Connected Quandles Associated with Pointed Abelian Groups

W. Edwin Clark, Mohamed Elhamdadi, Xiang-dong Hou,
Masahico Saito, Timothy Yeatman

Department of Mathematics and Statistics
University of South Florida

Abstract

A quandle is a self-distributive algebraic structure that appears in quasi-group and knot theories. For each abelian group A and $c \in A$ we define a quandle $G(A, c)$ on $\mathbb{Z}_3 \times A$. These quandles are generalizations of a class of non-medial Latin quandles defined by V. M. Galkin so we call them *Galkin quandles*. Each $G(A, c)$ is connected but not Latin unless A has odd order. $G(A, c)$ is non-medial unless $3A = 0$. We classify their isomorphism classes in terms of pointed abelian groups, and study their various properties. A family of symmetric connected quandles is constructed from Galkin quandles, and some aspects of knot colorings by Galkin quandles are also discussed.

1 Introduction

Sets with certain self-distributive operations called *quandles* have been studied since 1940s (for example, [28]) in various areas with different names. They have been studied, for example, as an algebraic system for symmetries and as quasi-groups. The *fundamental quandle* was defined in a manner similar to the fundamental group [14, 20], which made quandles an important tool in knot theory. Algebraic homology theories for quandles have been developed [3, 9], extensions of quandles by cocycles have been studied [1, 2], and applied to various properties of knots and knotted surfaces ([4], for example).

Before algebraic theories of extensions were developed, Galkin [11] defined a family of quandles that are extensions of the 3-element connected quandle R_3, and we call them *Galkin quandles*. Even though the definition of Galkin quandles is a special case of a cocycle extension described in [1], they have curious properties such as the explicit and simple defining formula, close connections to dihedral quandles, and the fact that they appear in the list of small connected quandles.

In this paper, we generalize Galkin's definition and define a family of quandles that are extensions of R_3, characterize their isomorphism classes, and study their properties. The definition is given in Section 3 after a brief review of necessary materials in Section 2. Isomorphism classes are characterized by pointed abelian groups in Section 4. Various algebraic properties of Galkin quandles are investigated in Section 5, and their knot colorings are studied in Section 6.

Acknowledgement: Special thanks to Michael Kinyon for bringing Galkin's paper [11] to our attention and pointing out the construction of non-medial, Latin quandles on page 950 of [11] that we call here Galkin quandles $G(\mathbb{Z}_p, c_1, c_2)$. We are also grateful to Professor Kinyon for helping us with using Mace4 for colorings of knots by quandles, and for telling us about Belousov's work on distributive quasigroups. Thanks to David Stanovsky for useful discussions on these matters. We are grateful to James McCarron for his help with the Magma package in *Maple 15* especially with isomorphism testing. M.S. was supported in part by NSF grant DMS #0900671.

2 Preliminaries

In this section we briefly review some definitions and examples of quandles. More details can be found, for example, in [1, 4, 9].

A *quandle* X is a non-empty set with a binary operation $(a, b) \mapsto a * b$ satisfying the following conditions.

$$\text{(Idempotency)} \qquad \text{For any } a \in X,\ a * a = a. \tag{1}$$

$$\text{(Invertibility)} \qquad \text{For any } b, c \in X, \text{ there is a unique } a \in X \text{ such that } a * b = c. \tag{2}$$

$$\text{(Right self-distributivity)} \qquad \text{For any } a, b, c \in X, \text{ we have } (a * b) * c = (a * c) * (b * c). \tag{3}$$

A *quandle homomorphism* between two quandles X, Y is a map $f : X \to Y$ such that $f(x *_X y) = f(x) *_Y f(y)$, where $*_X$ and $*_Y$ denote the quandle operations of X and Y, respectively. A *quandle isomorphism* is a bijective quandle homomorphism, and two quandles are *isomorphic* if there is a quandle isomorphism between them.

Typical examples of quandles include the following.

- Any non-empty set X with the operation $x * y = x$ for any $x, y \in X$ is a quandle called the *trivial* quandle.
- A group $X = G$ with n-fold conjugation as the quandle operation: $a * b = b^{-n} a b^n$.
- Let n be a positive integer. For $a, b \in \mathbb{Z}_n$ (integers modulo n), define $a * b \equiv 2b - a \pmod{n}$. Then $*$ defines a quandle structure called the *dihedral quandle*, R_n. This set can be identified with the set of reflections of a regular n-gon with conjugation as the quandle operation.
- Any $\mathbb{Z}[T, T^{-1}]$-module M is a quandle with $a*b = Ta+(1-T)b$, $a, b \in M$, called an *Alexander quandle*. An Alexander quandle is also regarded as a pair (M, T) where M is an abelian group and $T \in \mathrm{Aut}(M)$.

Let X be a quandle. The *right translation* $\mathcal{R}_a : X \to X$, by $a \in X$, is defined by $\mathcal{R}_a(x) = x * a$ for $x \in X$. Similarly the *left translation* $\mathcal{L}_a$ is defined by $\mathcal{L}_a(x) = a*x$. Then $\mathcal{R}_a$ is a permutation of X by Axiom (2). The subgroup of $\mathrm{Sym}(X)$ generated by the permutations $\mathcal{R}_a$, $a \in X$, is called the *inner automorphism group* of X, and is denoted by $\mathrm{Inn}(X)$. We list some definitions of commonly known properties of quandles below.

- A quandle is *connected* if $\mathrm{Inn}(X)$ acts transitively on X.
- A *Latin quandle* is a quandle such that for each $a \in X$, the left translation $\mathcal{L}_a$ is a bijection. That is, the multiplication table of the quandle is a Latin square.
- A quandle is *faithful* if the mapping $a \mapsto \mathcal{R}_a$ is an injection from X to $\mathrm{Inn}(X)$.
- A quandle X is *involutory*, or a *kei*, if the right translations are involutions: $\mathcal{R}_a^2 = \mathrm{id}$ for all $a \in X$.

- It is seen that the operation $\bar{*}$ on X defined by $a \mathbin{\bar{*}} b = \mathcal{R}_b^{-1}(a)$ is a quandle operation, and $(X, \bar{*})$ is called the *dual* quandle of $(X, *)$. If $(X, \bar{*})$ is isomorphic to $(X, *)$, then $(X, *)$ is called *self-dual*.
- A quandle X is *medial* if $(a * b) * (c * d) = (a * c) * (b * d)$ for all $a, b, c, d \in X$. It is also called *abelian*. It is known and easily seen that every Alexander quandle is medial.

A *coloring* of an oriented knot diagram by a quandle X is a map $\mathcal{C} : \mathcal{A} \to X$ from the set of arcs $\mathcal{A}$ of the diagram to X such that the image of the map satisfies the relation depicted in Figure 1 at each crossing. More details can be found in [4], for example. A coloring that assigns the same element of X for all the arcs is called trivial, otherwise non-trivial. The number of colorings of a knot diagram by a finite quandle is known to be independent of the choice of a diagram, and hence is a knot invariant. A coloring by a dihedral quandle R_n for a positive integer $n > 1$ is called an n-coloring. If a knot is non-trivially colored by a dihedral quandle R_n for a positive integer $n > 1$, then it is called *n-colorable*. In Figure 2, a non-trivial 3-coloring of the trefoil knot (3_1 in a common notation in a knot table [6]) is indicated. This is presented in a closed braid form. Each crossing corresponds to a standard generator σ_1 of the 2-strand braid group, and σ_1^3 represents three crossings together as in the figure. The dotted line indicates the closure, see [27] for more details of braids.

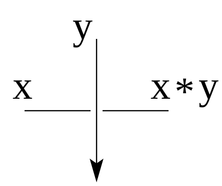

Figure 1: A coloring rule at a crossing

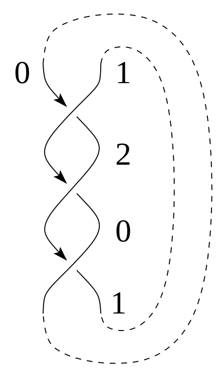

Figure 2: Tefoil as the closure of σ_1^3

The fundamental quandle is defined in a manner similar to the fundamental group [14, 20]. A *presentation* of a quandle is defined in a manner similar to groups as well, and a presentation of the fundamental quandle is obtained from a knot diagram (see, for example, [8]), by assigning generators to arcs of a knot diagram, and relations corresponding to crossings. The set of a coloring of a knot diagram K by a quandle X, then, is in one-to-one correspondence with the set of quandle homomorphisms from the fundamental quandle of K to X.

3 Definition and notation for Galkin quandles

Let A be an abelian group, also regarded naturally as a $\mathbb{Z}$-module. Let $\mu : \mathbb{Z}_3 \to \mathbb{Z}$, $\tau : \mathbb{Z}_3 \to A$ be functions. Define a binary operation on $\mathbb{Z}_3 \times A$ by

$$(x, a) * (y, b) = (2y - x, -a + \mu(x - y)b + \tau(x - y)) \quad x, y \in \mathbb{Z}_3,\ a, b \in A.$$

Proposition 3.1 *For any abelian group A, the above operation $*$ defines a quandle structure on $\mathbb{Z}_3 \times A$ if $\mu(0) = 2$, $\mu(1) = \mu(2) = -1$, and $\tau(0) = 0$.*

Galkin gave this definition in [11], page 950, for $A = \mathbb{Z}_p$. The proposition generalizes his result to any abelian group A. For the proof, we examine the axioms.

Lemma 3.2 *(A) The operation is idempotent (i.e., satisfies Axiom (1)) if and only if $\mu(0) = 2$ and $\tau(0) = 0$. (B) The operation as right action is invertible (i.e. satisfies Axiom (2)).*

Proof. Direct calculations. □

Lemma 3.3 *The operation $*$ on $\mathbb{Z}_3 \times A$ is right self-distributive (i.e., satisfies Axiom (3)) if and only if μ, τ satisfy the following conditions for any $X, Y \in \mathbb{Z}_3$:*

$$\begin{aligned} \mu(-X) &= \mu(X), & (4)\\ \mu(X+Y) + \mu(X-Y) &= \mu(X)\mu(Y), & (5)\\ \tau(X+Y) + \tau(Y-X) &= \tau(X) + \tau(-X) + \mu(X)\tau(Y). & (6) \end{aligned}$$

Proof. The right self-distributivity

$$((x,a) * (y,b)) * (z,c) = ((x,a) * (z,c)) * ((y,b) * (z,c)) \quad \text{for} \quad x,y,z \in \mathbb{Z}_3 \quad \text{and} \quad a,b,c \in A,$$

is satisfied if and only if

$$\begin{aligned} \mu(x-y) &= \mu(y-x),\\ \mu(2y-x-z) &= -\mu(x-z) + \mu(y-x)\mu(y-z),\\ -\tau(x-y) + \tau(2y-x-z) &= -\tau(x-z) + \mu(y-x)\tau(y-z) + \tau(y-x), \end{aligned}$$

by equating the coefficients of b, c, and the constant term.

The first one is equivalent to (4) by setting $X = x - y$. The second is equivalent to (5) by setting $X = y - x$ and $Y = z - y$. The third is equivalent to (6) by $X = y - x$ and $Y = y - z$. □

Proof of Proposition 3.1. Assume the conditions stated. By Lemma 3.2 Axioms (1) and (2) are satisfied under the specifications $\mu(0) = 2, \mu(1) = \mu(2) = -1$, and $\tau(0) = 0$.

If $X = 0$ or $Y = 0$, then (5) (together with (4)) becomes tautology. If $X - Y = 0$ or $X + Y = 0$, then (5) reduces to $\mu(2X) + 2 = \mu(X)^2$ which is satisfied by the above specifications. For R_3, if $X + Y \neq 0$ and $X - Y \neq 0$, then either $X = 0$ or $Y = 0$. Hence (5) is satisfied. For (6), it is checked similarly, for the two cases [$X = 0$ or $Y = 0$], and [$X - Y = 0$ or $X + Y = 0$]. □

Definition 3.4 Let A be an abelian group. The quandle defined by $*$ on $\mathbb{Z}_3 \times A$ by Proposition 3.1 with $\mu(0) = 2, \mu(1) = \mu(2) = -1$ and $\tau(0) = 0$ is called the *Galkin quandle* and denoted by $G(A, \tau)$.

Since τ is specified by the values $\tau(1) = c_1$ and $\tau(2) = c_2$, where $c_1, c_2 \in A$, we also denote it by $G(A, c_1, c_2)$.

Lemma 3.5 *For any abelian group A and $c_1, c_2 \in A$, $G(A, c_1, c_2)$ and $G(A, 0, c_2 - c_1)$ are isomorphic.*

Proof. Let $c = c_2 - c_1$. Define $\eta : G(A, c_1, c_2) \to G(A, 0, c)$, as a map on $\mathbb{Z}_3 \times A$, by $\eta(x, a) = (x, a + \beta(x))$, where $\beta(0) = \beta(1) = 0$, and $\beta(2) = -c_1$. This η is a bijection, and we show that it is a quandle homomorphism. We compute $\eta((x, a) * (y, b))$ and $\eta(x, a) * \eta(y, b)$ for $x, y \in \mathbb{Z}_3$, $a, b \in A$.

If $x = y$, then $\mu(x - y) = 2$ and $\tau(x - y) = 0$ for both $G(A, c_1, c_2)$ and $G(A, 0, c)$, so that

$$\begin{aligned} \eta((x,a)*(x,b)) &= \eta(x, 2b-a) = (x, 2b - a + \beta(x)), \\ \eta(x,a)*\eta(x,b) &= (x, a+\beta(x)) * (x, b+\beta(x)) = (\ x,\ 2(b+\beta(x)) - (a+\beta(x))\ ) \\ &= (x, 2b - a + \beta(x)) \end{aligned}$$

as desired.

If $x - y = 1 \in \mathbb{Z}_3$, then $\mu(x - y) = -1$ for both $G(A, c_1, c_2)$ and $G(A, 0, c)$ and $\tau(x - y) = c_1$ for $G(A, c_1, c_2)$ but $\tau(x - y) = 0$ for $G(A, 0, c)$, so that

$$\begin{aligned} \eta((x,a)*(y,b)) &= \eta(2y - x, -a - b + c_1) = (2y - x, -a - b + c_1 + \beta(2y - x), \\ \eta(x,a)*\eta(y,b) &= (x, a+\beta(x)) * (y, b+\beta(y)) = (\ 2y - x,\ -(a+\beta(x)) - (b+\beta(y))\ ). \end{aligned}$$

This holds if and only if $\beta(x) + \beta(y) + \beta(2y - x) = -c_1$, which is true since $x \neq y$ implies that exactly one of $x, y, 2y - x$ is $2 \in \mathbb{Z}_3$.

If $x - y = 2 \in \mathbb{Z}_3$, then $\mu(x - y) = -1$ for both $G(A, c_1, c_2)$ and $G(A, 0, c)$ and $\tau(x - y) = c_2$ for $G(A, c_1, c_2)$ but $\tau(x - y) = c_2 - c_1 = c$ for $G(A, 0, c)$, so that

$$\begin{aligned} \eta((x,a)*(y,b)) &= \eta(2y - x, -a - b + c_2) = (2y - x, -a - b + c_2 + \beta(2y - x)), \\ \eta(x,a)*\eta(y,b) &= (x, a+\beta(x)) * (y, b+\beta(y)) = (2y - x, -(a+\beta(x)) - (b+\beta(y))) \\ &= (2y - x, -a - b - \beta(x) - \beta(y) + (c_2 - c_1)), \end{aligned}$$

and again these are equal for the same reason as above. □

Notation. Since by Lemma 3.5, any Galkin quandle is isomorphic to $G(A, 0, c)$ for an abelian group A and $c \in A$, we denote $G(A, 0, c)$ by $G(A, c)$ for short.

Any finite abelian group is a product $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ where the positive integers n_j satisfy that $n_j | n_{j+1}$ for $j = 1, \ldots, k - 1$. In this case any element $c \in A$ is written in a vector form $[c_1, \ldots, c_k]$, where $c_j \in \mathbb{Z}_{n_j}$. Then the corresponding Galkin quandle is denoted by $G(A, [c_1, \ldots, c_k])$.

Remark 3.6 We note that the definition of Galkin quandles induces a functor. Let $\mathbf{Ab}_0$ denote the category of pointed abelian groups, that, is the category whose objects are pairs (A, c) where A is an abelian group and $c \in A$ and whose morphisms $f : (A, c) \to (B, d)$ are group homomorphisms $f : A \to B$ such that $f(c) = d$. Let $\mathbf{Q}$ be the category of quandles, consisting quandles as objects and quandle homomorphisms as morphisms.

Then the correspondence $(A, c) \overset{\mathcal{F}}{\mapsto} G(A, c)$ defines a functor $\mathcal{F} : \mathbf{Ab}_0 \to \mathbf{Q}$. It is easy to verify that if a morphism $f : (A, c) \to (B, d)$ is given then the mapping $\mathcal{F}(f)(x, a) = (x, f(a))$, $(x, a) \in G(A, c) = \mathbb{Z}_3 \times A$, is a homomophism from $G(A, c)$ to $G(B, d)$, and satisfies $\mathcal{F}(gf) = \mathcal{F}(g)\mathcal{F}(f)$ and $\mathcal{F}(\mathrm{id}_{(A,c)}) = \mathrm{id}_{G(A,c)}$.

4 Isomorphism classes

In this section we classify isomorphism classes of Galkin quandles.

Lemma 4.1 *Let A be an abelian group, and $h : A \to A'$ be a group isomorphism. Then Galkin quandles $G(A, \tau)$ and $G(A', h\tau)$ are isomorphic as quandles.*

Proof. Define $f : G(A, \tau) \to G(A', h\tau)$, as a map from $\mathbb{Z}_3 \times A$ to $\mathbb{Z}_3 \times A'$, by $f(x, a) = (x, h(a))$. This f is a bijection, and we show that it is a quandle homomorphism by computing $f((x, a) * (y, b))$ and $f(x, a) * f(y, b)$ for $x, y \in \mathbb{Z}_3$, $a, b \in A$.

If $x = y$, then $\mu(x - y) = 2$ and $\tau(x - y) = 0 = h\tau(0)$ for both $G(A, \tau)$ and $G(A', h\tau)$, so that

$$\begin{aligned} f((x, a) * (x, b)) &= f(x, 2b - a) = (x, h(2b - a)), \\ f(x, a) * f(x, b) &= (x, h(a)) * (x, h(b)) = (\ x,\ 2h(b) - h(a)\ ) \end{aligned}$$

as desired.

If $x - y = 1 \in \mathbb{Z}_3$, then $\mu(x - y) = -1$ for both $G(A, \tau)$ and $G(A', h\tau)$.

$$\begin{aligned} f((x, a) * (y, b)) &= f(2y - x, -a - b + \tau(x - y)) = (\ 2y - x,\ h(-a - b + \tau(x - y))\ ), \\ f(x, a) * f(y, b) &= (x, h(a)) * (y, h(b)) = (\ 2y - x,\ -h(a) - h(b) + h\tau(x - y)\ ) \end{aligned}$$

as desired. □

Lemma 4.2 *Let c, d, n be positive integers. If $\gcd(c, n) = d$, then $G(\mathbb{Z}_n, c)$ is isomorphic to $G(\mathbb{Z}_n, d)$.*

Proof. If $A = \mathbb{Z}_n$ then $\text{Aut}(A) = \mathbb{Z}_n^* =$ units of $\mathbb{Z}_n$, and the divisors of n are representatives of the orbits of $\mathbb{Z}_n^*$ acting on $\mathbb{Z}_n$. □

Thus we may choose the divisors of n for the values of c for representing isomorphism classes of $G(\mathbb{Z}_n, c)$.

Corollary 4.3 *If A is a vector space (elementary p-group) then there are exactly two isomorphism classes of Galkin quandles $G(A, \tau)$.*

Proof. If A is a vector space containing non-zero vectors c_1 and c_2, then there is a non-singular linear transformation h of A such that $h(c_1) = c_2$. That $G(A, 0)$ is not isomorphic to $G(A, c)$ if $c \neq 0$ follows from Lemma 4.5 below. □

For distinguishing isomorphism classes, cycle structures of the right action is useful, and we use the following lemmas.

Lemma 4.4 *For any abelian group A, the Galkin quandle $G(A, \tau)$ is connected.*

Proof. Recall that the operation is defined by the formula

$$(x,a)*(y,b) = (2y-x, -a+\mu(x-y)b+\tau(x-y)),$$

$\mu(0) = 2$, $\mu(1) = \mu(2) = -1$ and $\tau(0) = 0$. If $x \neq y$, then $(x,a)*(y,b) = (2y-x, -a-b+c_i) = (z,c)$ where $i = 1$ or 2 and $x,y \in \mathbb{Z}_3$, $a,b \in A$. Note that $\{x,y,2y-x\} = \mathbb{Z}_3$ if $x \neq y$. In particular, for any (x,a) and (z,c) with $x \neq z$, there is (y,b) such that $(x,a)*(y,b) = (z,c)$.

For any (x,a_1) and (x,a_2) where $x \in \mathbb{Z}_3$, $a_1, a_2 \in A$, take $(z,c) \in \mathbb{Z}_3 \times A$ such that $z \neq x$. Then there are $(y,b_1),(y,b_2)$ such that $x \neq y \neq z$ and $(x,a_1)*(y,b_1) = (z,c)$ and $(z,c)*(y,b_2) = (x,a_2)$. Hence $G(A,\tau)$ is connected. □

Lemma 4.5 *The cycle structure of a right translation in $G(A,\tau)$ where $\tau(0) = \tau(1) = 0$ and $\tau(2) = c$, consists of 1-cycles, 2-cycles and $2k$-cycles where k is the order of c in the group A.*

Since isomorphic quandles have the same cycle structure of right translations, $G(A,c)$ and $G(A,c')$ for $c,c' \in A$ are not isomorphic unless the orders of c and c' coincide.

Proof. Let $\tau(0) = 0$, $\tau(1) = 0$ and $\tau(2) = c$. Then by Lemma 4.4, the cycle structure of each column is the same as the cycle structure of the right translation by $(0,0)$, that is, of the permutation $f(x,a) = (x,a)*(0,0) = (-x, -a+\tau(x))$.

We show that this permutation has cycles of length only 1, 2 and twice the order of c in A. Since $f(0,a) = (0,-a)$ for $a \in A$, $a \neq 0$, we have $f^2(0,a) = (0,a)$ so that $(0,a)$ generates a 2-cycle, or a 1-cycle if $2a = 0$. Now from $f(1,a) = (2,-a)$ and $f(2,a) = (1,-a+c)$ for $a \in A$, by induction it is easy to see that for $k > 0$, $f^{2k}(1,a) = (1,a+kc)$ and $f^{2k}(2,a) = (2,a-kc)$. In the case of $(1,a)$, $a \neq 0$, the cycle closes when $a + kc = a$ in A. The smallest k for which this holds is the order of c, in which case the cycle is of length $2k$. A cycle beginning at $(2,a)$ similarly has this same length. □

Proposition 4.6 *Let n be a positive integer, $A = \mathbb{Z}_n$, and $c_i, c_i' \in \mathbb{Z}_n$ for $i = 1,2$. Two Galkin quandles $G(A,c_1,c_2)$ and $G(A,c_1',c_2')$ are isomorphic if and only if* $\gcd(c_1-c_2,n) = \gcd(c_1'-c_2',n)$.

Proof. If $\gcd(c_1-c_2,n) = \gcd(c_1'-c_2',n)$, then they are isomorphic by Lemmas 3.5 and 4.2. The cycle structures are different if $\gcd(c_1-c_2,n) \neq \gcd(c_1'-c_2',n)$ by Lemma 4.5, and hence they are not isomorphic. □

Remark 4.7 The cycle structure is not sufficient for non-cyclic groups A. For example, let $A = \mathbb{Z}_2 \times \mathbb{Z}_4$. Then $G(A,[1,0])$ and $G(A,[0,2])$ have the same cycle structure for right translations, with cycle lengths $\{2,2,4,4,4,4\}$ in a multiset notation, yet they are known to be not isomorphic. (In the notation of Example 4.12 (see below), $G(A,[1,0]) = C[24,29]$ and $G(A,[0,2]) = C[24,31]$, that are not isomorphic.) We note that there is no automorphism of A carrying $[1,0]$ to $[0,2]$.

More generally the isomorphism classes of Galkin quandles are characterized as follows.

Theorem 4.8 Suppose A, A' are finite abelian groups. Two Galkin quandles $G(A,\tau)$ and $G(A',\tau')$ are isomorphic if and only if there exists a group isomorphism $h : A \to A'$ such that $h\tau = \tau'$.

One implication is Lemma 4.1. For the other, first we prove the following two lemmas. We will use a well known description of the automorphisms of a finite abelian group which can be found in [13, 26].

Lemma 4.9 *Let A be a finite abelian p-group and let $f : pA \to pA$ be an automorphism. Then f can be extended to an automorphism of A.*

Proof. Let $A = \mathbb{Z}_{p^1}^{n_1} \times \cdots \times \mathbb{Z}_{p^k}^{n_k}$. Then

$$f(\begin{bmatrix} px_2 \\ \vdots \\ px_k \end{bmatrix}) = P \begin{bmatrix} px_2 \\ \vdots \\ px_k \end{bmatrix}, \qquad \begin{bmatrix} x_2 \\ \vdots \\ x_k \end{bmatrix} \in \mathbb{Z}_{p^2}^{n_2} \times \cdots \times \mathbb{Z}_{p^k}^{n_k}, \tag{7}$$

where

$$P = \begin{bmatrix} P_{22} & P_{23} & \cdots & P_{2k} \\ pP_{32} & P_{33} & \cdots & P_{3k} \\ \vdots & \vdots & & \vdots \\ p^{k-2}P_{k2} & p^{k-3}P_{k3} & \cdots & P_{kk} \end{bmatrix}, \tag{8}$$

$P_{ij} \in \mathrm{M}_{n_i \times n_j}(\mathbb{Z})$, $\det P_{ii} \not\equiv 0 \pmod p$. Define $g : A \to A$ by

$$g(\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix}) = \begin{bmatrix} I & \\ & P \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix}, \qquad \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix} \in \mathbb{Z}_{p^1}^{n_1} \times \mathbb{Z}_{p^2}^{n_2} \times \cdots \times \mathbb{Z}_{p^k}^{n_k}.$$

Then $g \in \mathrm{Aut}(A)$ and $g|_{pA} = f$. □

Lemma 4.10 *Let A be a finite abelian p-group and let $a, b \in A \setminus pA$. If there exists an automorphism $f : pA \to pA$ such that $f(pa) = pb$, then there exists an automorphism $g : A \to A$ such that $g(a) = b$.*

Proof. Let $A = \mathbb{Z}_{p^1}^{n_1} \times \cdots \times \mathbb{Z}_{p^k}^{n_k}$ and let f be defined by (7) and (8). Write

$$a = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}, \ b = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}, \quad a_i, b_i \in \mathbb{Z}_{p^i}^{n_i}.$$

Since $f(pa) = pb$, we have

$$p\Big(P \begin{bmatrix} a_2 \\ \vdots \\ a_n \end{bmatrix} - \begin{bmatrix} b_2 \\ \vdots \\ b_n \end{bmatrix}\Big) = 0,$$

i.e.,

$$P \begin{bmatrix} a_2 \\ \vdots \\ a_n \end{bmatrix} - \begin{bmatrix} b_2 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} pc_2 \\ \vdots \\ p^{k-1}c_k \end{bmatrix}, \quad c_i \in \mathbb{Z}_{p^i}^{n_i}, \ 2 \le i \le k. \tag{9}$$

Case 1. Assume that $\begin{bmatrix} a_2 \\ \vdots \\ a_n \end{bmatrix} \in pA$. Then by (9), $\begin{bmatrix} b_2 \\ \vdots \\ b_n \end{bmatrix} \in pA$. So $a_1 \neq 0$ and $b_1 \neq 0$. Then we have

$$\begin{bmatrix} pc_2 \\ \vdots \\ p^{k-1}c_k \end{bmatrix} = \begin{bmatrix} pQ_2 \\ \vdots \\ p^{k-1}Q_k \end{bmatrix} a_1$$

for some $Q_i \in \mathrm{M}_{n_i \times n_1}(\mathbb{Z})$, $2 \leq i \leq k$. Also, there exists $P_{11} \in \mathrm{M}_{n_1 \times n_1}(\mathbb{Z})$ such that $\det P_{11} \not\equiv 0 \pmod{p}$ and $P_{11}a_1 = b_1$. Let $g \in \mathrm{Aut}(A)$ be defined by

$$g\left(\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix}\right) = \begin{bmatrix} P_{11} & 0 \\ -pQ_2 & \\ \vdots & P \\ -p^{k-1}Q_k & \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix}, \qquad x_i \in \mathbb{Z}_{p^i}^{n_i}.$$

Then $g(a) = b$.

Case 2. Assume that $\begin{bmatrix} a_2 \\ \vdots \\ a_n \end{bmatrix} \notin pA$. Then there exists $2 \leq s \leq k$ such that $a_s \notin p\mathbb{Z}_{p^s}^{n_s}$. Then we have

$$\begin{bmatrix} c_2 \\ \vdots \\ p^{k-2}c_k \end{bmatrix} = \begin{bmatrix} Q_2 \\ \vdots \\ p^{k-2}Q_k \end{bmatrix} a_s$$

for some $Q_i \in \mathrm{M}_{n_i \times n_s}(\mathbb{Z})$, $2 \leq i \leq k$. Put

$$Q = \begin{bmatrix} 0 & \cdots & 0 & Q_2 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & p^{k-2}Q_k & 0 & \cdots & 0 \end{bmatrix},$$

where the (i,j) block is of size $n_i \times n_j$ and Q_2 is in the $(1,s)$ block. Then $Q \begin{bmatrix} a_2 \\ \vdots \\ a_k \end{bmatrix} = \begin{bmatrix} c_2 \\ \vdots \\ p^{k-2}c_k \end{bmatrix}$.

Also, there exist $U \in \mathrm{M}_{n_1 \times (n_2 + \cdots + n_k)}(\mathbb{Z})$ such that $U \begin{bmatrix} a_2 \\ \vdots \\ a_k \end{bmatrix} = b_1 - a_1$. Now define $g \in \mathrm{Aut}(A)$ by

$$g\left(\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix}\right) = \begin{bmatrix} I & U \\ 0 & P - pQ \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix}, \qquad x_i \in \mathbb{Z}_{p^i}^{n_i}.$$

Then $g(a) = b$. $\square$

Proof of Theorem 4.8. We assume that $|3A'| \leq |3A|$. Since $G(A', c')$ is connected, there exists an isomorphism $\phi : G(A, c) \to G(A', c')$ such that $\phi(0, 0) = (0, 0)$. Write

$$\phi(x, a) = (\alpha(x, a), \beta(x, a)), \quad (x, a) \in \mathbb{Z}_3 \times A.$$

Define $t : \mathbb{Z}_3 \to A$ by

$$t(x) = \begin{cases} 1 & \text{if } x = 2, \\ 0 & \text{if } x \neq 2, \end{cases}$$

so that for $(x, a), (y, b) \in \mathbb{Z}_3 \times A$, the operation on $G(A, c)$ is written by

$$(x, a) * (y, b) = (-x - y, -a + \mu(x - y)b + t(x - y)c).$$

Then $\phi((x, a) * (y, b)) = \phi(x, a) * \phi(y, b)$ is equivalent to

$$\alpha(-x - y, -a + \mu(x - y)b + t(x - y)c) = -\alpha(x, a) - \alpha(y, b), \tag{10}$$

$$\begin{aligned} &\beta(-x - y, -a + \mu(x - y)b + t(x - y)c) \\ = &- \beta(x, a) + \mu(\alpha(x, a) - \alpha(y, b))\beta(y, b) + t(\alpha(x, a) - \alpha(y, b))c'. \end{aligned} \tag{11}$$

1° We claim that $\alpha(0, \cdot) : A \to \mathbb{Z}_3$ is a homomorphism.

Setting $x = y = 0$ in (10) we have

$$\alpha(0, -a + 2b) = -\alpha(0, a) - \alpha(0, b). \tag{12}$$

Setting $b = 0$ in (12) we have

$$\alpha(0, -a) = -\alpha(0, a). \tag{13}$$

By the symmetry of the RHS of (12), we also have

$$\alpha(0, -a + 2b) = \alpha(0, -b + 2a), \quad a, b \in A. \tag{14}$$

Now we have

$$\begin{aligned} \alpha(0, a + b) &= \alpha(0, a - b + 2b) \\ &= \alpha(0, -b + 2(b - a)) && \text{(by (14))} \\ &= \alpha(0, b - 2a) \\ &= -\alpha(0, -b) - \alpha(0, -a) && \text{(by (12))} \\ &= \alpha(0, a) + \alpha(0, b) && \text{(by (13))}. \end{aligned}$$

2° We claim that there exists $u \in \mathbb{Z}_3$ such that

$$\alpha(x, a) = \alpha(0, a) + ux, \quad (x, a) \in \mathbb{Z}_3 \times A. \tag{15}$$

Setting $x = 1$ and $y = 0$ in (10) we have

$$\alpha(-1, -a - b) = -\alpha(1, a) - \alpha(0, b). \tag{16}$$

Setting $b = 0$ in (16) gives

$$\alpha(-1, -a) = -\alpha(1, a). \tag{17}$$

Letting $a = 0$ in (16) and using (17) we get

$$\alpha(1, b) = \alpha(0, b) + \alpha(1, 0), \qquad b \in A. \tag{18}$$

Equations (18) and (17) also imply that

$$\alpha(-1, -b) = \alpha(0, -b) - \alpha(1, 0), \qquad b \in A. \tag{19}$$

Let $u = \alpha(1, 0)$. Then

$$\alpha(x, a) = \alpha(0, a) + ux, \qquad (x, a) \in \mathbb{Z}_3 \times A.$$

3° We claim that

$$\alpha(0, c) = 0. \tag{20}$$

Substituting (15) in(10) we get

$$\alpha(0, -a + \mu(x - y)b + t(x - y)c) = -\alpha(0, a) - \alpha(0, b).$$

Setting $x - y = 2$ we have $\alpha(0, c) = 0$.

The remaining part of the proof is divided into two cases according as u is zero or nonzero in (15).

Case 1. Assume $u = 0$ in (15).

We have $\alpha(x, a) = \alpha(0, a)$ for all $(x, a) \in \mathbb{Z}_3 \times A$. We write $\alpha(a)$ for $\alpha(0, a)$. Then (11) becomes

$$\beta(-x - y, -a + \mu(x - y)b + t(x - y)c) = -\beta(x, a) + \mu(\alpha(a - b))\beta(y, b) + t(\alpha(a - b))c'. \tag{21}$$

1.1° We claim that $c = 0$.

Equation (21) with $x = 1$, $y = 0$, $a = b = 0$ yields

$$\beta(-1, 0) = -\beta(1, 0),$$

and with $x = -1$, $y = 0$, $a = b = 0$, it yields

$$\beta(1, c) = -\beta(-1, 0).$$

Thus $\beta(1, c) = \beta(1, 0)$. Since $\alpha(1, c) = 0 = \alpha(1, 0)$, we have $\phi(1, c) = \phi(1, 0)$. Thus $c = 0$.

1.2° We claim that $c' = 0$.

The homomorphism $\alpha : A \to \mathbb{Z}_3$ must be onto. (Otherwise ϕ is not onto.) Choose $d \in A$ such that $\alpha(d) = -1$. Equation (21) with $x = y = 0$, $a = d$, $b = 0$ gives

$$\beta(0, -d) = -\beta(0, d) + c',$$

and with $x = y = 0$, $a = -d$, $b = 0$, it gives

$$\beta(0, d) = -\beta(0, -d).$$

Therefore $c' = 0$.

1.3° Now (21) becomes

$$\beta(-x - y, -a + \mu(x - y)b) = -\beta(x, a) + \mu(\alpha(a - b))\beta(y, b). \tag{22}$$

Setting $y = 0$ and $b = 0$ in (22) we have

$$\beta(-x, -a) = -\beta(x, a). \tag{23}$$

1.4° We claim that $\beta(0, \cdot) : 3A \to A'$ is a 1-1 homomorphism.

Note that $3A \subset \ker \alpha$. Let $a, b \in 3A$ and $x = -1$, $y = 1$ in (22). We have

$$\beta(0, -a - b) = -\beta(-1, a) + 2\beta(1, b). \tag{24}$$

Setting $b = 0$ and $a = 0$, respectively, in (24) and using (23) we have

$$\beta(0, -a) = -\beta(-1, a) + 2\beta(1, 0) = \beta(1, -a) + 2\beta(1, 0), \tag{25}$$

$$\beta(0, -b) = -\beta(-1, 0) + 2\beta(1, b) = \beta(1, 0) + 2\beta(1, b). \tag{26}$$

Setting $a = b = 0$ in (24) we have

$$3\beta(1, 0) = 0. \tag{27}$$

Combining (24) – (27) we have

$$\beta(0, -a - b) = \beta(0, -a) + \beta(0, -b).$$

If $a \in 3A$ such that $\beta(0, a) = 0$, then $\phi(0, a) = (0, 0)$, so $a = 0$. Thus $\beta(0, \cdot) : 3A \to A'$ is 1-1.

1.5° We claim that $\beta(0, 3b) \in 3A'$ for all $b \in A$.

Let $x = y = 0$ and $a = -b$ in (22). We have

$$\begin{aligned}\beta(0, 3b) &= -\beta(0, -b) + \mu(\alpha(-2b))\beta(0, b)\\ &= \beta(0, b) + \mu(\alpha(b))\beta(0, b)\\ &\equiv 0 \pmod{3A'} \qquad \text{(since } \mu(\alpha(b)) \equiv -1 \pmod 3).\end{aligned}$$

1.6° Now $\beta(0, \cdot) : 3A \to 3A'$ is a 1-1 homomorphism. Since $|3A'| \le |3A|$, $\beta(0, \cdot) : 3A \to 3A'$ is an isomorphism. Since $|A| = |A'|$, we have $A \cong A'$. We are done in Case 1.

Case 2. Assume $u \neq 0$ in (15).

By the proofs of Lemma 3.5 and Proposition 5.5 (see below), $(x', a') \mapsto (-x', a' - t(-x')c')$ is an isomorphism from $G(A', c')$ to $G(A', -c')$. Thus we may assume $u = 1$ in (15). We have $\alpha(x, a) = \alpha(0, a) + x$ for all $(x, a) \in \mathbb{Z}_3 \times A$.

2.1° We claim that $\beta(0,\cdot):\ker\alpha(0,\cdot)\to A'$ is a 1-1 homomorphism.

In (11) let $a,b\in\ker\alpha(0,\cdot)$ and $x=-1$, $y=1$. We have

$$\beta(0,-a-b)=-\beta(-1,a)-\beta(1,b). \tag{28}$$

Eq.uation (28) with $a=-b$ yields

$$\beta(-1,-b)=-\beta(1,b). \tag{29}$$

So

$$\beta(0,-a-b)=\beta(1,-a)-\beta(1,b). \tag{30}$$

Letting $b=0$ and $a=0$ in (30), respectively, we have

$$\begin{aligned}\beta(0,-a) &= \beta(1,-a)-\beta(1,0),\\ \beta(0,-b) &= \beta(1,0)-\beta(1,b).\end{aligned}$$

Thus

$$\begin{aligned}\beta(0,-a)+\beta(0,-b) &= \beta(1,-a)-\beta(1,b)\\ &= \beta(0,-a-b) \qquad \text{(by (30))}.\end{aligned}$$

If $a\in\ker\alpha(0,\cdot)$ such that $\beta(0,a)=0$, then $\phi(0,a)=(0,0)$, so $a=0$. Hence $\beta(0,\cdot):\ker\alpha(0,\cdot)\to A'$ is 1-1.

2.2° We claim that $\beta(0,3a)\in 3A'$ for all $a\in A$.

Setting $x=y=0$ in (11) we have

$$\begin{aligned}\beta(0,-a+2b) &= -\beta(0,a)+\mu(\alpha(0,a-b))\beta(0,b)+t(\alpha(0,a-b))c'\\ &\equiv -\beta(0,a)-\beta(0,b)+t(\alpha(0,a-b))c' \pmod{3A'}.\end{aligned} \tag{31}$$

By (31),

$$\beta(0,3a)=\beta(0,-a+2(2a))\equiv -\beta(0,a)-\beta(0,2a)+t(\alpha(0,-a))c' \pmod{3A'}$$

and

$$\beta(0,2a)=\beta(0,0+2a)\equiv -\beta(0,a)+t(\alpha(0,-a))c' \pmod{3A'}.$$

Thus $\beta(0,3a)\equiv 0 \pmod{3A'}$.

2.3° By the argument in 1.6°, $\beta(0,\cdot):3A\to 3A'$ is an isomorphism and $A\cong A'$.

2.4° We claim that $\beta(0,c)=c'$.

Equation (11) with $x=1$, $y=-1$, $a=b=0$ yields

$$\begin{aligned}\beta(0,c) &= -\beta(1,0)-\beta(-1,0)+c'\\ &= c' \qquad \text{(by (29))}.\end{aligned}$$

2.4° Now we complete the proof in Case 2. Write $A=A_1\oplus A_2$ and $A'=A_1'\oplus A_2'$, where $3\nmid |A_1|$, $3\nmid |A_1'|$, $|A_2|$ and $|A_2'|$ are powers of 3. Write $c=c_1+c_2$, where $c_1\in A_1$, $c_2\in A_2$. Then

$C[6,1]$	$=$	$G(\mathbb{Z}_2,[0])$	1084	$C[24,28]$	$=$	$G(\mathbb{Z}_8,[4])$	1084
$C[6,2]$	$=$	$G(\mathbb{Z}_2,[1])$	1084	$C[24,29]$	$=$	$G(\mathbb{Z}_2\times\mathbb{Z}_4,[1,0],[1,2])$	1084
$C[9,2]$	$=$	$G(\mathbb{Z}_3,[0])$	1084	$C[24,30]$	$=$	$G(\mathbb{Z}_2\times\mathbb{Z}_4,[0,0])$	1084
$C[9,6]$	$=$	$G(\mathbb{Z}_3,[1])$	1084	$C[24,31]$	$=$	$G(\mathbb{Z}_2\times\mathbb{Z}_4,[0,2])$	1084
$C[12,5]$	$=$	$G(\mathbb{Z}_4,[2])$	1084	$C[24,32]$	$=$	$G(\mathbb{Z}_8,[1])$	1051
$C[12,6]$	$=$	$G(\mathbb{Z}_4,[0])$	1084	$C[24,33]$	$=$	$G(\mathbb{Z}_2\times\mathbb{Z}_4,[0,1],[1,1])$	1051
$C[12,7]$	$=$	$G(\mathbb{Z}_4,[1])$	1051	$C[24,38]$	$=$	$G(\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2,[0,0,1])$	1084
$C[12,8]$	$=$	$G(\mathbb{Z}_2\times\mathbb{Z}_2,[0,0])$	1084	$C[24,39]$	$=$	$G(\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2,[0,0,0])$	1084
$C[12,9]$	$=$	$G(\mathbb{Z}_2\times\mathbb{Z}_2,[1,0])$	1084	$C[27,2]$	$=$	$G(\mathbb{Z}_3\times\mathbb{Z}_3,[0,0])$	1084
$C[15,5]$	$=$	$G(\mathbb{Z}_5,[1])$	1440	$C[27,12]$	$=$	$G(\mathbb{Z}_9,[3])$	1084
$C[15,6]$	$=$	$G(\mathbb{Z}_5,[0])$	1512	$C[27,13]$	$=$	$G(\mathbb{Z}_9,[0])$	1084
$C[18,1]$	$=$	$G(\mathbb{Z}_2\times\mathbb{Z}_3,[0,0])$	1084	$C[27,23]$	$=$	$G(\mathbb{Z}_3\times\mathbb{Z}_3,[1,0])$	1084
$C[18,4]$	$=$	$G(\mathbb{Z}_2\times\mathbb{Z}_3,[1,0])$	1084	$C[27,55]$	$=$	$G(\mathbb{Z}_9,[1])$	1084
$C[18,5]$	$=$	$G(\mathbb{Z}_2\times\mathbb{Z}_3,[1,1])$	1084	$C[30,12]$	$=$	$G(\mathbb{Z}_2\times\mathbb{Z}_5,[0,1])$	1440
$C[18,8]$	$=$	$G(\mathbb{Z}_2\times\mathbb{Z}_3,[0,1])$	1084	$C[30,13]$	$=$	$G(\mathbb{Z}_2\times\mathbb{Z}_5,[0,0])$	1512
$C[21,7]$	$=$	$G(\mathbb{Z}_7,[1])$	1339	$C[30,14]$	$=$	$G(\mathbb{Z}_2\times\mathbb{Z}_5,[1,1])$	1440
$C[21,8]$	$=$	$G(\mathbb{Z}_7,[0])$	1386	$C[30,15]$	$=$	$G(\mathbb{Z}_2\times\mathbb{Z}_5,[1,0])$	1512
$C[24,26]$	$=$	$G(\mathbb{Z}_8,[2])$	1071	$C[33,10]$	$=$	$G(\mathbb{Z}_{11},[0])$	1260
$C[24,27]$	$=$	$G(\mathbb{Z}_8,[0])$	1084	$C[33,11]$	$=$	$G(\mathbb{Z}_{11},[1])$	1220

Table 1: Galkin quandles in the rig table

$c_1 \in A_1 \subset \ker\alpha(0,\cdot)$, so $c_2 = c - c_1 \in \ker\alpha(0,\cdot)$. Since $\beta(0,\cdot) : \ker\alpha(0,\cdot) \to A'$ is a homomorphism, we have

$$c' = \beta(0,c_1) + \beta(0,c_2) = c'_1 + c'_2,$$

where $c'_1 = \beta(0,c_1) \in A'_1$ and $c'_2 = \beta(0,c_2) \in A'_2$. By 2.3°, $\beta(0,\cdot) : A_1 \to A'_1$ is an isomorphism. So it suffices to show that there exists an isomorphism $f : A_2 \to A'_2$ such that $f(c_2) = c'_2$.

First assume $c_2 \in 3A_2$. Then $c'_2 \in 3A'_2$. By Lemma 4.9, the isomorphism $\beta(0,\cdot) : 3A \to 3A'$ can be extended to an isomorphism $f : A_2 \to A'_2$ and we are done.

Now assume that $c_2 \in A_2 \setminus 3A_2$. We claim that $c_2 \in A'_2 \setminus 3A'_2$. Assume to the contrary that $c'_2 \in 3A'_2$. By 2.3°, there exists $d \in A_2$ such that $\beta(0,3d) = c'_2 = \beta(0,c_2)$. By 2.1°, $c_2 = 3d$, which is a contradiction.

Note that $\beta(0,\cdot) : 3A_2 \to 3A'_2$ is an isomorphism and

$$\begin{aligned}\beta(0,3c_2) &= 3\beta(0,c_2) \qquad \text{(by 2.1°)}\\ &= 3c'_2.\end{aligned}$$

By Lemma 4.10, there exists an isomorphism $f : A_2 \to A'_2$ such that $f(c_2) = c'_2$. □

Remark 4.11 The numbers of isomorphism classes of order $3n$, from $n = 1$ to $n = 100$, are as follows:
1, 2, 2, 5, 2, 4, 2, 10, 5, 4, 2, 10, 2, 4, 4, 20, 2, 10, 2, 10, 4, 4, 2, 20, 5, 4, 10, 10, 2, 8, 2, 36, 4, 4, 4, 25, 2, 4, 4, 20, 2, 8, 2, 10, 10, 4, 2, 40, 5, 10, 4, 10, 2, 20, 4, 20, 4, 4, 2, 20, 2, 4, 10, 65, 4, 8, 2, 10, 4, 8, 2, 50, 2, 4, 10, 10, 4, 8,

$2, 40, 20, 4, 2, 20, 4, 4, 4, 20, 2, 20, 4, 10, 4, 4, 4, 72, 2, 10, 10, 25$.

In [7] it is shown that the number $N(n)$ of isomorphism classes of Galkin quandles of order n is multiplicative, that is, if $\gcd(n, m) = 1$ then $N(nm) = N(n)N(m)$, so it suffices to find $N(q^n)$ for all prime powers q^n. In [7] it is established that $N(q^n) = \sum_{0 \leq m \leq n} p(m)p(n-m)$, where $p(m)$ is the number of partitions of the integer m. In particular, $N(q^n)$ is independent of the prime q. The sequence $n \mapsto N(q^n)$ appears in the On-Line Encyclopedia of Integer Sequences (OEIS, [23]) as sequence $A000712$.

Example 4.12 In [30], connected quandles are listed up to order 35. For a positive integer $n > 1$, let $q(n)$ be the number of isomorphism classes of connected quandles of order n. For a positive integer $n > 1$, if $q(n) \neq 0$, then we denote by $C[n, i]$ the i-th quandle of order n in their list ($1 < n \leq 35$, $i = 1, \ldots, q(n)$). We note that $q(n) = 0$ for $n = 2, 14, 22, 26$, and 34 (for $1 < n \leq 35$). The quandle $C[n, i]$ is denoted by $Q_{n,i}$ in [31] (and they are left-distributive in [31], so that the matrix of $C[n, i]$ is the transpose of the matrix of $Q_{n,i}$). Isomorphism classes of Galkin quandles are identified with those in their list in Table 1.

The 4-digit numbers to the right of each row in Table 1 indicate the numbers of knots that are colored non-trivially by these Galkin quandles, out of total 2977 knots in the table [6] with 12 crossings or less. See Section 6 for more on this.

5 Properties of Galkin quandles

In this section, we investigate various properties of Galkin quandles.

Lemma 5.1 *The Galkin quandle $G(A, \tau)$ is Latin if and only if $|A|$ is odd.*

Proof. To show that it is Latin if n is odd, first note that R_3 is Latin. Suppose that $(x, a) * (y, b) = (x, a) * (y', b')$. Then we have the equations

$$-x + 2y = -x + 2y' \tag{32}$$

$$-a + \mu(x-y)b + \tau(x-y) = -a + \mu(x-y')b' + \tau(x-y'). \tag{33}$$

From (32) it follows that $y = y'$ and it follows from (33) that $\mu(x-y)b = \mu(x-y)b'$. Now since $|A|$ is odd, the left module action of 2 on A is invertible, and hence $b = b'$. If $|A|$ is even there is a non-zero element b of order 2 and hence $(0, 0) * (0, b) = (0, 0) * (0, 0)$, so the quandle is not Latin. □

Lemma 5.2 *Any Galkin quandle is faithful.*

Proof. We show that if $(x, a) * (y, b) = (x, a) * (y', b')$ holds for all (x, a), then $(y, b) = (y', b')$. We have $y = y'$ immediately. From the second factor

$$-a + \mu(x-y)b + \tau(x-y) = -a + \mu(x-y)b' + \tau(x-y),$$

we have $\mu(x-y)b = \mu(x-y)b'$ for any x. Pick x such that $x \neq y$, then $\mu(x-y) = -1$, hence $b = b'$. □

Lemma 5.3 *If A' is a subgroup of A and c' is in A', then $G(A', c')$ is a subquandle of $G(A, c')$.*

Proof. Immediate. □

Lemma 5.4 *Any Galkin quandle $G(A, \tau)$ consists of three disjoint subquandles $\{x\} \times A$ for $x \in \mathbb{Z}_3$, and each is a product of dihedral quandles.*

Proof. Immediate. □

We note the following somewhat curious quandles from Lemma 5.4: For a positive integer k, $G(\mathbb{Z}_2^k, [0, \ldots, 0])$ is a connected quandle that is a disjoint union of three trivial subquandles of order 2^k.

Lemma 5.5 *The Galkin quandle $G(A, \tau)$ has R_3 as a subquandle if and only if $\tau = 0$ or 3 divides $|A|$.*

Proof. If A is any group and $\tau = 0$, then $(x, 0) * (y, 0) = (2y - x, 0)$ for any $x, y \in \mathbb{Z}_3$, so that $\mathbb{Z}_3 \times \{0\}$ is a subquandle isomorphic to R_3. If 3 divides $|A|$, then A has a subgroup B isomorphic to $\mathbb{Z}_3$. In the subquandle $\{0\} \times B$, $(0, a) * (0, b) = (0, -a + 2b)$ for $a, b \in B$, so that $\{0\} \times B$ is a subquandle isomorphic to R_3.

Conversely, let $S = \{(x, a), (y, b), (z, d)\}$ be a subquandle of $G(A, c)$ isomorphic to R_3. Note that the quandle operation of R_3 is commutative, and the product of any two elements is equal to the third. We examine two cases.

Case 1: $x = y = z$. In this case we have

$$\begin{aligned} (x, a) * (x, b) &= (x, -a + 2b) &&= (x, d), \\ (x, b) * (x, a) &= (x, -b + 2a) &&= (x, d). \end{aligned}$$

Hence we have $-a + 2b = -b + 2a$ so that $3(a - b) = 0$. If there are no elements of order 3 in A, then we have $a - b = 0$ and so $b = a$. This is a contradiction to the fact that S contains 3 elements, so there is an element of order 3 in A, hence 3 divides $|A|$.

Case 2: x, y and z are all distinct (if two are distinct then all three are). In this case consider $S = \{(0, a), (1, b), (2, d)\}$. Now we have

$$\begin{aligned} (2, d) * (0, a) &= (1, -d - a + c) &&= (1, b), \\ (0, a) * (2, d) &= (1, -a - d) &&= (1, b). \end{aligned}$$

Hence we have $-d - a + c = -a - d$, so that $c = 0$, and we have $\tau = 0$. □

Lemma 5.6 *The Galkin quandle $G(A, \tau)$ is left-distributive if and only if $3A = 0$, i.e., every element of A has order 3.*

Proof. Let $\tau(1) = c_1, \tau(2) = c_2$. Let $a = (0, 0)$, $b = (0, \alpha)$ and $c = (1, 0)$ for $\alpha \in A$. Then we get $a * (b * c) = (1, \alpha - c_2 + c_1)$ and $(a * b) * (a * c) = (1, -2\alpha - c_2 + c_1)$. If these are equal, then $3\alpha = 0$ for any $\alpha \in A$.

Conversely, suppose that every element of A has order 3. Then we have $\mu(x)a = 2a$ for any $a \in A$. Then one computes

$$\begin{aligned}(x,a) * [(y,b) * (z,c)] \\ = (x * (y * z), -a + b + c - \tau(y - z) + \tau(x - y * z)),\end{aligned} \tag{34}$$

$$\begin{aligned}[(x,a) * (y,b)] * [(x,a) * (z,c)] \\ = ((x * y) * (x * z), -a + b + c - \tau(x - y) - \tau(x - z) + \tau(x * y - x * z)).\end{aligned} \tag{35}$$

If all x, y, z are distinct, then $x - y = 1$ or $x - y = 2$, and $x * y = z$, $x * z = y$, $y * z = x$. If $x - y = 1$, then $z = x + 1$ and $y - z = 1$, $x - z = 2$, and one computes that (34) $= -c_1 =$ (35). If $x - y = 2$, then one computes (34) $= -c_2 =$ (35). The other cases for x, y, z are checked similarly. □

Proposition 5.7 *The Galkin quandle $G(A, \tau)$ is Alexander if and only if $3A = 0$.*

Proof. If $G(A, \tau)$ is Alexander then since it is connected it is left-distributive, hence Lemma 5.6 implies $3A = 0$. Conversely, suppose $3A = 0$. Then $A = \mathbb{Z}_3^k$ for some positive integer k, and is an elementary 3-group. By Corollary 4.3 there are two isomorphism classes, $G(\mathbb{Z}_3^k, [0, \ldots, 0])$ and $G(\mathbb{Z}_3^k, [0, \ldots, 0, 1])$. The quandle $G(\mathbb{Z}_3, 1) = C[9, 6]$ is isomorphic to $\mathbb{Z}_3[t]/(t+1)^2$ by a direct comparison. Hence the two classes are isomorphic to the Alexander quandle R_3^k and $R_3^{k-2} \times \mathbb{Z}_3[t]/(t+1)^2$, respectively. □

Proposition 5.8 *The Galkin quandle $G(A, c)$ is medial if and only if $3A = 0$.*

Proof. We have seen that if $3A = 0$ then $G(A, c)$ is Alexander and hence is medial. Suppose $3b \neq 0$ for some $b \in A$. Then consider the products

$$\begin{aligned} X &= ((0,0) * (1,b)) * ((1,0) * (0,0)) = (-1, b - \tau(-1)) \quad \text{and} \\ Y &= ((0,0) * (1,0)) * ((1,b) * (0,0)) = (-1, -\tau(-1) - 2b). \end{aligned}$$

Since $3b \neq 0$ we have $X \neq Y$ and so $G(A, c)$ is not medial. □

Remark 5.9 The fact that the same condition appeared in 5.6, 5.7 and 5.8 is explained as follows. Alexander quandles are left-distributive and medial. It is easy to check that for a finite Alexander quandle (M, T) with $T \in \mathrm{Aut}(M)$, the following are equivalent: (1) (M, T) is connected, (2) $(1 - T)$ is an automorphism of M, and (3) (M, T) is Latin. It was also proved by Toyoda [29] that a Latin quandle is Alexander if and only if it is medial. As noted by Galkin, $G(\mathbb{Z}_5, 0)$ and $G(\mathbb{Z}_5, 1)$ are the smallest non-medial Latin quandles and hence the smallest non-Alexander Latin quandles.

We note that medial quandles are left-distributive (by idempotency). We show in Theorem 5.10 (below) that any left-distributive connected quandle is Latin. This implies, by Toyoda's theorem, that every medial connected quandle is Alexander and Latin. The smallest Latin quandles that are not left-distributive are the Galkin quandles of order 15.

It is known that the smallest left-distributive Latin quandle that is not Alexander is of order 81. This is due to V. D. Belousov. See, for example, [24] or Section 5 of Galkin [11].

Theorem 5.10 *Every finite connected left-distributive connected quandle is Latin.*

Proof. Let $(X, *)$ be a finite, connected, and left-distributive quandle. For each $a \in X$, let $X_a = \{a * x : x \in X\}$.

1° We claim that $|X_a| = |X_b|$ for all $a, b \in X$. For any $a, y \in X$, we have

$$|X_a| = |X_a * y| = |\{(a * x) * y : x \in X\}| = |\{(a * y) * (x * y) : x \in X\}| = |X_{a*y}|.$$

Since X is connected, we have $|X_a| = |X_b|$ for all $a, b \in X$.

2° Fix $a \in X$. If $|X_a| = X$, by 1°, $X_b = X$ for all $b \in X$ and we are done. So assume $|X_a| < |X|$. Clearly, $(X_a, *)$ is a left-distributive quandle. Since $(X, *)$ is connected and $x \mapsto a * x$ is an onto homomorphism form $(X, *)$ to $(X_a, *)$, $(X_a, *)$ is also connected. Using induction, we may assume that $(X_a, *)$ is Latin.

3° For each $y \in Y$, we claim that $X_{a*y} = X_a$. In fact,

$$\begin{aligned} X_{a*y} &\supset (a * y) * X_a \\ &= X_a \qquad \text{(since } X_a \text{ is Latin)}. \end{aligned}$$

Since $|X_{a*y}| = |X_a|$, we must have $X_{a*y} = X_a$.

4° Since $(X, *)$ is connected, by 3°, $X_b = X_a$ for all $b \in X$. Thus $X = \bigcup_{b \in X} X_b = X_a$, which is a contradiction. □

Proposition 5.11 *Any Galkin quandle is self-dual, that is, isomorphic to its dual.*

Proof. The dual quandle structure of $G(A, \tau) = G(A, c_1, c_2)$ is written by

$$(x, a) \mathbin{\bar{*}} (y, b) = (x \mathbin{\bar{*}} y, -a + \mu(y - x)b + \tau(y - x))$$

for $(x, a), (y, b) \in G(A, \tau)$. Note that $\mu(x - y) = \mu(y - x)$ and $\tau(y - x) = c_{-i}$ if $\tau(x - y) = c_i$ for any $x, y \in X$ and $i \in \mathbb{Z}_3$. Hence its dual is $G(A, c_2, c_1)$. The isomorphism is given by $f : \mathbb{Z}_3 \times A \to \mathbb{Z}_3 \times A$ that is defined by $f(x, a) = (-x, a)$. □

Corollary 5.12 *For any positive integer n, a Galkin quandle $G(A, c_1, c_2)$ is involutory (kei) if and only if $c_1 = c_2 \in A$.*

Proof. A quandle is a kei if and only if it is the same as its dual, i.e., the identity map is an isomorphism between the dual quandle and itself. Hence this follows from Proposition 5.11. □

A *good involution* [15, 16] ρ on a quandle $(X, *)$ is an involution $\rho : X \to X$ (a map with $\rho^2 = \mathrm{id}$) such that $x * \rho(y) = x \mathbin{\bar{*}} y$ and $\rho(x * y) = \rho(x) * y$ for any $x, y \in X$. A quandle with a good involution is called a *symmetric* quandle. A kei is a symmetric quandle with $\rho = \mathrm{id}$ (in this case ρ is said to be trivial). Symmetric quandles have been used for unoriented knots and non-orientable surface-knots.

Symmetric quandles with non-trivial good involution have been hard to find. Other than computer calculations, very few constructions have been known. In [15, 16], non-trivial good involutions were defined on dihedral quandles of even order, which are not connected. Infinitely many symmetric connected quandles were constructed in [5] as extensions of odd order dihedral quandles: For each odd $2n+1$ ($n \in \mathbb{Z}$, $n > 0$), a symmetric connected quandle of order $(2n+1)2^{2n+1}$ was given, that are not keis. Here we use Galkin quandles to construct more symmetric quandles.

Proposition 5.13 *For any positive integer n, there exists a symmetric connected quandle of order $6n$, that is not involutory.*

Proof. We show that if an abelian group A has an element $c \in A$ of order 2, then $G(A,c)$ is a symmetric quandle. (A finite abelian group A has an element of order 2 if and only if $|A|$ is even.) Note that $G(A,c)$ is not involutory by Corollary 5.12.

Define an involution $\rho : \mathbb{Z}_3 \times A \to \mathbb{Z}_3 \times A$ by $\rho(x,a) = (x, a+c)$, where $c \in A$ is a fixed element of order 2 and $x \in \mathbb{Z}_3$, $a \in A$. The map ρ is an involution. It satisfies the required conditions as we show below. For $x, y \in \mathbb{Z}_3$, we have

$$\begin{aligned} (x,a) * \rho(y,b) &= (x,a) * (y, b+c) \ = \ (2y-x, -a+\mu(x-y)(b+c)+\tau(x-y), \\ (x,a) \,\bar{*}\, (y,b) &= (2y-x, -a+\mu(y-x)b+\tau(y-x)), \end{aligned}$$

where the last equality follows from the proof of Proposition 5.11. If $x = y$, then $\mu(x-y) = 2 = \mu(y-x)$ and $\tau(x-y) = 0 = \tau(y-x)$, and the above two terms are equal. If $x \neq y$, then $\mu(x-y) = -1 = \mu(y-x)$, and exactly one of $\tau(x-y)$ and $\tau(y-x)$ is c and the other is 0, so that the equality holds.

Next we compute

$$\begin{aligned} &\rho(\ (x,a) * (y,b)\ ) \\ &\quad = \ \rho(2y-x, -a+\mu(x-y)b+\tau(x-y)) \ = \ (2y-x, -a+\mu(x-y)b+\tau(x-y)+c), \\ &\rho(x,a) * (y,b) \\ &\quad = \ (x, a+c) * (y,b) \ = \ (2y-x, -a-c+\mu(x-y)b+\tau(x-y)) \end{aligned}$$

and these are equal. □

For equations in Lemma 3.3, we have the following for $\mathbb{Z}_p$.

Lemma 5.14 Let $p > 3$ be a prime and let $\mu : \mathbb{Z}_p \to \mathbb{Z}$ be a function satisfying $\mu(0) = 2$ and

$$\mu(x+y) + \mu(x-y) = \mu(x)\mu(y) \tag{36}$$

for any $x, y \in \mathbb{Z}_p$. Then $\mu(x) = 2$ for all $x \in \mathbb{Z}_p$.

Proof. First we note that we only need to prove $\sum_{x \in \mathbb{Z}_p} \mu(x) \neq 0$. Denote this sum by S. Summing Equation (36) as y runs over $\mathbb{Z}_p$, we have $2S = S\mu(x)$. So if $S \neq 0$, we have $\mu(x) = 2$ for all $x \in \mathbb{Z}_p$.

Assume to the contrary that $S = 0$. Since $\mu(kx)\mu(x) = \mu((k+1)x) + \mu((k-1)x)$, it is easy to see by induction that

$$\mu(x)^k = \frac{1}{2} \sum_{0 \le i \le k} \binom{k}{i} \mu((k-2i)x). \tag{37}$$

(Here we also use the fact that $\mu(-x) = \mu(x)$, which follows from the fact that $\mu(x-y) = \mu(x)\mu(y) - \mu(x+y)$ is symmetric in x and y.) In particular,

$$\mu(x)^{2p} = \frac{1}{2} \sum_{0 \le i \le 2p} \binom{2p}{i} \mu(2(p-i)x).$$

Since $\sum_{x\in\mathbb{Z}_p}\mu(x)=0$, we have

$$\sum_{x\in\mathbb{Z}_p}\mu(x)^{2p}=\Big[2+\binom{2p}{p}\Big]p.$$

Since $\mu(x)=\mu(\frac{x}{2})^2-2$, we have $\mu(x)=-2,-1,2,7,\cdots$.

Case 1. Assume that there exists $0\neq x\in\mathbb{Z}_p$ such that $\mu(x)\geq 7$. Then

$$\Big[2+\binom{2p}{p}\Big]p=\sum_{x\in\mathbb{Z}_p}\mu(x)^{2p}\geq 7^{2p},$$

which is not possible.

Case 2. Assume that $\mu(x)\in\{-2,-1,2\}$ for all $x\in\mathbb{Z}_p$. Let $a_i=|\mu^{-1}(i)|$. Since $\sum_{x\in\mathbb{Z}_p}\mu(x)=0$ and $\sum_{x\in\mathbb{Z}_p}\mu(x)^3=0$, where the second equation follows from (37), we have

$$\begin{cases}-2a_{-2}-a_{-1}+2a_2=0,\\ -8a_{-2}-a_{-1}+8a_2=0.\end{cases}$$

So $a_{-1}=0$, i.e., $\mu(x)=\pm 2$ for all $x\in\mathbb{Z}_p$. Then

$$\sum_{x\in\mathbb{Z}_p}\mu(x)\equiv 2p\equiv 2 \pmod 4,$$

which is a contradiction. □

6 Knot colorings by Galkin quandles

In this section we investigate knot colorings by Galkin quandles. Recall from Lemma 5.4 that any Galkin quandle $G(A,\tau)$ consists of three disjoint subquandles $\{x\}\times A$ for $x\in\mathbb{Z}_3$, and each is a product of dihedral quandles. Also any Galkin quandle has R_3 as a quotient. Thus we look at relations between colorings by dihedral quandles and those by Galkin quandles.

First we present the numbers of n-colorable knots with 12 crossings or less, out of 2977 knots in the knot table from [6], for comparison with Table 1. These are for dihedral quandles and their products that may be of interest and relevant for comparisons.

R_3: 1084,	R_5: 670,	R_7: 479,	R_{11}: 285,	R_{15}: 1512,	R_{17}: 192,
R_{19}: 159,	R_{21}: 1386,	R_{23}: 128,	R_{29}: 97	R_{31}: 87,	R_{33}: 1260.

Remark 6.1 We note that many rig Galkin quandles in Table 1 have the same number (1084) of non-trivially colorable knots as the number of 3-colorable knots. We make a few observations on these Galkin quandles.

By Lemma 5.5, a Galkin quandle has R_3 as a subquandle if $\tau=0$ or 3 divides $|A|$, and among rig Galkin quandles with the number 1084, 17 of them satisfy this condition. Hence any 3-colorable knot is non-trivially colored by these Galkin quandles. The converse is not necessarily true: $G(\mathbb{Z}_5,0)$ has $\tau=0$ but has the number 1512. See Corollary 6.5 for more on these quandles.

The remaining 6 rig Galkin quandles with the number 1084 have $C[6,2]$ as a subquandle:

$$C[12,5],\ C[12,9],\ C[24,28],\ C[24,29],\ C[24,31],\ C[24,33].$$

It was conjectured [5] that if a knot is 3-colorable, then it is non-trivially colored by $C[6,2]$ ($\tilde{R}_3$ in their notation). It is also seen that any non-trivial coloring by $C[6,2]$ descends to a non-trivial 3-coloring via the surjection $C[6,2] \to R_3$, so if the conjecture is true, then any knot is non-trivially colored by these quandles if and only if it is 3-colorable. See also Remarks 6.6 and 6.7.

Proposition 6.2 *Let K be a knot with a prime determinant $p > 3$. Then K is non-trivially colored by a finite Galkin quandle $G(A,\tau)$ if and only if p divides $|A|$.*

Proof. Let K be a knot with the determinant that is a prime $p > 3$. By Fox's theorem [10], for any prime p, a knot is p-colorable if and only if its determinant is divisible by p. Hence K is p-colorable, and not 3-colorable.

Let $G(A,\tau)$ be any Galkin quandle and $\mathcal{C} : \mathcal{A} \to G(A,\tau)$ be a coloring, where $\mathcal{A}$ is the set of arcs of a knot diagram of K. By the surjection $r : G(A,\tau) \to R_3$, the coloring $\mathcal{C}$ induces a coloring $r \circ \mathcal{C} : \mathcal{A} \to R_3$. Since K is not 3-colorable, it is a trivial coloring, and therefore, $\mathcal{C}(\mathcal{A}) \subset r^{-1}(x)$ for some $x \in R_3$. The subquandle $r^{-1}(x)$ for any $x \in R_3$ is an Alexander quandle $\{x\} \times A$ with the operation $(x,a) * (x,b) = (x, 2b-a)$, so that it is a product of dihedral quandles $\{x\} \times A = R_{q_1} \times \cdots \times R_{q_k}$ for some positive integer k and prime powers q_j, $j = 1, \ldots, k$ (Lemma 5.4). It is known that the number of colorings by a product quandle $X_1 \times \cdots \times X_k$ is the product of numbers of colorings by X_i for $i = 1, \ldots, k$. It is also seen that a knot is non-trivially colored by R_{p^k} for a prime p if and only if it is p-colorable. Hence K is non-trivially colored by $\{x\} \times A$ if and only if one of $q_1, \ldots, q_k$ is a power of p. □

Corollary 6.3 *For any positive integer n not divisible by 3 and any finite Galkin quandle $G(A,\tau)$, all 2-bridge knots with the determinant n have the same number of colorings by $G(A,\tau)$.*

Proof. Let K be a two-bridge knot with the determinant $n = p_1^{m_1} \cdots p_\ell^{m_\ell}$ (in the prime decomposition form), where $p_i \neq 3$ for $i = 1, \ldots, \ell$, and let $A = R_{q_1} \times \cdots \times R_{q_k}$ be the decomposition for prime powers, as a quandle. By Fox's theorem [10], for a prime p, K is p-colorable if and only if p divides the determinant of K. Hence K is p_i-colorable for $i = 1, \ldots, \ell$, and not 3-colorable. By the proof of Proposition 6.2, the number of colorings by a Galkin quandle $G(A,\tau)$ of K is determined by the number of colorings by the dihedral quandles R_{q_j} that are factors of A.

The double branched cover $M_2(K)$ of the 3-sphere $\mathbb{S}^3$ along a 2-bridge knot K is a lens space ([27], for example) and its first homology group $H_1(M_2(K), \mathbb{Z})$ is cyclic. If the determinant of K is n then it is isomorphic to $\mathbb{Z}_n$ ([19], for example). It is known [25] that the number of colorings by R_{q_j} is equal to the order of the group $(\mathbb{Z} \oplus H_1(M_2(K), \mathbb{Z})) \otimes \mathbb{Z}_{q_j}$, which is determined by n and q_j alone. □

Example 6.4 Among knots with 8 crossings or less, the following sets of knots have the same numbers of colorings by all finite Galkin quandles from Corollary 6.3: $\{4_1, 5_1\}$ (determinant 5), $\{5_2, 7_1\}$ (7), $\{6_2, 7_2\}$ (11), $\{6_3, 7_3, 8_1\}$ (13), $\{7_5, 8_2, 8_3\}$ (17), $\{7_6, 8_4\}$ (19), $\{8_6, 8_7\}$ (23), $\{8_8, 8_9\}$ (25), $\{8_{12}, 8_{13}\}$ (29). This exhausts such sets of knots up to 8 crossings.

Computer calculations show that the set of knots up to 8 crossings with determinant 9 is $\{6_1, 8_{20}\}$, and these have different numbers of colorings by some Galkin quandles. The determinant was looked up at KnotInfo [6].

There are two knots (7_4 and 8_{21}, up to 8 crossings) with determinant 15. They can be distinguished by the numbers of colorings by some Galkin quandles, according to computer calculations.

Corollary 6.5 *Let p be an odd prime. Then a knot K is non-trivially colored by the Galkin quandle $G(\mathbb{Z}_p, 0)$ if and only if it is $3p$-colorable.*

Proof. Suppose it is $3p$-colorable, then it is non-trivially colored by R_{3p} which is isomorphic to $R_3 \times R_p$, so that it is either 3-colorable or p-colorable. If K is 3-colorable, then since $G(\mathbb{Z}_p, 0)$ has R_3 as a subquandle by Lemma 5.5, K is non-trivially colored by $G(\mathbb{Z}_p, 0)$. If K is p-colorable, then since $G(\mathbb{Z}_p, 0)$ has $\{0\} \times R_p$ as a subquandle by Lemma 5.4, K is non-trivially colored by $G(\mathbb{Z}_p, 0)$.

Suppose a knot K is non-trivially colored by $G(\mathbb{Z}_p, 0)$, where p is an odd prime. If K is 3-colorable, then it is $3p$-colorable, and we are done. If K is not 3-colorable, then by the proof of Proposition 6.2, K is non-trivially colored by $\{x\} \times R_p$, where $x \in \mathbb{Z}_3$. Hence K is p-colorable, and so $3p$-colorable. $\square$

Remark 6.6 According to computer calculations, the following sets of Galkin quandles (in the numbering of Table 1) have the same numbers of colorings for all 2977 knots with 12 crossings or less. Thus we conjecture that it is the case for all knots. If a Galkin quandle does not appear in the list, then it means that it has different numbers of colorings for some knots, comparing to other Galkin quandles. The numbers of colorings are distinct for distinct sets listed below as well.

$$\begin{aligned}
&\{C[6,1], C[6,2]\}, \{C[12,5], C[12,6]\}, \{C[12,8], C[12,9]\}, \{C[18,1], C[18,4]\},\\
&\{C[18,5], C[18,8]\}, \{C[24,27], C[24,28]\}, \{C[24,29], C[24,30], C[24,31]\},\\
&\{C[24,38], C[24,39]\}, \{C[30,12], C[30,14]\}, \{C[30,13], C[30,15]\}.
\end{aligned}$$

Remark 6.7 In contrast to the preceding remark, if we relax the requirement of coloring the same number of times, and instead consider two quandles equivalent if each colors the same knots non-trivially (among these 2977 knots), then we get the following 4 equivalence classes.

$$\begin{aligned}
&\{C[3,1], C[6,1], C[6,2], C[9,2], C[9,6], C[12,5], C[12,6], C[12,8], C[12,9], C[18,1], C[18,4],\\
&C[18,5], C[18,8], C[24,27], C[24,28], C[24,29], C[24,30], C[24,31], C[24,38], C[24,39], C[27,2],\\
&C[27,12], C[27,13], C[27,23], C[27,55]\},\\
&\{C[12,7], C[24,32], C[24,33]\},\\
&\{C[15,5], C[30,12], C[30,14]\},\\
&\{C[15,6], C[30,13], C[30,15]\}.
\end{aligned}$$

Thus we conjecture that it is the case for all knots. Of these, the first family with many elements consists of quandles with $C[3,1]$, $C[6,1]$ or $C[6,2]$ as a subquandle. Hence, in fact, the conjecture about this family follows from the conjecture about $\{C[6,1], C[6,2]\}$ in the preceding remark.

Remark 6.8 Also in contrast to Remark 6.6, there exists a virtual knot K (see, for example, [18]) such that the numbers of colorings by $C[6,1]$ and $C[6,2]$ are distinct. A virtual knot K with the following property was given in [5], Remark 4.6: K is 3-colorable, but does not have a non-trivial coloring by $C[6,2]$. Since $C[6,1]$ has R_3 as a subquandle, this virtual knot K has a non-trivial coloring by $C[6,1]$. Hence the numbers of colorings by $C[6,1]$ and $C[6,2]$ are distinct for K. Thus we might conjecture that for any pair of non-isomorphic Galkin quandles, there is a virtual knot with different numbers of colorings.

Remark 6.9 For any finite Galkin quandle $G(A,\tau)$, there is a knot K with a surjection $\pi_Q(K) \to G(A,\tau)$ from the fundamental quandle $\pi_Q(K)$. In fact, a connected sum of trefoil can be taken as K as follows (see, for example, [27] for connected sum).

First we take a set of generators of $G(A,\tau)$ as follows. Let $A = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, where $k, n_1, \ldots, n_k$ are positive integers such that n_i divides n_{i+1} for $i = 1, \ldots, k$. Let $S = \{(x, e_i) \mid x \in \mathbb{Z}_3, i = 0, \ldots, k\}$, where $e_0 = 0 \in A$ and $e_i \in A$ $(i = 1, \ldots, k)$ is an elementary vector $[0, \ldots, 0, 1, 0, \ldots, 0] \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ with a single 1 at the i-th position. Note that R_n is generated by $0, 1$ as $0 * 1 = 2$, $1 * 2 = 3$, and inductively, $i * (i+1) = i+2$ for $i = 0, \ldots, n-2$. Since $\{x\} \times A$ is isomorphic to a product of dihedral quandles for each $x \in \mathbb{Z}_3$, S generates $G(A,\tau)$.

For a 2-string braid σ_1^3 whose closure is trefoil (see Figure 2), we note that if $x \neq y \in \mathbb{Z}_3$, then for any $a, b \in A$, the pair of colors $(x,a), (y,b) \in G(A,\tau)$ at top arcs extends to the bottom, i.e., the bottom arcs receive the same pair. This can be computed directly.

For copies of trefoil, we assign pairs $[(0, e_0), (x, e_i)]$ as colors where $x = 1, 2$ and $i = 0, \ldots k$, and take connected sums on the portion of the arcs with the common color $(0, e_0)$. Further we take pairs $[(0, e_j), (1, e_0)]$ for $j = 1, \ldots, k$, for example, and take connected sum on the arcs with the common color $(1, e_0)$, to obtain a connected sum of trefoil with all elements of S used as colors. Such a coloring gives rise to a quandle homomorphism $\pi_Q(K) \to G(A,\tau)$ whose image contains generators S, hence defines a surjective homomorphism.

References

[1] Andruskiewitsch, N.; Graña, M., *From racks to pointed Hopf algebras*, Adv. in Math., 178 (2003), 177–243.

[2] Carter, J.S.; Elhamdadi, M.; Nikiforou, M.A.; Saito, M., *Extensions of quandles and cocycle knot invariants,* J. of Knot Theory and Ramifications, 12 (2003) 725–738.

[3] Carter, J.S.; Jelsovsky, D.; Kamada, S.; Langford, L.; Saito, M., *Quandle cohomology and state-sum invariants of knotted curves and surfaces,* Trans. Amer. Math. Soc., 355 (2003), 3947–3989.

[4] Carter, J.S.; Kamada, S.; Saito, M., Surfaces in 4-space, Encyclopaedia of Mathematical Sciences, Vol. 142, Springer Verlag, 2004.

[5] Carter, J.S., Oshiro, K., Saito, M., *Symmetric extensions of dihedral quandles and triple points of non-orientable surfaces,* Topology and its appl. 157 (2010), 857–869.

[6] Cha, J. C.; Livingston, C., *KnotInfo: Table of Knot Invariants,* http://www.indiana.edu/∼knotinfo, May 26, 2011.

[7] Clark, W.E.; Hou, X., *Galkin Quandles, Pointed Abelian Groups, and Sequence A*000712, to appear.

[8] Fenn, R.; Rourke, C., *Racks and links in codimension two*, J. Knot Theory Ramifications 1 (1992), 343–406.

[9] Fenn, R.; Rourke, C.; Sanderson, B., *Trunks and classifying spaces,* Appl. Categ. Structures 3 (1995), no. 4, 321–356.

[10] Fox, R.H., *A Quick Trip Through Knot Theory*, in Topology of Manifolds, Prentice Hall (1962).

[11] Galkin, V. M., *Quasigroups*, Itogi Nauki i Tekhniki, Algebra. Topology. Geometry, Vol. 26 (Russian), 344, 162, Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow (1988), Translated in J. Soviet Math. 49 (1990), no. 3, 941967.

[12] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.12; 2008. (http://www.gap-system.org).

[13] Hillar, C.J.; Rhea, D.L., *Automorphisms of finite abelian groups*, Amer. Math. Monthly, 114 (2007), 917 – 923.

[14] Joyce, D., *A classifying invariant of knots, the knot quandle,* J. Pure Appl. Alg., 23 (1983), 37–65.

[15] Kamada, K., *Quandles with good involutions, their homologies and knot invariants*, in: Intelligence of Low Dimensional Topology 2006, Eds. J. S. Carter et. al., World Scientific Publishing Co. (2007), 101–108.

[16] Kamada, S.; Oshiro, K., *Homology groups of symmetric quandles and cocycle invariants of links and surface-links*, Trans. Amer. Math. Soc. 362 (2010), 5501–5527.

[17] Maple 15- Magma package-copywrite by Maplesoft, a division of Waterloo Maple, Inc, 1981–2011.

[18] Kauffman, L.H., *Virtual knot theory*, European J. Comb. (1999) Vol. 20, 663–690.

[19] Lickorish, W.B.R., *An introduction to knot theory*, Graduate Texts in Mathematics, 175, Springer-Verlag, New York, 1997.

[20] Matveev, S., *Distributive groupoids in knot theory.* (Russian) Mat. Sb. (N.S.) 119(161) (1982), no. 1, 78–88, 160.

[21] McCune, W., *Prover9 and Mace4*, http://www.cs.unm.edu/∼mccune/Prover9, 2005–2010.

[22] Nelson, S., *Classification of finite Alexander quandles,* Topology Proceedings 27 (2003), 245–258.

[23] The On-Line Encyclopedia of Integer Sequences, http://oeis.org/.

[24] Pflugfelder, H.O., *Quasigroups and loops: introduction*, Heldermann Verlag, 1990.

[25] Przytycki, J.H., 3*-colorings and other elementary invariants of knots,* Banach Center publications vol. 42, knot theory (1998), 275–295.

[26] Ranum, A., *The group of classes of congruent matrices with application to the group of isomorphisms of any abelian group*, Trans. Amer. Math. Soc. 8 (1907), 71 – 91.

[27] Rolfsen, D., *Knots and Links*, Publish or Perish Press, Berkley, 1976.

[28] Takasaki, M., *Abstraction of symmetric transformation,* (in Japanese), Tohoku Math. J. 49 (1942/3), 145–207.

[29] Toyoda, K., *On axioms of linear functions*, Proceedings of the Imperial Academy, 17(7) (1941), 221–227.

[30] Vendramin, L., *RIG - a GAP package for racks and quandles,* May 22, 2011, http://code.google.com/p/rig/.

[31] Vendramin, L., *On the classification of quandles of low order*, arXiv:1105:5341, 28 May 2011.