. In more detail, consider

$Q \in \mathcal{Q}_{\mathbf{B}}(F, A)$. For every $x \in Q$ we have precalculated the numerical invariant $I_x = (I_{x,1}, \dots, I_{x,6})$, where

$$\begin{aligned}
I_{x,1} &= \text{ the cycle structure of } L_x,\\
I_{x,2} &= |x|,\\
I_{x,3} &= (|\{y \in Q \mid y^2 = x\}|, |\{y \in Q \mid y^3 = x\}|, |\{y \in Q \mid y^4 = x\}|),\\
I_{x,4,a} &= |\{y \in Q \mid x(xy) = (xx)y \text{ and } |y| = a\}|,\\
I_{x,5,a,b} &= |\{(y,z) \in Q \times Q \mid y(zx) = (yz)x \text{ and } |y| = a,\ |z| = b\}|,\\
I_{x,6,a} &= |\{y \in Q \mid xy = yx \text{ and } |y| = a\}|.
\end{aligned}$$

(These invariants are not necessarily independent and we have used proper subsets of the invariants in certain situations.) Let $I(Q)$ be the lexicographically ordered multiset $\{I_x \mid x \in Q\}$. The equivalence relation $\sim$ on $\mathcal{Q}_{\mathbf{B}}(F, A)$ defined by $Q_1 \sim Q_2$ if and only if $I(Q_1) = I(Q_2)$ induces a partition of $\mathcal{Q}_{\mathbf{B}}(F, A)$, and isomorphism checks need to be performed only within each part of the partition. Moreover, given $Q \in \mathcal{Q}_B(F, A)$, the equivalence relation $\approx$ on Q defined by $x \approx y$ if and only if $I_x = I_y$ induces a partition of Q that must be preserved by any isomorphism from Q to another loop.

Using these invariants, the number of required isomorphism checks in the above example was reduced from 435848050 to 52475, which took a few days to perform.

When F is a commutative automorphic loop of order p^k, we proceed analogously. The vector space $C_{\mathbf{A}}(F, A)$ consists of the solutions to the homogeneous system of $2|F| + |F|^2 + |F|^4 = 2p^k + p^{2k} + p^{4k}$ linear equations corresponding to the identities (4.2), (5.4) and (5.5).

6.2. Central extensions of A by all factors of order p^k. Let $F_1, \dots, F_m$ be a complete collection of left Bruck loops of order p^k up to isomorphism. Then $\bigcup_{i=1}^{m} \mathcal{Q}^*_{\mathbf{B}}(F_i, A)$ contains all left Bruck loops of order p^{k+1} up to isomorphism, but the union is not necessarily disjoint. To wit, when a constructed loop Q of order p^{k+1} possesses a center of order bigger than p, it might also posses two central subloops Z_1, Z_2 such that Q/Z_1, Q/Z_2 are not isomorphic.

Fortunately, it is not necessary to perform any additional isomorphism checks among loops of order p^{k+1}. Instead, suppose that we would like to decide if a loop $Q \in \mathcal{Q}^*_{\mathbf{B}}(F_i, A)$ of order p^{k+1} has been seen before. We calculate the center $Z(Q)$ of Q. If $|Z(Q)| = p$ then Q can only be obtained as an extension of $Z(Q) \cong \mathbb{Z}_p$ by $Q/Z(Q) \cong F_i$, and we keep Q. Otherwise, we calculate all central subloops Z_1, $\dots$, Z_ℓ of $Z(Q)$ of order p, and we calculate the factors Q/Z_j for $1 \le j \le \ell$. If, for some $1 \le j \le \ell$, Q/Z_j is isomorphic to F_t with $t < i$, we discard Q since it has already been seen in $\mathcal{Q}^*_{\mathbf{B}}(F_t, A)$; otherwise we keep Q.

Although this algorithm avoids isomorphism checks among loops of order p^{k+1}, it requires a large number of isomorphism checks among loops of order p^k to identity the factor loops Q/Z_j. It took several days of computing time to perform this step of the algorithm for left Bruck loops of order 3^5.

Altogether, the enumeration of left Bruck loops of order 3^k with $k \le 5$ took several months of computing time.

Similarly for commutative automorphic loops.

7. Results

Our results are summarized in Tables 1, 2 and 3. We recall that involutory latin quandles are in one-to-one correspondence with uniquely 2-divisible left Bruck loops (cf. Theorem 3.1).

factor	B	$C_{\mathbf{B}}$	$n_{\mathbf{B}}$	comment
3/1	1	2	2	$\mathbb{Z}_3$
9/1	6	10	6	$\mathbb{Z}_3^2$
9/2	7	8	2	$\mathbb{Z}_9$
27/1	23	34	47	$\mathbb{Z}_3^3$
27/2	24	28	11	$\mathbb{Z}_3 \times \mathbb{Z}_9$
27/3	24	27	10	14 elements of order 3
27/4	24	28	13	20 elements of order 3
27/5	24	27	6	2 elements of order 3
27/6	24	27	10	8 elements of order 3
27/7	25	26	2	$\mathbb{Z}_{27}$

TABLE 1. The number $n_{\mathbf{B}}$ of left Bruck loops of order 3^{k+1} that are central extensions of $\mathbb{Z}_3$ by a given factor of order 3^k, up to isomorphism.

Table 1 lists all left Bruck loops F of order 3, 9 and 27. For each such loop F of order 3^k we give the dimension B of the vector space of coboundaries $B(F, \mathbb{Z}_3)$, the dimension $C_{\mathbf{B}}$ of the vector space $C_{\mathbf{B}}(F, \mathbb{Z}_3)$ of left Bruck loop cocycles, and the number $n_{\mathbf{B}}$ of left Bruck loops of order 3^{k+1} up to isomorphism that are central extensions of $\mathbb{Z}_3$ by F. The last column of Table 1 contains structural information that uniquely identifies F, either as an abelian group or as a nonassociative left Bruck loop with a given number of elements of order 3.

As an outcome of this classification, we have observed that given a left Bruck loop of order $3^k \leq 81$, the associated Γ-loop (cf. Theorem 3.2) is always a commutative automorphic loop.

Table 2 is similar to Table 1 but for left Bruck loops of order 81 used as factors. We were not able to complete the enumeration for the elementary abelian group of order 81 (the loop 81/1). There appear to be no compact invariants that could distinguish the 72 left Bruck loops of order 81, and we therefore do not give any structural information about the factors.

Unlike for orders $3^k \leq 3^4$, there exists a left Bruck loop of order 3^5 whose associated Γ-loop is not a commutative automorphic loop. (A multiplication table of this loop can be downloaded from the homepage of the second author.) We therefore report in Table 2 also data for commutative automorphic loops. Given a left Bruck loop F of order 3^4, let G be the associated commutative automorphic loop. In the row corresponding to F, we give the dimension $C_{\mathbf{A}}$ of the vector space $C_{\mathbf{A}}(G, \mathbb{Z}_3)$ of commutative automorphic loop cocycles, and the number $n_{\mathbf{A}}$ of commutative automorphic loops up to isomorphism that are central extensions of $\mathbb{Z}_3$ by G.

Note that for most but not all factors we have $C_{\mathbf{B}} = C_{\mathbf{A}}$ and $n_{\mathbf{B}} = n_{\mathbf{A}}$. The first difference occurs in the row indexed by the factor 81/46.

factor	B	$C_{\mathbf{B}}$	$n_{\mathbf{B}}$	$C_{\mathbf{A}}$	$n_{\mathbf{A}}$	factor	B	$C_{\mathbf{B}}$	$n_{\mathbf{B}}$	$C_{\mathbf{A}}$	$n_{\mathbf{A}}$
81/1	76	100	?	100	?	81/37	77	87	4940	87	4940
81/2	77	88	162	88	162	81/38	77	87	5018	87	5018
81/3	77	87	994	87	994	81/39	77	87	9584	87	9584
81/4	77	88	634	88	634	81/40	77	87	26882	87	26882
81/5	77	87	633	87	633	81/41	77	87	26865	87	26865
81/6	77	87	979	87	979	81/42	77	87	9582	87	9582
81/7	77	87	3865	87	3865	81/43	77	87	9584	87	9584
81/8	77	87	7438	87	7438	81/44	77	87	1169	87	1169
81/9	77	87	26913	87	26913	81/45	77	87	2261	87	2261
81/10	77	87	14313	87	14313	81/46	77	90	260	87	26
81/11	77	87	14231	87	14231	81/47	77	87	189	87	189
81/12	77	87	14226	87	14226	81/48	78	82	11	82	11
81/13	77	87	9630	87	9630	81/49	78	83	17	82	13
81/14	77	87	26902	87	26902	81/50	78	81	8	81	8
81/15	77	87	9584	87	9584	81/51	78	82	6	82	6
81/16	77	87	26904	87	26904	81/52	78	82	13	82	13
81/17	77	87	7332	87	7332	81/53	78	82	7	82	7
81/18	77	87	26903	87	26903	81/54	78	82	16	82	16
81/19	77	87	9624	87	9624	81/55	78	81	10	81	10
81/20	77	87	26846	87	26846	81/56	78	81	10	81	10
81/21	77	87	3708	87	3708	81/57	78	81	8	81	8
81/22	77	87	9630	87	9630	81/58	78	84	36	82	15
81/23	77	87	660	87	660	81/59	78	82	12	81	10
81/24	77	87	9637	87	9637	81/60	78	82	8	80	4
81/25	77	87	1759	87	1759	81/61	78	80	3	80	3
81/26	77	87	1759	87	1759	81/62	78	80	4	80	4
81/27	77	87	14228	87	14228	81/63	78	81	10	81	10
81/28	77	87	4940	87	4940	81/64	78	82	13	82	13
81/29	77	87	4986	87	4986	81/65	78	81	6	81	6
81/30	77	87	14227	87	14227	81/66	78	81	10	81	10
81/31	77	87	3822	87	3822	81/67	78	82	11	81	9
81/32	77	87	14226	87	14226	81/68	78	81	13	81	13
81/33	77	87	14239	87	14239	81/69	78	81	13	81	13
81/34	77	87	4938	87	4938	81/70	78	81	13	81	13
81/35	77	87	14218	87	14218	81/71	78	82	3	80	2
81/36	77	87	1928	87	1928	81/72	79	80	2	80	2

TABLE 2. The number of left Bruck loops ($n_{\mathbf{B}}$) and commutative automorphic loops ($n_{\mathbf{A}}$) of order 3^5 that are central extensions of $\mathbb{Z}_3$ by a given factor of order 3^4, up to isomorphism.

Finally, Table 3 gives the number $n_{\mathbf{B}}$ of left Bruck loops and the number $n_{\mathbf{A}}$ of commutative automorphic loops of order n up to isomorphism. For $n = 243$, we only give the number of left Bruck loops (resp. commutative automorphic loops) that are *not* central extensions of $\mathbb{Z}_3$ by the elementary abelian group $\mathbb{Z}_3^4$.

n	3	9	27	81	243*
$n_{\mathbf{B}}$	1	2	7	72	118673*
$n_{\mathbf{A}}$	1	2	7	72	118405*

TABLE 3. The number of left Bruck loops ($n_{\mathbf{B}}$) and commutative automorphic loops ($n_{\mathbf{A}}$) of orders 3, 9, 27, 81, 243, up to isomorphism, excluding central extensions of $\mathbb{Z}_3$ by $\mathbb{Z}_3^4$.

It turns out that for each factor $F = 81/i$ with $2 \leq i \leq 47$ there is precisely one left Bruck loop up to isomorphism that is a central extension of $\mathbb{Z}_3$ by $\mathbb{Z}_3^4$ (namely the direct product $\mathbb{Z}_3 \times F$). The resulting 46 left Bruck loops are pairwise non-isomorphic and they are *not* included in the count of Table 3. For the factors $F = 81/i$ with $48 \leq i \leq 72$, no central extension of $\mathbb{Z}_3$ by F is also a central extension of $\mathbb{Z}_3$ by $\mathbb{Z}_3^4$. The situation is completely analogous for commutative automorphic loops.

Therefore, if $N_{\mathbf{B}}$ (resp. $N_{\mathbf{A}}$) is the number of left Bruck loops (resp. commutative automorphic loops) of order 243 up to isomorphism that are central extensions of $\mathbb{Z}_3$ by $\mathbb{Z}_3^4$, then the number of left Bruck loops (resp. commutative automorphic loops) of order 243 up to isomorphism is $N_{\mathbf{B}} + 118673$ (resp. $N_{\mathbf{A}} + 118405$).

8. Open problems

Let p be an odd prime. In [**14**], Greer asked if the Γ-loops associated with left Bruck loops of order p^3 are always commutative automorphic loops. We can generalize his question as follows:

PROBLEM 8.1. For which odd primes p and positive integers k is there a one-to-one correspondence between left Bruck loops of order p^k and commutative automorphic loops of order p^k?

By the results mentioned in the introduction, the answer is positive when $k \leq 2$. Our results imply that the answer is positive for $p^k \in \{3^3, 3^4\}$ and negative for $p^k = 3^5$. We have also verified that the answer is positive for $p^k \in \{5^3, 7^3, 11^3\}$, the case 11^3 taking several days of computing time to complete.

PROBLEM 8.2. Let p be an odd prime and k a positive integer. Is there an abstract description of left Bruck loops of order p^k for which all associated Γ-loops are commutative automorphic loops?

Acknowledgment

We thank David Stanovský for bringing the correspondence between involutory latin quandles and uniquely 2-divisible left Bruck loops to our attention. We also thank an anonymous referee for several comments that improved the manuscript. The calculations took place on the high performance computing cluster of the University of Denver—we thank Benjamin Fotovich for providing assistance with the computing cluster.

References

1. Richard Hubert Bruck, *A survey of binary systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Heft **20**, Springer Verlag, Berlin-Göttingen-Heidelberg 1958.

2. R.H. Bruck and Lowell J. Paige, *Loops whose inner mappings are automorphisms*, Ann. of Math. (**2**) **63** (1956), 308–323.
3. R.P. Burn, *Finite Bol loops*, Math. Proc. Cambridge Philos. Soc. **84** (1978), no. **3**, 377–385.
4. Piroska Csörgő, *All automorphic loops of order p^2 for some prime p are associative*, J. Algebra Appl. **12** (2013), no. **6**, 1350013, 8 pp.
5. Dylene Agda Souza De Barros, Alexander Grishkov and Petr Vojtěchovský, *Commutative automorphic loops of order p^3*, J. Algebra Appl. **11** (2012), no. **5**, 1250100, 15 pp.
6. V.G. Drinfeld, *On some unsolved problems in quantum group theory*, Quantum groups (Leningrad, 1990), 1–8, Lecture Notes in Math. **1510**, Springer, Berlin, 1992.
7. Mohamed Elhamdadi and Sam Nelson, *Quandles-an introduction to the algebra of knots*, Student Mathematical Library **74**, American Mathematical Society, Providence, RI, 2015.
8. Michael Eisermann, *Yang-Baxter deformations of quandles and racks*, Algebr. Geom. Topol. **5** (2005), 537–562.
9. David Joyce, *A classifying invariant of knots, the knot quandle*, J. Pure Appl. Algebra **23** (1982), no. **1**, 37–65.
10. V.M. Galkin, *Left distributive finite order quasigroups* (Russian), Quasigroups and loops. Mat. Issled. No. **51** (1979), 43–54, 163.
11. The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.8.8*; 2017, `(https://www.gap-system.org)`.
12. George Glauberman, *On loops of odd order*, J. Algebra **1** (1964), 374–396.
13. George Glauberman, *On loops of odd order II*, J. Algebra **8** (1968), 393–414.
14. Mark Greer, *A class of loops categorically isomorphic to Bruck loops of odd order*, Comm. Algebra **42** (2014), no. **8**, 3682–3697.
15. Alexander Grishkov, Michael Kinyon and Gábor P. Nagy, *Solvability of commutative automorphic loops*, Proc. Amer. Math. Soc. **142** (2014), no. **9**, 3029–3037.
16. Alexander Hulpke, David Stanovský and Petr Vojtěchovský, *Connected quandles and transitive groups*, J. Pure Appl. Algebra **220** (2016), no. **2**, 735–758.
17. Přemysl Jedlička, Michael Kinyon and Petr Vojtěchovský, *Constructions of commutative automorphic loops*, Comm. Algebra **38** (2010), no. **9**, 3243–3267.
18. Přemysl Jedlička, Michael Kinyon and Petr Vojtěchovský, *Nilpotency in automorphic loops of prime power order*, J. Algebra **350** (2012), 64–76.
19. Přemysl Jedlička, Michael Kinyon and Petr Vojtěchovský, *The structure of commutative automorphic loops*, Trans. Amer. Math. Soc. **363** (2011), no. **1**, 365–384.
20. Hubert Kiechle, *Theory of K-loops*, Lecture Notes in Mathematics **1778**, Springer-Verlag, Berlin, 2002.
21. Michihiko Kikkawa, *On some quasigroups of algebraic models of symmetric spaces*, Mem. Fac. Lit. Sci. Shimane Univ. Natur. Sci. No. **6** (1973), 9–13.
22. Michael Kinyon, Kenneth Kunen, J.D. Phillips and Petr Vojtěchovský, *The structure of automorphic loops*, Trans. Amer. Math. Soc. **368** (2016), no. **12**, 8901–8927.
23. S.V. Matveev, *Distributive groupoids in knot theory* (Russian), Mat. Sb. (N.S.) **119**(**161**) (1982), no. **1**, 78–88.
24. Gábor P. Nagy and Petr Vojtěchovský, *The Moufang loops of order* 64 *and* 81, J. Symbolic Comput. **42** (2007), no. **9**, 871–883.
25. Gábor P. Nagy and Petr Vojtěchovský, *LOOPS: Computing with quasigroups and loops in GAP*, available at `http://www.math.du.edu/~petr/loops`
26. Hala O. Pflugfelder, *Quasigroups and loops: introduction*, Sigma Series in Pure Mathematics **7**, Heldermann Verlag, Berlin, 1990.
27. D.A. Robinson, *A loop-theoretic study of right-sided quasigroups*, Ann. Soc. Sci. Bruxelles Sr. I **93** (1979), no. **1**, 7–16.
28. David Stanovský, *A guide to self-distributive quasigroups, or latin quandles*, Quasigroups and Related Systems **23** (2015), no. **1**, 91–128.
29. Abraham A. Ungar, *Beyond the Einstein addition law and its gyroscopic Thomas precession. The theory of gyrogroups and gyrovector spaces.*, Fundamental Theories of Physics **117**, Kluwer Academic Publishers Group, Dordrecht, 2001.

Department of Mathematics, Penn State University, 54 McAllister Street, University Park, State College, PA 16801, U.S.A.
E-mail address: ius68@psu.edu

Department of Mathematics, University of Denver, 2390 S York Street, Denver, Colorado 80208, U.S.A.
E-mail address: petr@math.du.edu