SUBQUANDLES OF AFFINE QUANDLES

PŘEMYSL JEDLIČKA, AGATA PILITOWSKA, DAVID STANOVSKÝ, AND ANNA ZAMOJSKA-DZIENIO

Abstract. A quandle will be called quasi-affine, if it embeds into an affine quandle. Our main result is a characterization of quasi-affine quandles, by group-theoretic properties of their displacement group, by a universal algebraic condition coming from the commutator theory, and by an explicit construction over abelian groups. As a consequence, we obtain efficient algorithms for recognizing affine and quasi-affine quandles, and we enumerate small quasi-affine quandles. We also prove that the "abelian implies quasi-affine" problem of universal algebra has affirmative answer for the class of quandles.

1. Introduction

Affine quandles (also called Alexander quandles) play a prominent role in quandle theory, both from the algebraic perspective [1, 7, 10, 11, 12, 13], and in applications in knot theory, due to a close connection between affine colorings and the Alexander invariant [2, 5, 15]. In the present paper, we look at the structure and abstract properties of quandles that embed into affine quandles, that is, that are isomorphic to a subquandle of an affine quandle. We will call such quandles *quasi-affine*. For example, free medial quandles are quasi-affine, but not affine [14].

At the moment, our motivation is purely algebraic, with emphasis on computational aspects. What is their structure? How many are there? How to recognize them? We will present both a structural theorem, and a computationally feasible characterization of quasi-affine quandles (Theorem 2.2). The former goal is achieved using a special kind of central extension (Definition 4.1). Together with a convenient isomorphism theorem (Theorem 8.7), this allows fairly efficient enumeration (Section 9). We also present polynomial-time algorithms (subquadratic with respect to the input size) for recognition of affine and quasi-affine quandles (Algorithms 7.1 and 7.4). The key property behind the results is abelianness and semiregularity of the displacement group.

A secondary motivation for our study comes from universal algebra. One of the major projects in universal algebra is to determine abstract conditions under which a general algebraic structure embeds into an affine one; formally, when it is a subreduct of a module [24, 25]. Such algebras are also called quasi-affine. In particular, a longstanding open problem asks, whether every idempotent algebraic structure satisfying certain syntactic condition called *abelianness* is quasi-affine [16]. We confirm the conjecture for the class of quandles. As far as we know, after [22], this is only the second result when the problem is confirmed for a broad class of idempotent algebras failing every non-trivial Mal'tsev condition.

Our results are also interesting in the context of the theory of *modes* [20], which develops its own theory of linear representations (medial quandles are examples of modes).

Date: August 7, 2017.

2010 *Mathematics Subject Classification.* 20N02, 57M27, 08A05, 15A78.

Key words and phrases. Quandles, medial quandles, affine quandles, commutator theory, abelian algebras, quasi-affine algebras, quasi-affine modes.

Our joint research started within the framework of the Czech-Polish cooperation grants 7AMB13PL013 and 8829/R13/R14. The second and the fourth authors were supported by the statutory grant of the Warsaw University of Technology 504/02476/1120. The third author was partly supported by the Czech Science Foundation grant 13-01832S.

As a byproduct, we prove several new results for affine quandles, complementing existing theory [9, 11]. Our main tool, Theorem 2.3, characterizes affine quandles in a way similar to Theorem 2.2, and is of independent interest. In particular, our characterization of the displacement groups results in an algorithm for recognition of affine quandles which is a tremendous improvement over the brute-force method of [18].

Affine quandles are *medial*, and so are their subquandles. We could therefore build upon the structure theory developed in [13], where we represented medial quandles by certain heterogeneous affine structure. However, it turned out that our theory was easier to develop from scratch, because meshes of quasi-affine quandles are very symmetric and thus better viewed as extensions. We will use the results of [13] in the final sections: the isomorphism theorem for quasi-affine quandles will be proved by specializing the (more general) isomorphism theorem for affine meshes.

The paper is organized as follows. In Section 2, we recall some of the quandle theory needed in the paper, and we formulate our main results, Theorems 2.2 and 2.3. Section 3 contains an auxiliary module-theoretic result, called the *Hou-Šťovíček extension lemma*. We see it as *the* module-theoretic principle behind the structure theory of affine quandles. In Section 4, we introduce semiregular extensions, a concept used to represent quasi-affine quandles, and prove a few elementary properties. Section 5 relates the universal algebraic and quandle theoretic principles. In Section 6, we prove Theorems 2.2 and 2.3. In the finite case, the somewhat cumbersome characterization of affine quandles can be replaced by a more esthetic condition; this is the subject of Theorem 6.2. We also include several interesting examples and counterexamples related to the abstract conditions that appear throughout the paper. Section 7 contains the recognition algorithms based on our characterizing theorems, including their complexity analysis. In Section 8, we relate semiregular extensions to the affine meshes of [13], and prove the isomorphism theorem for semiregular extensions. In the last section, we apply it to enumerate small quasi-affine quandles.

The paper is aimed at both quandlists and universal algebraists. The proof of the main theorems does not rely on the universal algebraic concepts, and thus Section 5 could be safely skipped. Nevertheless, we advise to take this interesting abstraction into account. A universal algebraic background can be learnt from [3]. Our approach to quandles is best summarized in the introductory parts of [12]. A comprehensive study of affine quandles can be found in [10, 11], an alternative approach was developed by Holmes in her Master's thesis [9]. The present work was influenced by some of her ideas presented in the thesis.

2. Terminology and main results

2.1. **Quandles.** All unproved results stated in this section can be found in the introductory part of [12] (using the present notation), and most of them also elsewhere (often in a different notation).

We will write mappings acting on the left, hence conjugation in groups will be denoted by $x^y = yxy^{-1}$, and consequently, the commutator will be defined as $[x,y] = y^x y^{-1} = xyx^{-1}y^{-1}$.

A *quandle* is an algebraic structure $Q = (Q, *)$ which is *idempotent* (it satisfies the identity $x * x = x$), *uniquely left divisible* (for every x, y, there is a unique z such that $x * z = y$, to be denoted $z = x\backslash y$), and *left distributive* (it satisfies the identity $x * (y * z) = (x * y) * (x * z)$). The mappings $L_x : Q \to Q$, $L_x(y) = x * y$, will be called *left translations*. It follows from the quandle axioms that all left translations are automorphisms of Q. We will often drop the adjective "left". For universal-algebraic purposes, we will regard left division as a basic operation, i.e., it can be used in terms.

Two important permutation groups are associated to every quandle: the (left) *multiplication group*, generated by all (left) translations,

$$\mathrm{LMlt}(Q) = \langle L_a : \ a \in Q \rangle \leq \mathrm{Aut}(Q),$$

and its subgroup, the *displacement group*, defined by

$$\mathrm{Dis}(Q) = \langle L_a L_b^{-1} : \ a, b \in Q \rangle \leq \mathrm{LMlt}(Q).$$

Both groups have the same orbits of the natural action on Q, to be called *orbits* of the quandle Q, and denoted

$$Qe = \{\alpha(e) : \ \alpha \in \mathrm{LMlt}(Q)\} = \{\alpha(e) : \ \alpha \in \mathrm{Dis}(Q)\}.$$

Orbits are subquandles of Q. They form a block system, to be called the *orbit decomposition* of Q.

A quandle is called *medial* if it satisfies the identity $(x * y) * (u * v) = (x * u) * (y * v)$. This is equivalent to abelianness of the displacement group. Therefore, if Q is medial, $\alpha \in \mathrm{Dis}(Q)$ and $x, y \in Q$, we have $\alpha^{L_y^{-1} L_x} = \alpha$, and thus

$$\alpha^{L_x} = \alpha^{L_y}. \tag{2.1}$$

Let $(A, +)$ be an abelian group, f its automorphism, and define an operation on the set A by

$$a * b = (1 - f)(a) + f(b).$$

Then $(A, *)$ is a medial quandle, to be denoted $\mathrm{Aff}(A, f)$, and called *affine* over the group $(A, +)$. Here 1 refers to the identity mappings, hence $g = 1 - f$ is the mapping $g(x) = x - f(x)$. A product of two affine quandles $Q = \mathrm{Aff}(A, f)$ and $R = \mathrm{Aff}(B, g)$ is affine since $Q \times R = \mathrm{Aff}(A \times B, f \times g)$. Affine quandles with $f = 1$ will be called *projection quandles*, since the operation is the right projection, $a * b = b$. The projection quandle of size k (possibly infinite) will be denoted by $\mathrm{Proj}(k)$.

Following the universal algebraic terminology, quandles embeddable into affine quandles will be called shortly *quasi-affine*. (Contrary to universal algebra, quandle-theoretic definition of affineness is weaker. In universal algebra, an algebraic structure is called affine if and only if it is polynomially equivalent to a module; affine quandles are only assumed to be reducts of modules.)

We will say that $\mathrm{Dis}(Q)$ is *tiny* if $\mathrm{Dis}(Q) = \{L_x L_e^{-1} : \ x \in Q\}$ for some $e \in Q$. Affine quandles have tiny displacement groups (the converse is not true): for $Q = \mathrm{Aff}(A, f)$ we have

$$\mathrm{Dis}(Q) = \{x \mapsto a + x : \ a \in \mathrm{Im}(1 - f)\} = \{L_x L_0^{-1} : x \in Q\},$$

since $L_a L_b^{-1}(x) = (1 - f)(a - b) + x$. Hence $\mathrm{Dis}(Q) \simeq \mathrm{Im}(1 - f)$, and the orbits of Q are the cosets of $\mathrm{Im}(1 - f)$.

2.2. **Multitransversals.** Informally, a *multiset* is a generalization of the notion of a set where elements can repeat. Tuples can be turned into multisets, forgetting the indexing. Multisets will be denoted by double brackets $\{\{...\}\}$.

A multitransversal for a block system is a multiset which takes from each block the same amount of elements, i.e., a multiset T such that $|T \cap B_1| = |T \cap B_2|$ for every pair of blocks B_1, B_2; the size of the intersection will be called the *multiplicity* of T. If G is a group and H its subgroup, then by a (left) multitransversal of G/H we mean a multitransversal of the block system $\{a + H : a \in G\}$.

Lemma 2.1. *Let G be a group, $\varphi \in \mathrm{End}(G)$, and let T be a left transversal of $G/\mathrm{Im}(\varphi)$. Then $\varphi(T)$, as a multiset, is a left multitransversal of $\mathrm{Im}(\varphi)/\mathrm{Im}(\varphi^2)$. The multiplicity of $\varphi(T)$ is equal to $|\mathrm{Ker}(\varphi)/\mathrm{Ker}(\varphi) \cap \mathrm{Im}(\varphi)|$.*

Proof. Let $t, s \in T$. We have $\varphi(t)\varphi(s)^{-1} \in \mathrm{Im}(\varphi^2)$ if and only if $\varphi(ts^{-1}) = \varphi^2(a)$ for some $a \in G$. Now $\varphi(ts^{-1}) = \varphi^2(a)$ if and only if $\varphi(ts^{-1}\varphi(a)^{-1}) = 1$, that is, if and only if $ts^{-1}\varphi(a)^{-1} \in \mathrm{Ker}(\varphi)$. Consequently, $\varphi(t)\varphi(s)^{-1} \in \mathrm{Im}(\varphi^2)$ if and only if $ts^{-1} \in \mathrm{Ker}(\varphi) \cdot \mathrm{Im}(\varphi)$. Each block of $G/(\mathrm{Ker}(\varphi) \cdot \mathrm{Im}(\varphi))$ contains the same amount of blocks of $G/\mathrm{Im}(\varphi)$, and thus the same amount of elements of T. Looking at the block $\mathrm{Ker}(\varphi) \cdot \mathrm{Im}(\varphi)$, we see that the multiplicity is $|(\mathrm{Ker}(\varphi) \cdot \mathrm{Im}(\varphi))/\mathrm{Im}(\varphi)|$. By the second isomorphism theorem, this is equal to $|\mathrm{Ker}(\varphi)/\mathrm{Ker}(\varphi) \cap \mathrm{Im}(\varphi)|$. □

2.3. **Main results.** Now we can formulate the main results, the characterization theorems for affine and quasi-affine quandles.

Recall that a permutation group G acting on a set X is called *semiregular* (the terms *free* or *fixpoint-free* are also used in literature) if non-trivial permutations from G are regular, i.e., have no fixed points. In other words, if $g(x) \neq x$ for every $1 \neq g \in G$ and $x \in X$.

The *semiregular extension*, $\mathrm{Ext}(A, f, \bar{d})$, will be defined in Section 4. It is a particular type of a central extension of a projection quandle over the affine quadle $\mathrm{Aff}(A, f)$ (for more information on centrality see Remark 4.10).

In condition (4), abelianness refers to a certain syntactic condition, to be explained in Section 5. It is a generalization of the idea that a group G is abelian if and only if the diagonal of G^2 forms a normal subgroup.

Theorem 2.2. *The following statements are equivalent for a quandle Q:*

(1) *Q is quasi-affine;*
(2) $\mathrm{Dis}(Q)$ *is abelian and semiregular;*
(3) *Q is isomorphic to $\mathrm{Ext}(A, f, \bar{d})$ for some abelian group A, its automorphism f and some tuple $\bar{d} = (d_i : i \in I)$ of elements of A;*
(4) *Q is abelian (in the sense of* [8]*).*

Theorem 2.3. *The following statements are equivalent for a quandle Q:*

(1) *Q is affine;*
(2) $\mathrm{Dis}(Q)$ *is abelian, semiregular and the multiset $\{\{L_a L_e^{-1} : a \in T\}\}$ is balanced for every $e \in Q$ and every transversal T of the orbit decomposition.*
(2') $\mathrm{Dis}(Q)$ *is abelian, semiregular and the multiset $\{\{L_a L_e^{-1} : a \in T\}\}$ is balanced for some $e \in Q$ and some transversal T of the orbit decomposition.*
(3) *Q is isomorphic to $\mathrm{Ext}(A, f, \bar{d})$ for some abelian group A, its automorphism f and some balanced tuple $\bar{d} = (d_i : i \in I)$ of elements of A.*

A multiset $\{\{L_a L_e^{-1} : a \in T\}\}$ is called *balanced* if it is a multitransversal of $\mathrm{Dis}(Q)/[\mathrm{Dis}(Q), L_e]$. A tuple $\bar{d}$ is called *balanced*, if it is a multitransversal of $A/\mathrm{Im}(1-f)$. As we shall see in Theorem 6.2, if Q is finite, than these two balancedness conditions are equivalent to the fact that the multiplication table of Q is balanced in a particularly nice way.

Proving the implications (1) $\Rightarrow$ (2) is fairly straightforward, and the semiregular extensions are designed in a way that the implications (2) $\Rightarrow$ (3) also prove smoothly. The real work is proving the implications (3) $\Rightarrow$ (1). In either case, we are given a particular semiregular extension Q, and we need to find an affine representation, that is, a concrete group A and its automorphism f such that Q is isomorphic to, resp. embeds into, $\mathrm{Aff}(A, f)$. This is not as easy as one might expect. One of the difficulties is that the group A is not determined uniquely, not even in the affine case. Our method relies on the Hou-Šťovíček extension lemma, which provides a suitable group in the affine case. Therefore, we first prove Theorem 2.3, and then obtain Theorem 2.2 as a corollary.

Our proof of the Hou-Šťovíček extension lemma is not constructive: the abelian group is proved to exist, but no concrete description is given. At the moment, we do not know an explicit construction of the affine representation. This has an algorithmic consequence: we are able to check efficiently whether a given multiplication table defines an affine (or quasi-affine) quandle, but we do not know an efficient way to determine the actual group and automorphism.

The universal algebraic perspective also suggests that calculating an explicit affine representation might be difficult: it was so for many of the general results. For example, the quasi-affine representation proved in [22] for differential modes is also non-constructive, using the indirect syntactic method of [24].

3. The Hou-Šťovíček extension lemma

Lemma 3.1 (Hou-Šťovíček extension lemma)**.** *Let A be an abelian group and φ its endomorphism. Then there exist an abelian group $E \geq A$ and an epimorphism $\psi : E \to A$ such that $\psi|_A = \varphi$ and $\psi/A : E/A \simeq A/\mathrm{Im}(\varphi)$.*

Here ψ/A is defined by $x + A \mapsto \psi(x) + \mathrm{Im}(\varphi)$. It is a well defined homomorphism, because $x - y \in A$ if and only if $\psi(x) - \psi(y) \in \mathrm{Im}(\varphi)$.

A similar statement was originally proved by Hou [11, Theorem 4.2] under the assumption that A is finite, and used in his enumeration of small affine quandles (or $\mathbb{Z}[t, t^{-1}]$-modules, from his perspective). Later, it found use in Holmes' alternative approach to affine quandles [9], and in the present paper, it serves as *the* underlying result behind finding the affine representation in the proof of the main theorems.

Šťovíček deserves credit for pointing out that the statement is actually a special case of a classical result in homological algebra, a characterization of hereditary rings in terms of the Ext^2 functor, and that it holds without the finiteness assumption [23]. In fact, the statement is true for modules over any hereditary ring, not just for $\mathbb{Z}$-modules. A ring R is called (left) *hereditary* if submodules of projective (left) R-modules are projective, or equivalently, if $\mathrm{Ext}^2(A, B) = 0$ for every pair of (left) R-modules A, B [21, Chapter 8]. The ring of integers is hereditary, because subgroups of free abelian groups are free.

Lemma 3.2 (Hou-Šťovíček extension lemma, a general version)**.** *Let R be a hereditary ring, A an R-module and φ its endomorphism. Then there exist an R-module $E \geq A$ and an epimorphism $\psi : E \to A$ such that $\psi|_A = \varphi$ and $\psi/A : E/A \simeq A/\mathrm{Im}(\varphi)$.*

Proof. Consider an arbitrary short exact sequence

$$0 \longrightarrow K \longrightarrow E \xrightarrow{\varphi} I \longrightarrow 0.$$

Applying the $\mathrm{Hom}(X, -)$ functor, we obtain an exact sequence

$$\ldots \longrightarrow \mathrm{Ext}^1(X, E) \xrightarrow{\mathrm{Hom}(X,\varphi)} \mathrm{Ext}^1(X, I) \longrightarrow \mathrm{Ext}^2(X, K) \longrightarrow \ldots$$

(see [21, Corollary 6.46]). Over a hereditary ring, $\mathrm{Ext}^2(X, K) = 0$, and thus $\mathrm{Hom}(X, \varphi)$ is onto.

Applying the general idea to the exact sequence

$$0 \longrightarrow \mathrm{Ker}(\varphi) \longrightarrow A \xrightarrow{\varphi} \mathrm{Im}(\varphi) \longrightarrow 0$$

and $X = A/\mathrm{Im}(\varphi)$, we obtain that $\mathrm{Ext}^1(A/\mathrm{Im}(\varphi), \varphi)$ maps the group $\mathrm{Ext}^1(A/\mathrm{Im}(\varphi), A)$ onto the group $\mathrm{Ext}^1(A/\mathrm{Im}(\varphi), \mathrm{Im}(\varphi))$. Considering a preimage of the exact sequence

$$0 \longrightarrow \mathrm{Im}(\varphi) \longrightarrow A \xrightarrow{\pi} A/\mathrm{Im}(\varphi) \longrightarrow 0,$$

we obtain a module E and homomorphisms i, ρ, ψ such that

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{\rho} & A/\mathrm{Im}(\varphi) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \psi} & & \| & & \\
0 & \longrightarrow & \mathrm{Im}(\varphi) & \xrightarrow{\subseteq} & A & \xrightarrow{\pi} & A/\mathrm{Im}(\varphi) & \longrightarrow & 0
\end{array}$$

is a commutative diagram where the left square is a pushout [21, Lemma 7.28]. Since i is injective (the sequence is exact), we can assume it is an inclusion. Since φ is surjective, so is ψ, as in any pushout. From the left square, we see that $\psi i = \varphi$, i.e., $\psi|_A = \varphi$. From the right square, we see that $\rho(x) = \pi\psi(x) = \psi(x) + \mathrm{Im}(\varphi)$, and since $\mathrm{Ker}(\rho) = A$, we obtain that $\psi/A : E/A \simeq A/\mathrm{Im}(\varphi)$. □

4. Semiregular extensions

Definition 4.1. Let A be an abelian group, f an automorphism of A, I a non-empty set and $d_i \in A$ for $i \in I$. Define an operation on the set $I \times A$ by

$$(i,a) * (j,b) = (j, (1-f)(a) + f(b) + d_i - d_j).$$

It is straightforward to check that the resulting structure $(I \times A, *)$ is a quandle, with

$$(i,a) \backslash (j,b) = (j, (1-f^{-1})(a) + f^{-1}(b - d_i + d_j)).$$

The projection $\pi : I \times A \to I$ is a quandle homomorphism onto the projection quandle over I, and the blocks of $\mathrm{Ker}(\pi)$, as subquandles, are all isomorphic to the affine quandle $\mathrm{Aff}(A, f)$. We will denote the quandle $(I \times A, *)$ by $\mathrm{Ext}(A, f, \bar{d})$, where $\bar{d} = (d_i : i \in I)$, and call it a *semiregular extension over* $\mathrm{Aff}(A, f)$.

The name is justified by the following lemma.

Lemma 4.2. *Let A be an abelian group, f an automorphism of A, $\bar{d} = (d_i : i \in I)$ a tuple of elements from A, and let $Q = \mathrm{Ext}(A, f, \bar{d})$. Then $\mathrm{Dis}(Q)$ is an abelian semiregular group.*

Proof. It is straightforward to calculate that

$$L_{(i,a)} L^{-1}_{(j,b)}(k,c) = (k, c + (1-f)(a-b) + d_i - d_j) = (k, c + t_{i,j,a,b}),$$

where $t_{i,j,a,b} \in A$ is an element of A independent of k, c. We see that all generators of $\mathrm{Dis}(Q)$ act as translations over the abelian group A, therefore, $\mathrm{Dis}(Q)$ is commutative and semiregular. □

A converse also holds: every quandle with an abelian and semiregular displacement group admits a representation as a semiregular extension. An extension $E = \mathrm{Ext}(A, f, \bar{d})$ is called *indecomposable*, if the fibers $\{i\} \times A$ are the orbits of E.

Lemma 4.3. *Let Q be a medial quandle. Let*

$$E = \mathrm{Ext}(\mathrm{Dis}(Q), f, (L_x L_e^{-1} : x \in T)),$$

where $e \in Q$, T is a transversal of the orbit decomposition of Q, and f is the automorphism of $\mathrm{Dis}(Q)$ defined by $f(\alpha) = \alpha^{L_e}$. Then E maps homomorphically onto Q, and if $\mathrm{Dis}(Q)$ is semiregular, then E is indecomposable and isomorphic to Q.

Proof. We have $E = T \times \mathrm{Dis}(Q)$. Define a mapping

$$\Phi : E \to Q, \quad (x, \alpha) \mapsto \alpha(x).$$

It is onto Q, because T is a transversal of the action of $\mathrm{Dis}(Q)$ on Q. We prove that the mapping Φ is a homomorphism:

$$\begin{aligned}
\Phi((x,\alpha) * (y,\beta)) &= \Phi(y, (1-f)(\alpha) + f(\beta) + d_x - d_y) \\
&= (\alpha(\alpha^{-1})^{L_e})\beta^{L_e}(L_x L_e^{-1})(L_y L_e^{-1})^{-1}(y) \\
&= \alpha(\alpha^{-1}\beta)^{L_e} L_x(y) \overset{(2.1)}{=} \alpha(\alpha^{-1}\beta)^{L_x} L_x(y) \\
&= \alpha(x * \alpha^{-1}\beta(y)) = \alpha(x) * \beta(y) = \Phi(x,\alpha) * \Phi(y,\beta).
\end{aligned}$$

Now, $\Phi(x,\alpha) = \Phi(y,\beta)$, i.e., $\alpha(x) = \beta(y)$, if and only if $\beta^{-1}\alpha(x) = y$, which can only happen if x, y are in the same orbit, and since x, y were chosen from a transversal, it can only happen if $x = y$. So, we have $\alpha(x) = \beta(y)$ if and only if $x = y$ is a fixed point of $\beta^{-1}\alpha$. Consequently, if $\mathrm{Dis}(Q)$ is semiregular, the mapping Φ is one-to-one.

Indecomposability follows from the fact that the orbits in Q are $Qx = \{\alpha(x) : \alpha \in \mathrm{Dis}(Q)\}$, and their preimages under Φ are the fibers of E. □

Note that the two lemmas establish the equivalence (2) $\Leftrightarrow$ (3) of Theorem 2.2.

Example 4.4. Consider an affine quandle $Q = \mathrm{Aff}(A, f)$. Then

- $Q = \mathrm{Ext}(A, f, (0))$, hence $\mathrm{Dis}(Q)$ is abelian and semiregular according to Lemma 4.2.
- $Q \simeq \mathrm{Ext}(\mathrm{Im}(1-f), f, ((1-f)(a) : a \in T))$, where T is a transversal of the orbit decomposition, as follows from Lemma 4.3 under the isomorphism $\mathrm{Im}(1-f) \simeq \mathrm{Dis}(Q)$. This extension is indecomposable, the fiber $\{a\} \times \mathrm{Im}(1-f)$ corresponds to the orbit Qa.

Example 4.5. There are three quasi-affine quandles of order four, and all of them are affine:

$$\begin{aligned}\mathrm{Aff}(\mathbb{Z}_4, 1) &\simeq \mathrm{Aff}(\mathbb{Z}_2^2, 1) \simeq \mathrm{Ext}(\mathbb{Z}_1, 1, (0,0,0,0)),\\ \mathrm{Aff}(\mathbb{Z}_4, -1) &\simeq \mathrm{Aff}(\mathbb{Z}_2^2, \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)) \simeq \mathrm{Ext}(\mathbb{Z}_2, 1, (0,1)),\\ &\mathrm{Aff}(\mathbb{Z}_2^2, \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)) \simeq \mathrm{Ext}(\mathbb{Z}_2^2, \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right), (0)).\end{aligned}$$

Consider a semiregular extension $\mathrm{Ext}(A, f, (d_1, \dots, d_k))$ such that $|A| \cdot k = 4$. If $A = \mathbb{Z}_1$, we have only one option, $\mathrm{Ext}(\mathbb{Z}_1, 1, (0,0,0,0))$, which is a projection quandle. If $A = \mathbb{Z}_2$, we have four options $\mathrm{Ext}(\mathbb{Z}_2, 1, (d_1, d_2))$. The cases $(0,0)$ and $(1,1)$ result in the projection quandle, and it is easy to check that both cases $(0,1)$, $(1,0)$ are isomorphic to $\mathrm{Aff}(\mathbb{Z}_4, -1)$. If $A = \mathbb{Z}_2^2$ or $A = \mathbb{Z}_4$, the value of $\bar{d} = (d)$ is irrelevant, and we obtain one of the three affine quandles.

Example 4.6. There are four quasi-affine quandles of order six (see Proposition 9.2):

$$\begin{aligned}\mathrm{Aff}(\mathbb{Z}_6, 1) \simeq &\mathrm{Ext}(\mathbb{Z}_1, 1, (0,0,0,0,0,0)),\\ &\mathrm{Ext}(\mathbb{Z}_2, 1, (0,0,1)),\\ &\mathrm{Ext}(\mathbb{Z}_3, 1, (0,1)),\\ \mathrm{Aff}(\mathbb{Z}_6, -1) \simeq &\mathrm{Ext}(\mathbb{Z}_3, 2, (0,0)).\end{aligned}$$

The second and third quandles are non-isomorphic, because they have different orbit sizes. They are not affine, since they violate condition (3) of Theorem 2.3. In the second case, $\mathrm{Im}(1-f) = \{0\}$ and $\{0\}$ has two representatives in $\bar{d}$ whereas $\{1\}$ has only one. In the third case, $\mathrm{Im}(1-f) = \{0\}$ and $\{2\}$ has no representative in $\bar{d}$.

Free medial quandles can also be presented using semiregular extensions. This is essentially proved in [14, Theorem 3.3].

Example 4.7. Let X be a set, $x_0 \in X$ and denote $X^- = X \setminus \{x_0\}$. Let $A = \bigoplus_{x \in X^-} \mathbb{Z}[t, t^{-1}]$ be the free $\mathbb{Z}[t, t^{-1}]$-module over a free base $(e_x : x \in X^-)$ and put $e_{x_0} = 0$. Then the free medial quandle of rank $|X|$ can be represented as $\mathrm{Ext}(A, t, \bar{e})$, with the free base $((e_x, 0) : x \in X)$.

In Theorem 2.3(3), we represent affine quandles using a tuple $\bar{d}$ which is a *multi*transversal. The following result explains the role of its multiplicity.

Proposition 4.8. *Let A be an abelian group, f an automorphism of A, and $(d_i : i \in I)$ a multitransversal of $A/\mathrm{Im}(1-f)$ of multiplicity k. Let $J \subseteq I$ such that $(d_i : i \in J)$ is a transversal of $A/\mathrm{Im}(1-f)$. Then $\mathrm{Ext}(A, f, (d_i : i \in I))$ is isomorphic to the direct product*

$$\mathrm{Ext}(A, f, (d_i : i \in J)) \times \mathrm{Proj}(k).$$

Proof. Let K be a set of size k and let ξ be a bijection $J \times K \to I$ such that $d_i - d_{\xi(i,u)} \in \mathrm{Im}(1-f)$, for every $i \in J$ and $u \in K$ (this is possible, because each block of $\mathrm{Im}(1-f)$ contains the same number of representatives in $\bar{d}$). Choose witnesses $c_{i,u} \in A$ such that $d_i - d_{\xi(i,u)} = (1-f)(c_{i,u})$. Consider the mapping

$$\begin{aligned}\Phi : \mathrm{Ext}(A, f, (d_i : i \in J)) \times \mathrm{Proj}(k) &\to \mathrm{Ext}(A, f, (d_i : i \in I)),\\ ((i, a), u) &\mapsto (\xi(i, u),\ a + c_{i,u}).\end{aligned}$$

This is clearly a bijection, and a straightforward calculation shows that it is an isomorphism:

$$\begin{aligned}\Phi((i,a),u)*\Phi((j,b),v) &= (\xi(i,u),\ a+c_{i,u}))*(\xi(j,v),b+c_{j,v})\\ &= (\xi(j,v),\ (1-f)(a+c_{i,u})+f(b+c_{j,v})+d_{\xi(i,u)}-d_{\xi(j,v)})\\ &= (\xi(j,v),\ (1-f)(a)+f(b)+(1-f)(c_{i,u})+c_{j,v}-(1-f)(c_{j,v})+d_{\xi(i,u)}-d_{\xi(j,v)})\\ &= (\xi(j,v),\ (1-f)(a)+f(b)+d_i-d_{\xi(i,u)}+c_{j,v}-d_j+d_{\xi(j,v)}+d_{\xi(i,u)}-d_{\xi(j,v)})\\ &= (\xi(j,v),\ (1-f)(a)+f(b)+d_i-d_j+c_{j,v})\\ &= \Phi((j,(1-f)(a)+f(b)+d_i-d_j),v) = \Phi(((i,a),u)*((j,b),v)).\end{aligned}$$

□

As a consequence, we obtain an interesting decomposition theorem. It is related to [13, Theorem 5.5] which states a similar result covering all medial quandles: every medial quandle where all orbits are latin, is a direct product of an affine quandle and a projection quandle.

Corollary 4.9. *Let A be an abelian group and f its automorphism such that $1-f$ is onto. Then, for any tuple $\bar{d}$, the extension $\mathrm{Ext}(A,f,\bar{d})$ is isomorphic to the direct product of the affine quandle $\mathrm{Aff}(A,f)$ and a projection quandle.*

Proof. Since $\mathrm{Im}(1-f)=A$, there is only one coset of $\mathrm{Im}(1-f)$, hence $\bar{d}$ is a multitransversal of A/A, and Proposition 4.8 applies. Clearly, $\mathrm{Ext}(A,f,(d_1))=\mathrm{Aff}(A,f)$. □

Remark 4.10. The quandle $\mathrm{Ext}(A,f,(d_i:i\in I))$ is a *central extension* of the projection quandle $(I,*)$ over the affine quandle $\mathrm{Aff}(A,f)$, with the cocycle $\theta_{i,j}=d_i-d_j$. Here we mean central extensions in the sense of [8, Chapter 7]. An ongoing project [4] aims at adapting the general theory of abelian and central extensions of [8] to quandles.

5. A universal algebraic characterization

In universal algebra [3], an algebraic structure A is called *abelian* if for every $(k+1)$-ary term operation t and every $a,b,u_1,\dots,u_k,v_1,\dots,v_k\in A$, the following implication holds:

$$t(a,u_1,\dots,u_k)=t(a,v_1,\dots,v_k)\ \Rightarrow\ t(b,u_1,\dots,u_k)=t(b,v_1,\dots,v_k)$$

The condition may look ad hoc, but it has a natural meaning: It is not hard to prove that an algebra A is abelian if and only if, in the direct power A^2, the diagonal $\{(a,a):a\in A\}$ is a block of a congruence [3, Theorem 7.30]. Consequently, a group G is abelian in the present sense (i.e., the diagonal is a normal subgroup of G^2) if and only if G is abelian in the usual sense.

It turns out that this syntactic condition is closely related to representability of general algebraic structures by modules (see [24, 25] for a detailed account). In one direction, consider a module M over a ring R. Every term operation $t(x,x_1,\dots,x_k)$ can be written as $rx+\sum_{i=1}^k r_ix_i$ for some $r,r_i\in R$. Then $t(a,u_1,\dots,u_k)=t(a,v_1,\dots,v_k)$ implies that $\sum_{i=1}^k r_iu_i=\sum_{i=1}^k r_iv_i$, and thus we have $t(b,u_1,\dots,u_k)=t(b,v_1,\dots,v_k)$ for every $b\in M$. Hence every module is abelian. The same argument shows that every algebraic structure defined by term operations over a module is abelian, too. And indeed, a subalgebra of an abelian algebra is also abelian. We just proved that every quasi-affine algebraic structure is abelian.

The converse implication is more complicated. It holds in many particular cases [24, 25], but not in general [19]. As the first step towards establishing that abelian quandles are quasi-affine, we prove that they satisfy condition (2) of Theorem 2.2.

Lemma 5.1. *Let Q be an abelian quandle. Then $\mathrm{Dis}(Q)$ is a semiregular abelian group.*

Proof. First we show that Q is medial, and thus $\mathrm{Dis}(Q)$ is abelian. Let $t(x,y,u,v) = (x*y)*(u*v)$ and consider any $a,b,c,d \in Q$. Using idempotence and left distributivity,

$$t(a,a,b,c) = (a*a)*(b*c) = (a*b)*(a*c) = t(a,b,a,c).$$

Using abelianness, we obtain

$$(d*a)*(b*c) = t(d,a,b,c) = t(d,b,a,c) = (d*b)*(a*c).$$

For semiregularity, consider $\alpha = L_{a_1}L_{b_1}^{-1}\dots L_{a_n}L_{b_n}^{-1} \in \mathrm{Dis(Q)}$ such that $\alpha(c) = c$ for some $c \in Q$. We shall prove that α is the identity mapping. Let $t(z,x_1,\dots,x_n,y_1,\dots,y_n)$ be the term that represents the formal expression $L_{x_1}L_{y_1}^{-1}\dots L_{x_n}L_{y_n}^{-1}(z)$. Then

$$t(c,a_1,\dots,a_n,b_1,\dots,b_n) = \alpha(c) = c = L_cL_c^{-1}\dots L_cL_c^{-1}(c) = t(c,c,\dots,c,c,\dots,c).$$

Using abelianness, we obtain

$$\alpha(d) = t(d,a_1,\dots,a_n,b_1,\dots,b_n) = t(d,c,\dots,c,c,\dots,c) = L_cL_c^{-1}\dots L_cL_c^{-1}(d) = d$$

for every $d \in Q$. □

Remark 5.2. We just proved that abelian quandles are medial. In the next section, we will prove that abelian quandles are quasi-affine. A different but related affine representation result was established by Kearnes in [16, Theorem 1.5]: *Every medial quandle Q admits a strongly abelian congruence θ such that Q/θ is quasi-affine.* It is not difficult to prove that, in quandles, strongly abelian congruences are precisely those below the kernel of the Cayley mapping $x \mapsto L_x$ (see [4]).

6. Characterization theorems

In the present section, we prove the main results. We start with the characterization theorem for affine quandles.

Proof of Theorem 2.3. (1) ⇒ (2). Let $Q = \mathrm{Aff}(A,f)$. Recall that

$$\mathrm{Dis}(Q) = \{x \mapsto a + x : \ a \in \mathrm{Im}(1-f)\}.$$

It immediately follows that $\mathrm{Dis}(Q)$ is abelian and semiregular. Next we prove that

$$[\mathrm{Dis}(Q), L_e] = \{x \mapsto b + x : \ b \in \mathrm{Im}((1-f)^2)\}.$$

For $\alpha \in \mathrm{Dis}(Q)$, $\alpha(x) = a + x$, we have

$$[\alpha, L_e](x) = a + (1-f)(e) + f(-a + (1-f^{-1})(e) + f^{-1}(x)) = (1-f)(a) + x.$$

Indeed, $(1-f)(a) \in \mathrm{Im}((1-f)^2)$, and every element of $\mathrm{Im}((1-f)^2)$ can be written this way.

Now we finish the proof of (2). Fix $e \in \mathrm{Dis}(Q)$ and a transversal T of the orbit decomposition, that is, a transversal of $A/\mathrm{Im}(1-f)$. We shall prove that $\{\{L_aL_e^{-1} : a \in T\}\}$ is a multitransversal of $\mathrm{Dis}(Q)/[\mathrm{Dis}(Q), L_e]$. Since $L_aL_e^{-1}(x) = (1-f)(a-e) + x$, this is equivalent to the fact that $\{\{(1-f)(a-e) : a \in T\}\}$ is a multitransversal of $\mathrm{Im}(1-f)/\mathrm{Im}((1-f)^2)$. Now apply Lemma 2.1 to $G = A$, $\varphi = 1-f$ and the transversal $\{a-e : a \in T\}$ of $A/\mathrm{Im}(1-f)$.

(2) ⇒ (2′) is trivial.

(2′) ⇒ (3). Let $A = \mathrm{Dis}(Q)$, $f(\alpha) = \alpha^{L_e}$ and put $d_x = L_xL_e^{-1}$, $x \in T$. Observe that $[\mathrm{Dis}(Q), L_e] = \mathrm{Im}(1-f)$, because

$$[\alpha, L_e] = \alpha L_e \alpha^{-1} L_e^{-1} = \alpha f(\alpha)^{-1} = (1-f)(\alpha).$$

According to Lemma 4.3, Q is isomorphic to the extension $\mathrm{Ext}(\mathrm{Dis}(Q), f, (L_xL_e^{-1} : x \in T))$. By assumptions, $\bar{d}$ is a multitransversal of $\mathrm{Dis}(Q)/[\mathrm{Dis}(Q), L_e] = A/\mathrm{Im}(1-f)$.

(3) ⇒ (1). According to Proposition 4.8, Q is a product of a projection quandle (which is affine) and an extension $\mathrm{Ext}(A, f, \bar{e})$ where $\bar{e}$ is a transversal. Since the product of affine quandles is affine, it remains to prove that the implication holds assuming that $\bar{d}$ is a transversal.

According to the Hou-Šťovíček Lemma 3.1 for $\varphi = 1 - f$, there is an abelian group $E \geq A$ and an epimorphism $\psi : E \to A$ such that $\psi|_A = 1 - f$ and $\psi/A : E/A \simeq A/\mathrm{Im}(1-f)$. Let $g = 1 - \psi$. First we prove that $g \in \mathrm{Aut}(E)$. Indeed, it is an endomorphism. Given $y \in E$, we will find all $x \in E$ such that $g(x) = (1-\psi)(x) = y$, that is, such that $\psi(x) = x - y$. Since $\mathrm{Im}(\psi) = A$, we must have $x - y \in A$, and thus we can assume that $x = y + a$ for some $a \in A$. Now, on one hand, we have

$$\psi(y + a) = \psi(x) = x - y = y + a - y = a,$$

and on the other hand, we have

$$\psi(y + a) = \psi(y) + \psi(a) = \psi(y) + a - f(a),$$

because $\psi|_A = 1 - f$. Putting together, $x = y + a$ is a solution to the equation $g(x) = y$ if and only if $\psi(y) = f(a)$, that is, if and only if $a = f^{-1}\psi(y)$. Therefore, the equation has a unique solution, and thus g is bijective.

Consider a transversal $(e_i)_{i\in I}$ of E/A such that $\psi(e_i) = d_i$. Define a mapping

$$\Phi : I \times A \to E, \qquad (i, a) \mapsto e_i + a.$$

We prove that this is a quandle isomorphism $\mathrm{Ext}(A, f, \bar{d}) \simeq \mathrm{Aff}(E, g)$. It is indeed bijective: given $u \in E$, there is a unique decomposition $u = e_i + a$ where e_i is the representative of the coset such that $u \in e_i + A$, and thus (i, a) is the unique preimage. To show that Φ is a homomorphism, we calculate

$$\begin{aligned}
\Phi(i, a) * \Phi(j, b) &= (e_i + a) * (e_j + b) \\
&= (1 - g)(e_i + a) + g(e_j + b) \\
&= (1 - g)(a) + g(b) + (1 - g)(e_i) - (1 - g)(e_j) + e_j \\
&= (1 - f)(a) + f(b) + \psi(e_i) - \psi(e_j) + e_j \\
&= (1 - f)(a) + f(b) + d_i - d_j + e_j \\
&= \Phi(j, (1 - f)(a) + f(b) + d_i - d_j) \\
&= \Phi((i, a) * (j, b))
\end{aligned}$$

for every $i, j \in I$ and $a, b \in A$. □

Now, using Theorem 2.3, we can prove the characterization theorem for quasi-affine quandles.

Proof of Theorem 2.2. (1) ⇒ (2). Let Q be a subquandle of $\mathrm{Aff}(A, f) = \mathrm{Ext}(A, f, (0))$. According to Lemma 4.2, $G = \mathrm{Dis}(\mathrm{Aff}(A, f))$ is an abelian semiregular permutation group. The group $\mathrm{Dis}(Q)$ is a subgroup of permutations from G restricted to the subset $Q \subseteq A$, hence it is also abelian and semiregular.

(2) ⇒ (3) was proved in Lemma 4.3.

(3) ⇒ (1). Assume that $Q = \mathrm{Ext}(A, f, \bar{d})$ where $\bar{d} = (d_i : i \in I)$. Extend the set I and the tuple $\bar{d}$ into a set $J \supseteq I$ and a tuple $\bar{e} = (e_j : j \in J)$ such that $\bar{e}$ is a multitransversal of $A/\mathrm{Im}(1-f)$ and $e_i = d_i$ for every $i \in I$. Then $Q = \mathrm{Ext}(A, f, \bar{d})$ is a subquandle of $\mathrm{Ext}(A, f, \bar{e})$, which is affine according to Theorem 2.3.

(Extending the tuple $\bar{d}$ is indeed possible: from each coset $x + \mathrm{Im}(1-f)$, add sufficiently many elements so that all cosets have the same number of representatives. Here is a formal description. Choose a transversal T of $A/\mathrm{Im}(1-f)$. For $x \in T$, let $n_x = |\bar{d} \cap (x + \mathrm{Im}(1-f))|$ and put $n = \sup\{n_x : x \in T\}$. Let $J = I \cup \bigcup_{x\in T} J_x$, where J_x are pairwise disjoint sets, disjoint with I, such that $|J_x| + n_x = n$. Define $e_i = d_i$ for every $i \in I$, and for every $j \in J_x$, choose $e_j \in x + \mathrm{Im}(1-f)$ arbitrarily.)

(1) ⇒ (4) holds for all algebraic structures, see Section 5.

(4) ⇒ (2) was proved in Lemma 5.1. □

Corollary 6.1. *Let Q be a quasi-affine quandle. Then there exists an abelian group A and its automorphism f such that Q embeds into* $\mathrm{Aff}(A, f)$ *and* $|A| \le |Q| \cdot |\mathrm{Dis}(Q)| \le |Q|^2$.

Proof. According to Lemma 4.3, $Q \simeq \mathrm{Ext}(D, g, \bar{d})$ such that $D = \mathrm{Dis}(Q)$ and $\bar{d}$ is indexed by T, a set of orbit representatives. In particular, $|Q| = |\mathrm{Dis}(Q) \times T| = |\mathrm{Dis}(Q)| \cdot |T|$. Using the construction from the proof of Theorem 2.2, (3) $\Rightarrow$ (1), Q embeds into an affine quandle $R = \mathrm{Ext}(D, g, \bar{e})$ where $\bar{e}$ is indexed by a set not larger than $|T| \cdot |D/\mathrm{Im}(1-f)| \le |T| \cdot |\mathrm{Dis}(Q)| = |Q|$. Therefore, $|R| \le |\mathrm{Dis}(Q)| \cdot |Q| \le |Q|^2$. □

For *finite* quandles, the balancedness conditions of Theorem 2.3 can be formulated alternatively, perhaps more esthetically: a quasi-affine quandle is affine if and only if, in every column (equivalently, in some column) of the multiplication table, each entry has the same number of occurences.

Let $m_{x,y}$ denote the number of occurrences of y in the column of x in the multiplication table of Q; formally,

$$m_{x,y} = |\{z \in Q : \ z * x = y\}|.$$

Indeed $m_{x,y} = 0$ if $y \notin Qx$.

Theorem 6.2. *The following statements are equivalent for a finite quasi-affine quandle Q:*

(1) *Q is affine;*
(2) *for every $x \in Q$ and every $y_1, y_2 \in Qx$, $m_{x,y_1} = m_{x,y_2}$;*
(3) *there exists $x \in Q$ such that for every $y_1, y_2 \in Qx$, $m_{x,y_1} = m_{x,y_2}$.*

Proof. (1) $\Rightarrow$ (2). Let $Q = \mathrm{Aff}(A, f)$. Then $m_{x,y} = |\{z \in Q : \ (1-f)(z) = y - f(x)\}|$. Assuming that $y \in Qx$, there is $u \in A$ such that $y = (1-f)(u) + x$, and thus

$$m_{x,y} = |\{z \in Q : \ (1-f)(z) = (1-f)(x+u)\}| = |\mathrm{Ker}(1-f)|,$$

because $(1-f)(a) = (1-f)(a')$ if and only if $a - a' \in \mathrm{Ker}(1-f)$. We see that $m_{x,y}$ is independent of y.

(2) $\Rightarrow$ (3) is trivial.

(3) $\Rightarrow$ (1). Assume that $Q = \mathrm{Ext}(A, f, \bar{d})$ is an indecomposable extension and take $j \in I$, $b \in A$ such that $x = (j, b)$. Consider $y = (j, c) \in Qx$. We have

$$m_{(j,b),(j,c)} = |\{(i,a) : \ (i,a) * (j,b) = (j,c)\}| = |\{(i,a) : \ (1-f)(a) + f(b) + d_i - d_j = c\}|.$$

Given i, j, b, c, the number of a's satisfying the equation is precisely $|\mathrm{Ker}(1-f)|$, hence

$$m_{(j,b),(j,c)} = |\mathrm{Ker}(1-f)| \cdot |\{i : \ d_i - d_j + f(b) - c \in \mathrm{Im}(1-f)\}|.$$

Denoting $u_c = d_j - f(b) + c$, we obtain

$$m_{(j,b),(j,c)} = |\mathrm{Ker}(1-f)| \cdot |\{i : \ d_i \in u_c + \mathrm{Im}(1-f)\}|.$$

According to (3), this expression shall be independent of $y = (j, c)$. Running over all $c \in A$, the element u_c also runs over all elements of A, and thus all cosets of $\mathrm{Im}(1-f)$ must contain the same number of d_i's. In other terms, $\bar{d}$ is a multitransversal of $A/\mathrm{Im}(1-f)$. According to Theorem 2.3, the quandle Q is affine. □

The finiteness assumption in Theorem 6.2 could be weakened: we used finiteness only in the last step of the proof (independence of $m_{(j,b),(j,c)}$ on (j, c) implies independence of the right factor on (j, c)), and it would have been sufficient to assume only that $\mathrm{Ker}(1-f)$ is finite. Nevertheless, infinite counterexamples to Theorem 6.2 are abundant.

Example 6.3. Let $Q = \mathrm{Ext}(\mathbb{Z}, 1, \bar{d})$, where $\bar{d}$ contains every non-zero integer once and zero twice. Then $\bar{d}$ is not a multitransversal of $\mathbb{Z}/\mathrm{Im}(1-f) = \mathbb{Z}/0$, hence Q is not affine. But $m_{x,y}$ is infinite countable for every x, y, hence Q satisfies condition (2) of Theorem 6.2.

The following example shows that the implication (2) ⇒ (1) of Theorem 6.2 does not hold without the assumption that Q is quasi-affine.

Example 6.4. Let Q be the quandle defined by the following multiplication table:

Q	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	1	2	3	4	5	6	7	8
3	2	1	3	4	6	5	8	7
4	2	1	3	4	6	5	8	7
5	2	1	4	3	5	6	8	7
6	2	1	4	3	5	6	8	7
7	1	2	4	3	6	5	7	8
8	1	2	4	3	6	5	7	8

.

It satisfies condition (2) of Theorem 6.2 but it is not quasi-affine, since $\mathrm{Dis}(Q)$ is not semiregular. (The example is a 2-reductive medial quandle and it was constructed using the methods of [13, Section 6].)

The following example shows that it is not possible to characterize affine quandles by a first-order property of the displacement group.

Example 6.5. Let $Q_1 = \mathrm{Ext}(\mathbb{Z}_3, 1, (0,1))$ and $Q_2 = \mathrm{Ext}(\mathbb{Z}_3, 2, (0,0)) = \mathrm{Aff}(\mathbb{Z}_6, -1)$. Then both $\mathrm{Dis}(Q_1)$ and $\mathrm{Dis}(Q_2)$ are isomorphic to $\mathbb{Z}_3$, but Q_1 is not affine (see Example 4.6).

Affine quandles have tiny displacement groups, but the converse is not true. In fact, the conditions "$\mathrm{Dis}(Q)$ is tiny" and "Q is quasi-affine" are independent for medial quandles, as witnessed by the following example.

Example 6.6.

- The quandle $Q = \mathrm{Ext}(\mathbb{Z}_2, 1, (0,0,1))$ is quasi-affine, $\mathrm{Dis}(Q)$ is tiny but Q is not affine.
- The quandle $Q = \mathrm{Ext}(\mathbb{Z}_3, 1, (0,1))$ is quasi-affine but $\mathrm{Dis}(Q)$ is not tiny.
- The quandle $Q = \mathrm{Aff}(\mathbb{Z}_4, -1)/\alpha$, where α is the congruence with blocks $\{0,2\}$, $\{1\}$, $\{3\}$, is not quasi-affine, because $\mathrm{Dis}(Q)$ does not act semiregularly (it fixes the block $\{0,2\}$), but $\mathrm{Dis}(Q)$ is tiny.

Remark 6.7. A quandle is a homomorphic image of a quasi-affine quandle if and and only if it is medial. The latter is clearly a necessary condition, and the other direction follows immediately from Theorem 2.2 and Lemma 4.3: every medial quandle is a homomorphic image of some $E = \mathrm{Ext}(A, f, \bar{d})$.

7. Algorithms

We will discuss two decision problems. On input, we have a quandle. We are asked to decide whether the quandle is affine or quasi-affine, respectively. We will assume that the input quandle is in the form of a multiplication table, although one can imagine other representations for which the algorithms work efficiently. Both algorithms are based on the properties of the displacement group, as described in conditions (2) of Theorems 2.2 and 2.3. Since the input is finite, we will check balancedness using Theorem 6.2. Let us start with the affine case.

Algorithm 7.1.
In: a quandle Q
Out: is Q affine?
1. pick $e \in Q$
2. $D := \{L_x L_e^{-1} : x \in Q\}$
3. **for each** $\alpha \in D$ **do**
4. **if** $0 < |Fix(\alpha)| < |Q|$ **then return** false
5. **for each** $\beta \in D$ **do**
6. **if** $\alpha\beta \neq \beta\alpha$ **then return** false
7. **if** $\alpha\beta \notin D$ **then return** false
8. $m_x := 0$ for each $x \in Q$
9. **for each** $x \in Q$ **do** $m_{xe} := m_{xe} + 1$
10. **for each** $x \in Q$ **do if** $m_{xe} \neq m_e$ **then return** false
11. **return** true

In the first part of the algorithm (lines 1–7), it is checked whether $\mathrm{Dis}(Q)$ is semiregular, abelian and tiny. All of these are necessary conditions for a quandle to be affine, and sufficient to be quasi-affine. If succeeded, the algorithm checks condition (2) of Theorem 6.2, picking the column e. We use an observation that if $\mathrm{Dis}(Q)$ is tiny then $Qe = \{xe : x \in Q\}$.

Proposition 7.2. *Algorithm 7.1 runs in $\mathcal{O}(n^3 \log n)$ time with respect to $n = |Q|$.*

Proof. All operations performed with permutations on Q (comparison, composition, counting fixed points) can be calculated in $\mathcal{O}(n \log n)$ time. In the first part (lines 1–7), we run over n^2 pairs of permutations α, β, performing a fixed amount of operations with them, resulting in $\mathcal{O}(n^3 \log n)$ time. The remaining part of the algorithm takes essentially linear time. □

In the quasi-affine case, we do not have the convenient condition that the displacement group is tiny. To avoid a blow-up during calculation of $\mathrm{Dis}(Q)$ when the input is not quasi-affine, we implement a convenient upper bound on $|\mathrm{Dis}(Q)|$ under the assumption of semiregularity.

Lemma 7.3. *Let Q be a quandle with $\mathrm{Dis}(Q)$ acting semiregularly. Then $|\mathrm{Dis}(Q)| \leq |Q|$.*

Proof. For any group, we have $|G| = |G_e| \cdot |Orb(e)|$. In particular, $|\mathrm{Dis}(Q)| = |\mathrm{Dis}(Q)_e| \cdot |Qe|$. If $\mathrm{Dis}(Q)$ acts semiregularly, then $|\mathrm{Dis}(Q)_e| = 1$, and thus $|\mathrm{Dis}(Q)| = |Qe| \leq |Q|$. □

Algorithm 7.4.
In: a quandle Q
Out: is Q quasi-affine?
1. pick $e \in Q$
2. $D := \{L_x L_e^{-1} : x \in Q\}$
3. **for each** $\alpha \in D$ **do**
4. **if** $0 < |Fix(\alpha)| < |Q|$ **then return** false
5. **for each** $\beta \in D$ **do**
6. **if** $\alpha\beta \neq \beta\alpha$ **then return** false
7. $P := \{\{\alpha, \beta\} : \alpha, \beta \in D\}$
8. **while** $P \neq \emptyset$ **do**
9. select $\{\alpha, \beta\} \in P$, remove $\{\alpha, \beta\}$ from P
10. **if** $\alpha\beta \notin D$ **then**
11. **if** $|D| \geq |Q|$ **then return** false
12. **if** $0 < |Fix(\alpha\beta)| < |Q|$ **then return** false
13. $D := D \cup \{\alpha\beta\}$
14. $P := P \cup \{\{\alpha\beta, \delta\} : \delta \in D\}$
15. **return** true

In the first part of the algorithm (lines 1–6), we consider the generators of $\mathrm{Dis}(Q)$ and check whether they commute and have the correct number of fixed points. If succeeded, on lines 7–14, the algorithm generates $\mathrm{Dis}(Q)$ in a standard way. (In the expression $\{\alpha, \beta\}$, we allow $\alpha = \beta$. Then the result is a one-element set that represents the mapping α^2.) Whenever we find a composition $\alpha\beta$ not yet in D, we check whether it has the correct number of fixed points, and if so, $\alpha\beta$ is added to D and P is expanded accordingly (no need to check commutativity, since a group is abelian if and only if its generators commute). The algorithm terminates on line 11 if it realizes that $|\mathrm{Dis}(Q)| > |Q|$, thanks to Lemma 7.3.

Proposition 7.5. *Algorithm 7.4 runs in $\mathcal{O}(n^3 \log n)$ time with respect to $n = |Q|$.*

Proof. As in Proposition 7.2, the first part (lines 1–6) results in $\mathcal{O}(n^3 \log n)$ time. In the second part, we start with $|P| \leq n^2$. The condition on line 10 is satisfied at most n times, thanks to Lemma 7.3 employed on line 11. Therefore, during the run of the algorithm, at most n^2 unordered pairs are added to $|P|$ on line 14, an the loop will finish after at most $2n^2$ steps. Each step only does a fixed amount of operations with permutations on Q, hence the loop requires $\mathcal{O}(n^3 \log n)$ time. □

Both algorithms solve the decision problems (the answer is yes/no). To output the actual affine representation is a more complex problem. We can indeed retrieve a representation in the form of a semiregular extension, as suggested by Lemma 4.3, as all information is readily available. Given $Q = \mathrm{Ext}(A, f, \bar{d})$, the proof of Theorem 2.2 explains how to expand $\bar{d}$ so that the result is an affine quandle into which Q embeds; this expansion can be implemented efficiently. However, given an affine quandle in the form of a semiregular extension, it is not clear how to obtain the actual affine representation $\mathrm{Aff}(E, g)$. In the proof of Theorem 2.3, we used the Hou-Šťovíček lemma to find the pair (E, g), but its proof is not constructive and cannot be transformed into an algorithm.

Remark 7.6. Universal algebra suggests an alternative approach to checking whether a given quandle is quasi-affine. Theorem 2.2 states that a quandle Q is quasi-affine if and only if it is abelian (in the universal algebraic sense). Then Q is abelian if and only if the diagonal is a block of a congruence in the direct power Q^2, that is, if and only if the congruence of Q^2 generated by the diagonal has the diagonal as its block. Congruences of binary algebras can be generated in cubic time with respect to the number of elements, see [6] for a fast algorithm. This provides an alternative to Algorithm 7.4, but the time complexity seems to be much worse.

8. Affine meshes and the isomorphism theorem

In [13], we developed a representation of medial quandles by certain heterogeneous affine structure, called affine meshes. First, we recall essential constructions and results.

Definition 8.1. An *affine mesh* over a non-empty set I is a triple

$$\mathcal{A} = ((A_i)_{i\in I}, (\varphi_{i,j})_{i,j\in I}, (c_{i,j})_{i,j\in I})$$

where A_i are abelian groups, $\varphi_{i,j} : A_i \to A_j$ homomorphisms, and $c_{i,j} \in A_j$ constants, satisfying the following conditions for every $i, j, j', k \in I$:

(M1) $1 - \varphi_{i,i}$ is an automorphism of A_i;
(M2) $c_{i,i} = 0$;
(M3) $\varphi_{j,k}\varphi_{i,j} = \varphi_{j',k}\varphi_{i,j'}$, i.e., the following diagram commutes:

$$\begin{array}{ccc} A_i & \xrightarrow{\varphi_{i,j}} & A_j \\ \downarrow{\scriptstyle \varphi_{i,j'}} & & \downarrow{\scriptstyle \varphi_{j,k}} \\ A_{j'} & \xrightarrow{\varphi_{j',k}} & A_k \end{array}$$

(M4) $\varphi_{j,k}(c_{i,j}) = \varphi_{k,k}(c_{i,k} - c_{j,k})$.

The mesh is called *indecomposable* if for every $j \in I$, the group A_j is generated by the set

$$\{c_{i,j}, \varphi_{i,j}(a) : \ i \in I, a \in A_i\}.$$

If the index set is clear from the context, we shall write briefly $\mathcal{A} = (A_i, \varphi_{i,j}, c_{i,j})$.

Definition 8.2. The *sum of an affine mesh* $(A_i, \varphi_{i,j}, c_{i,j})$ over a set I is an algebraic structure defined on the disjoint union of the sets A_i by

$$a * b = c_{i,j} + \varphi_{i,j}(a) + (1 - \varphi_{j,j})(b),$$

for every $a \in A_i$ and $b \in A_j$.

The sum Q of an affine mesh is a medial quandle. The fibers A_i, $i \in I$, form subquandles of Q which are affine, namely, $\mathrm{Aff}(A_i, 1 - \varphi_{i,i})$. If the mesh is indecomposable, then the fibers are precisely the orbits of Q.

Theorem 8.3. [13, Theorem 3.14] *An algebraic structure $(Q, *)$ is a medial quandle if and only if it is the sum of an indecomposable affine mesh.*

A quasi-affine quandle is medial, hence it is the sum of an affine mesh. The structure of the mesh is easily derived from the parameters of the semiregular extension.

Observation 8.4. *A semiregular extension* $\mathrm{Ext}(A, f, (d_i : i \in I))$ *is the sum of an affine mesh*

$$((A)_{i \in I}, \ (1 - f)_{i,j \in I}, \ (d_i - d_j)_{i,j \in I}).$$

The mesh (and thus the extension) is indecomposable if and only if the group A is generated by the set

$$\mathrm{Im}(1 - f) \cup \{d_i - d_j : \ i, j \in I\}.$$

Definition 8.5. Two affine meshes, $\mathcal{A} = (A_i, \varphi_{i,j}, c_{i,j})$ over an index set I, and $\mathcal{A}' = (A'_i, \varphi'_{i,j}, c'_{i,j})$ over an index set I', are called *homologous*, if there exist a bijection $\pi : I \to I'$, group isomorphisms $\psi_i : A_i \to A'_{\pi(i)}$, and constants $e_i \in A'_{\pi(i)}$, such that, for every $i, j \in I$,

(H1) $\psi_j \varphi_{i,j} = \varphi'_{\pi(i),\pi(j)} \psi_i$, i.e., the following diagram commutes:

$$\begin{array}{ccc} A_i & \xrightarrow{\varphi_{i,j}} & A_j \\ \downarrow{\scriptstyle \psi_i} & & \downarrow{\scriptstyle \psi_j} \\ A'_{\pi(i)} & \xrightarrow{\varphi'_{\pi(i),\pi(j)}} & A'_{\pi(j)} \end{array}$$

(H2) $\psi_j(c_{i,j}) = c'_{\pi(i),\pi(j)} + \varphi'_{\pi(i),\pi(j)}(e_i) - \varphi'_{\pi(j),\pi(j)}(e_j)$.

Theorem 8.6. [13, Theorem 4.2] *Let $\mathcal{A} = (A_i, \varphi_{i,j}, c_{i,j})$ and $\mathcal{A}' = (A'_i, \varphi'_{i,j}, c'_{i,j})$ be two indecomposable affine meshes. The sums of $\mathcal{A}$ and $\mathcal{A}'$ are isomorphic quandles if and only if the meshes $\mathcal{A}$, $\mathcal{A}'$ are homologous.*

Specializing Theorem 8.6, we obtain an isomorphism theorem for indecomposable semiregular extensions.

Theorem 8.7. *Let* $\mathrm{Ext}(A, f, (d_i : i \in I))$ *and* $\mathrm{Ext}(A', f', (d'_i : i \in I'))$ *be two indecomposable extensions. They are isomorphic if and only if there exist a bijection $\pi : I \to I'$, an isomorphism $\psi : A \to A'$, and an element $a \in A'$ such that*

(E1) $\psi f = f' \psi$,

(E2) $\psi(d_i) - d'_{\pi(i)} \in a + \mathrm{Im}(1 - f')$ *for every $i \in I$.*

Proof. Combining Observation 8.4 and Theorem 8.6, we see that the two extensions are isomorphic if and only if there exist a bijection $\pi : I \to I'$, isomorphisms $\psi_i : A \to A'$, and elements $e_i \in A'$ such that for every $i, j \in I$

(H1) $\psi_i(1-f) = (1-f')\psi_j$,
(H2) $\psi_j(d_i - d_j) = d'_{\pi(i)} - d'_{\pi(j)} + (1-f')(e_i) - (1-f')(e_j)$.

($\Rightarrow$). Consider π, ψ_i and e_i as above. Choose $k \in I$ and define $\psi = \psi_k$ and $a = \psi_k(d_k) - d'_{\pi(k)} - (1-f')(e_k)$. Then condition (E1) is a special case of (H1) for $i = j = k$, and condition (E2) follows from (H2) with $j = k$, since $\psi(d_i) = \psi(d_k) + d'_{\pi(i)} - d'_{\pi(k)} + (1-f')(e_i) - (1-f')(e_k) = d'_{\pi(i)} + (1-f')(e_i) + a$, and thus $\psi(d_i) - d'_{\pi(i)} \in a + \mathrm{Im}(1-f')$.

($\Leftarrow$). Consider π, ψ, a as in the statement of the theorem. For every $i \in I$ define $\psi_i = \psi$ and select e_i such that $\psi(d_i) - d'_{\pi(i)} = a + (1-f')(e_i)$. Then condition (H1) immediately follows from (E1) and the fact that $\psi_i = \psi_j$ for every i, j, and condition (H2) immediately follows from (E2) applied to both i and j (the two occurences of a in the expression cancel). □

If the extensions represent affine quandles, the theorem simplifies.

Corollary 8.8. *Let* $\mathrm{Ext}(A, f, (d_i : i \in I))$ *and* $\mathrm{Ext}(A', f', (d'_i : i \in I'))$ *be two indecomposable extensions such that* $\bar{d}$ *is a multitransversal of* $A/\mathrm{Im}(1-f)$ *and* $\bar{d}'$ *is a multitransversal of* $A'/\mathrm{Im}(1-f')$*. The extensions are isomorphic if and only if there is an isomorphism* $\psi : A \to A'$ *such that*

(E1) $\psi f = f'\psi$,
(E2') *the multiplicities of* $\bar{d}$, $\bar{d}'$ *are equal.*

Proof. We need to prove that (E2') holds if and only if there exist π and a satisfying (E2).

($\Leftarrow$) Choose a coset of $\mathrm{Im}(1-f)$ and consider the subset $J \subseteq I$ of all indices j such that d_j belongs to this coset. Then (E2) implies that all $d'_{\pi(j)}$, $j \in J$, belong to the same coset of $\mathrm{Im}(1-f')$, hence the multiplicity of $\bar{d}'$ must be greater of equal. A reverse argument shows that they are equal.

($\Rightarrow$) Let $a = 0$ and take π such that $d_i \in u + \mathrm{Im}(1-f)$ if and only if $d'_{\pi(i)} \in \psi(u) + \mathrm{Im}(1-f')$. This is possible since $\bar{d}$, $\bar{d}'$ are multitransversals of block systems with the same numbers of blocks and the same multiplicity. Now, $\psi(d_i) \in \psi(u + \mathrm{Im}(1-f)) = \psi(u) + \mathrm{Im}(1-f')$, and thus $\psi(d_i) - d'_{\pi(i)} \in \mathrm{Im}(1-f')$. □

Translating the previous statement to the affine setting, we obtain Hou's isomorphism theorem for affine quandles.

Corollary 8.9. [10, Theorem 3.1] *Two affine quandles* $\mathrm{Aff}(A, f)$, $\mathrm{Aff}(B, g)$ *are isomorphic if and only if there exists an isomorphism* $\psi : \mathrm{Im}(1-f) \to \mathrm{Im}(1-g)$ *such that* $\psi f(u) = g\psi(u)$ *for every* $u \in \mathrm{Im}(1-f)$*, and*

$$|\mathrm{Ker}(1-f)/\mathrm{Ker}(1-f) \cap \mathrm{Im}(1-f)| = |\mathrm{Ker}(1-g)/\mathrm{Ker}(1-g) \cap \mathrm{Im}(1-g)|.$$

Proof. According to Example 4.4, $\mathrm{Aff}(A, f) \simeq \mathrm{Ext}((1-f)(A), f, ((1-f)(t) : t \in T))$ where T is a transversal of $A/\mathrm{Im}(1-f)$, and $\mathrm{Aff}(B, g) \simeq \mathrm{Ext}((1-g)(B), g, ((1-b)(s) : s \in S))$ where S is a transversal of $B/\mathrm{Im}(1-g)$. Now, Corollary 8.8 applies: the conditions on ψ are identical, and according to Lemma 2.1, $|\mathrm{Ker}(1-f)/\mathrm{Ker}(1-f) \cap \mathrm{Im}(1-f)|$ equals the multiplicity of $\{\{(1-f)(t) : t \in T\}\}$. □

9. Enumeration

First, we outline an enumeration procedure for quasi-affine quandles of given order n. Theorem 8.7 suggests to start with a choice of

- an index set I of order k dividing n (then k will be the number of orbits),

- an abelian group A of order n/k up to isomorphism (then n/k will be the orbit size),
- its automorphism f up to conjugacy (the orbit subquandles will be $\simeq \mathrm{Aff}(A, f)$).

The number of quandles of the form $\mathrm{Ext}(A, f, (d_1, \ldots, d_k))$ will be denoted by $\varepsilon(A, f, k)$, and we will often shortcut $\varepsilon_{n,k} = \varepsilon(\mathbb{Z}_n, 1, k)$. In some cases, the enumeration is easy to do with ad hoc arguments.

Proposition 9.1. *There are exactly $p-1$ quasi-affine quandles of order p, p prime, up to isomorphism. All of them are affine.*

Proof. We will follow the procedure outlined above. We can choose $k = 1$ or $k = p$. For $k = 1$, we have $A = \mathbb{Z}_p$ and $f(x) = ax$ for some $a \in \{1, \ldots, p-1\}$. The extension is indecomposable if and only if $a \neq 1$. The choice of $\bar{d} = (d_1)$ is irrelevant and we obtain $p-2$ connected affine quandles. For $k = p$, we have $A = \{0\}$ the trivial group, $f = 1$, and there is only one choice $\bar{d} = (0, \ldots, 0)$. We obtain one affine (projection) quandle. □

Proposition 9.2. *Let p, q be distinct primes. Up to isomorphism, there are exactly*

(1) *$2p^2 - 2p - 2 + \varepsilon_{p,p}$ quasi-affine quandles of order p^2,*
(2) *$pq - p - q + 1 + \varepsilon_{p,q} + \varepsilon_{q,p}$ quasi-affine quandles of order pq.*

Proof. We will follow the procedure outlined above.

(1) For $k = 1$, we have $|A| = p^2$ and we obtain precisely the connected affine quandles of order p^2. It was determined by Hou [11] that there are $2p^2 - 3p - 1$ such quandles, up to isomorphism.

For $k = p$, we have $A = \mathbb{Z}_p$. *Subcase 1:* $f(x) = ax$ for $a \in \{2, \ldots, p-1\}$. Then the orbits are latin subquandles, and according to Corollary 4.9, $Q = \mathrm{Aff}(A, f) \times \mathrm{Proj}(p)$; this way, we obtain $p-2$ affine quandles. *Subcase 2:* $f = 1$. This case contributes $\varepsilon_{p,p}$ quandles.

For $k = p^2$, we have $A = \{0\}$ the trivial group, $f = 1$, and there is only one choice $\bar{d} = (0, \ldots, 0)$. We obtain one affine (projection) quandle.

(2) For $k = 1$, we have $A = \mathbb{Z}_p \times \mathbb{Z}_q$ and we obtain precisely the products of connected affine quandles of orders p and q, that is, $(p-2)(q-2)$ quandles.

For $k = q$, we have $A = \mathbb{Z}_p$. The discussion is exactly as in the second case of part (1), obtaining $p-2$ quandles of the form $Q = \mathrm{Aff}(A, f) \times \mathrm{Proj}(q)$ and $\varepsilon_{q,p}$ quandles with $f = 1$. The case $k = p$ in analogical, with the role of p and q switched, contributing $q - 2 + \varepsilon_{p,q}$ quandles.

The case $k = pq$ is exactly as the last case of part (1). □

Now, we will address how to calculate the numbers $\varepsilon(A, f, k)$. Let $Q = \mathrm{Ext}(A, f, (d_1, \ldots, d_k))$ and $Q' = \mathrm{Ext}(A, f, (d'_1, \ldots, d'_k))$ be two indecomposable semiregular extensions. Theorem 8.7 says that $Q \simeq Q'$ if and only if $\bar{d}'$ is obtained from $\bar{d}$ using the following four types of transformations:

(T1) the sequence can be permuted;
(T2) any element of the sequence can be replaced by an element from the same coset of $\mathrm{Im}(1-f)$;
(T3) all elements of the sequence can be translated (simultaneously) by an element of A (i.e., we apply the mapping $x \mapsto x + u$ on every element of the sequence);
(T4) all elements of the sequence can be mapped (simultaneously) by an automorphism of A which commutes with f, i.e., by an element of the centralizer $C_{\mathrm{Aut}(A)}(f)$.

An application of the following proposition allows to reduce many enumeration problems to the case $f = 1$. Observe that, for $\psi \in C_{\mathrm{Aut}(A)}(f)$, the mapping $\psi/\mathrm{Im}(1-f)$ defined by $a + \mathrm{Im}(1-f) \mapsto \psi(a) + \mathrm{Im}(1-f)$ is a well defined automorphism of $A/\mathrm{Im}(1-f)$.

Proposition 9.3. *For every A, f, k,*

$$\varepsilon(A, f, k) \leq \varepsilon(A/\mathrm{Im}(1-f), 1, k).$$

Moreover, equality holds if

$$\mathrm{Aut}(A/\mathrm{Im}(1-f)) = \{\psi/\mathrm{Im}(1-f) : \ \psi \in C_{\mathrm{Aut}(A)}(f)\}.$$

In particular, it holds for every A cyclic.

Proof. First, consider $\varepsilon(A, f, k)$. Choose a transversal T to $A/\mathrm{Im}(1-f)$. Due to (T2), we can assume that all $d_i \in T$. Now (T1) say that we count such tuples $\bar{d}$ up to the order of their entries. By (T3) we count up to translation by an element of A modulo $\mathrm{Im}(1-f)$, i.e., applying $x \mapsto x+u$, if $x+u \notin T$, it is replaced by a representative of its coset. And by (T4) we count up to application of an automorphism $\psi \in C_{\mathrm{Aut}(A)}(f)$ modulo $\mathrm{Im}(1-f)$, i.e., if $\psi(x) \notin T$, it is replaced by a representative of its coset.

Next, consider $\varepsilon(A/\mathrm{Im}(1-f), 1, k)$. Here (T2) is trivial, and (T1), (T3), (T4) says that we count tuples $\bar{d}$ up to the order of their entries, translation by an element of $A/\mathrm{Im}(1-f)$ and application of an automorphism $\psi \in \mathrm{Aut}(A/\mathrm{Im}(1-f))$.

Indeed, $\mathrm{Aut}(A/\mathrm{Im}(1-f)) \supseteq \{\psi/\mathrm{Im}(1-f) : \psi \in C_{\mathrm{Aut}(A)}(f)\}$ for any A, f. Since bigger groups have less orbits, we obtain the inequality. If the two sets are equal, we obtain equality. For cyclic groups, the two sets are always equal: given an automorphism ρ of $A/\mathrm{Im}(1-f)$, choose $u \in A$ such that $\rho(1+\mathrm{Im}(1-f)) = u + \mathrm{Im}(1-f)$ and define $\psi(x) = ux$. Indeed, $\psi \in C_{\mathrm{Aut}(A)}(f) = \mathrm{Aut}(A)$ and $\psi/\mathrm{Im}(1-f) = \rho$. □

In particular, if $1-f$ is onto, we obtain that $\varepsilon(A, f, k) = 1$. This is in accordance with Corollary 4.9 which says that this one quandle is the direct product $\mathrm{Aff}(A, f) \times \mathrm{Proj}(k)$.

Automorphisms of $\mathrm{Aut}(A/\mathrm{Im}(1-f))$ are not always quotients of automorphisms from $C_{\mathrm{Aut}(A)}(f)$. For example, if

$$A = \mathbb{Z}_2^3 \text{ and } f = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

then $\mathrm{Im}(1-f) = \langle (1,0,0) \rangle$. Hence $|\mathrm{Aut}(A/\mathrm{Im}(1-f))| = 6$, but the centralizer $C_{\mathrm{Aut}(A)}(f)$ is the subgroup of all upper triangular matrices with 1s on the diagonal and $|\{g/\mathrm{Im}(1-f) : g \in C_{\mathrm{Aut}(A)}(f)\}| = 2$.

In the rest of the paper, we will address the case $f = 1$. The direct approach outlined above is good if k is very small.

Proposition 9.4. *$\varepsilon(A, 1, 2) = 1$ if A is cyclic, and $\varepsilon(A, 1, 2) = 0$ otherwise.*

Proof. Let $Q = \mathrm{Ext}(A, 1, (d_1, d_2))$. The extension is indecomposable if and only if $A = \langle d_1 - d_2 \rangle$. This is not possible unless A is cyclic. Now, due to (T1) and (T3), we can assume that $d_1 = 0$ and $d_2 = u$ is a generator of A. But then $x \mapsto ux$ is an automorphism of A, and thus $\mathrm{Ext}(A, f, (0, u)) \simeq \mathrm{Ext}(A, f, (0, 1))$ by (T4). □

As k grows, an analysis as in the previous proof becomes infeasible (already for $\varepsilon_{p,3}$, this method would result in a tedious case study). To proceed further, we need a better approach.

Let us start calculating $\varepsilon(A, 1, k)$. By (T1), the order of $\bar{d}$ is irrelevant, hence we can record only the numbers c_a, $a \in A$, of occurences of elements of A in the tuple $\bar{d}$. Clearly, the sum $\sum_{a \in A} c_a$ must be equal to k, the length of $\bar{d}$. Let

$$C(A, k) = \{(c_a : a \in A) : \sum_{a \in A} c_a = k \text{ and the corresponding extension is indecomposable}\}.$$

If A is cyclic, the corresponding extension is indecomposable if and only if $\bar{d}$ is not constant, that is, if and only if $c_a \neq k$ for every $a \in A$. Using a standard combinatorial trick [17, Section 3.3], we see that

$$|C(\mathbb{Z}_n, k)| = \binom{n+k-1}{n-1} - n.$$

(If A is not cyclic, the condition is more complicated; the discussion is omitted here.)

Lemma 9.5. *The number $\varepsilon(A, 1, k)$ is equal to the number of orbits of the holomorph $A \rtimes \mathrm{Aut}(A)$ acting on $C(A, k)$ by permuting indices, i.e., under the action $(u, \psi)(c_a : a \in A) = (c_{u+\psi(a)} : a \in A)$.*

Proof. The transformation (T2) is trivial if $f = 1$. The transformation (T3) corresponds to the action of the mapping $x \mapsto x + u$ on the indices of the sequence $\bar{c}$. The transformation (T4) corresponds to the action of the mapping $\psi \in \mathrm{Aut}(A) = C_{\mathrm{Aut}(A)}(1)$ on the indices of $\bar{c}$. Therefore, two sequences $\bar{d}, \bar{d}'$ yield isomorphic quandles if and only if the corresponding sequences $\bar{c}, \bar{c}'$ are in the same orbit of the action of the holomorph $A \rtimes \mathrm{Aut}(A)$ on $C(A, k)$. □

To calculate the number of orbits, we can use Burnside's orbit counting lemma:

$$\varepsilon(A, 1, f) = \frac{1}{|A| \cdot |\mathrm{Aut}(A)|} \cdot \sum_{g \in A \rtimes \mathrm{Aut}(A)} \mathrm{Fix}(g),$$

where $\mathrm{Fix}(g)$ denotes the number of sequences from $C(A, k)$ fixed by g.

Proposition 9.6. *For every k, we have*

$$\varepsilon_{2,k} = \left\lfloor \frac{k}{2} \right\rfloor,$$

$$\varepsilon_{3,k} = \frac{1}{12}\left(k^2 + 6k - 4 + \xi_k\right), \text{ where } \xi_k = \begin{cases} 4 \text{ if } k \equiv 0 \pmod 6, \\ 1 \text{ if } k \equiv 3 \pmod 6, \\ 0 \text{ if } k \equiv 2, 4 \pmod 6, \\ -3 \text{ if } k \equiv 1, 5 \pmod 6, \end{cases}$$

$$\varepsilon_{4,3} = 2, \quad \varepsilon_{5,3} = 2, \quad \varepsilon(\mathbb{Z}_2^2, 1, 3) = 1.$$

Proof. For $\varepsilon_{2,k}$, we consider pairs (c_0, c_1) such that $c_0 + c_1 = k$, $c_i \neq k$. The holomorph acts on indices as the permutation group $\langle (0\ 1) \rangle$, hence the orbits can be uniquely represented by the pairs with $c_0 \leq c_1$, and thus there are $\lfloor \frac{k}{2} \rfloor$ orbits.

For $\varepsilon_{3,k}$, we have $C(\mathbb{Z}_3, k) = \{(c_0, c_1, c_2) : \ c_0 + c_1 + c_2 = k, \ c_i \neq k\}$, and the holomorph acts on indices as the group $G = \langle (0\ 1\ 2), (0\ 1) \rangle = S_3$, the symmetric group on three elements. Applying Burnside's formula, we obtain

$$\varepsilon_{3,k} = \frac{1}{6} \cdot \left(\binom{k+2}{2} - 3 + 2 \cdot \zeta_k + 3 \cdot \left\lfloor \frac{k}{2} \right\rfloor \right),$$

where ζ_k counts the number of triples fixed by a 3-cycle, that is, $\zeta_k = 1$ if $k \equiv 0 \pmod 3$, and $\zeta_k = 0$ otherwise. The last term, $\lfloor \frac{k}{2} \rfloor$, is the number of triples fixed by a 2-cycle: such triples must have two entries equal to a number $\leq k/2$. Replacing $\lfloor \frac{k}{2} \rfloor$ by $\frac{k}{2}$ plus 0 or $-\frac{1}{2}$, depending on parity of k, we obtain the expression stated above.

For $\varepsilon_{4,k}$, we have $C(\mathbb{Z}_4, k) = \{(c_0, c_1, c_2, c_3) : \ c_0 + c_1 + c_2 + c_3 = k, \ c_0 + c_2 \neq k, \ c_1 + c_3 \neq k\}$ (here, the indecomposability condition requires that the differences $d_i - d_j$ contain 1 or 3). The holomorph acts as the group $\langle (0\ 1\ 2\ 3), (1\ 3) \rangle = D_8$, the dihedral group on 8 elements. For $k = 3$, the only admissible quadruples contain 2,1,0,0 or 1,1,1,0 (in an arbitrary order), and thus the Burnside's formula gives $(12 + 2 \cdot 2)/8 = 2$, where the first term comes from $g = 1$, the identity, and the second term comes from the two transpositions.

For $\varepsilon_{5,k}$, we have $C(\mathbb{Z}_5, k) = \{(c_0, ..., c_4) : \ \sum c_i = k, \ c_i \neq k\}$ and the holomorph acts as the group $\langle (0\ 1\ 2\ 3\ 4), (1\ 4)(2\ 3) \rangle$. For $k = 3$, the only admissible quadruples contain 2,1,0,0,0 or 1,1,1,0,0, and thus the Burnside's formula gives $(30 + 5 \cdot 2)/20 = 2$, where the first term comes from $g = 1$ and the second one from the five permutations with two 2-cycles.

For $\varepsilon(\mathbb{Z}_2^2, 1, 3)$, the set $C(\mathbb{Z}_2^2, 3)$ contains only four quadruples consisting of 1,1,1,0, and the holomorph acts as the symmetric group on four elements, hence the Burnside's formula gives $(4 + 6 \cdot 2 + 8 \cdot 1)/24 = 1$, where the first term comes from $g = 1$, the second from transpositions and the third from 3-cycles. □

Corollary 9.7. *There are, up to isomorphism,* $(3p-1)/2$ *quasi-affine quandles of order* $2p$*, for a prime* $p > 2$*.*

In Figure 1, we display the number of quasi-affine and affine quandles of orders up to 15. For prime orders, see Proposition 9.1. For orders $2p$ we use Corollary 9.7. For orders $4, 9, 15$, combine Propositions 9.2 and 9.6. To complete orders 8 and 12, we need a more detailed analysis in the case when $1 - f$ is neither an automorphism, nor zero, see Examples 9.8 and 9.9. The numbers of affine quandles come from [11].

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
quasi-affine	1	1	2	3	4	4	6	9	12	7	10	17	12	10	14
affine	1	1	2	3	4	2	6	7	11	4	10	6	12	6	8

FIGURE 1. The number of quasi-affine and affine quandles of order n, up to isomorphism.

Example 9.8. We will calculate the number of quasi-affine quandles of order 8 up to isomorphism, following the procedure outlined at the beginning of this section. For $k = 1$, we have $|A| = 8$ and we obtain precisely the connected affine quandles of order 8. It is well known (cf. [11]) that there are two of them. For $k = 2$, we have $A = \mathbb{Z}_4$ or $A = \mathbb{Z}_2^2$. Let $\{1, f, g\}$ be representatives of conjugacy classes of $\mathrm{Aut}(\mathbb{Z}_2^2)$, with f of order 2 and g of order 3. The contribution is

$$\varepsilon(\mathbb{Z}_4, 1, 2) + \varepsilon(\mathbb{Z}_4, -1, 2) + \varepsilon(\mathbb{Z}_2^2, 1, 2) + \varepsilon(\mathbb{Z}_2^2, f, 2) + \varepsilon(\mathbb{Z}_2^2, g, 2) = 1 + \varepsilon_{2,2} + 0 + \varepsilon_{2,2} + 1 = 4,$$

using Propositions 9.4, 9.3, 9.4, 9.3, and 4.9, respectively. For $k = 4$, we have $A = \mathbb{Z}_2$ and the contribution is $\varepsilon_{2,4} = 2$. For $k = 8$, we obtain one projection quandle of order 8. The total is $2 + 4 + 2 + 1 = 9$ quasi-affine quandles of order 8 up to isomorphism.

Example 9.9. We will calculate the number of quasi-affine quandles of order 12 up to isomorphism, following the procedure outlined at the beginning of this section. For $k = 1$, we obtain precisely the connected affine quandles of order 12, which decompose to a direct product of one of order 4 and one of order 3. There is precisely one such pair. For $k = 2$, we have $A = \mathbb{Z}_6$, contributing $\varepsilon(\mathbb{Z}_6, 1, 2) + \varepsilon(\mathbb{Z}_6, -1, 2) = \varepsilon_{6,2} + \varepsilon_{2,2} = 2$ quandles, using Propositions 9.4 and 9.3, respectively. For $k = 3$, we have $A = \mathbb{Z}_4$ or $A = \mathbb{Z}_2^2$. Let $\{1, f, g\}$ be representatives of conjugacy classes of $\mathrm{Aut}(\mathbb{Z}_2^2)$, with f of order 2 and g of order 3. The contribution is

$$\varepsilon(\mathbb{Z}_4, 1, 3) + \varepsilon(\mathbb{Z}_4, -1, 3) + \varepsilon(\mathbb{Z}_2^2, 1, 3) + \varepsilon(\mathbb{Z}_2^2, f, 3) + \varepsilon(\mathbb{Z}_2^2, g, 3) = \varepsilon_{4,3} + \varepsilon_{2,2} + 1 + \varepsilon_{2,3} + 1 = 6,$$

using Propositions 9.6, 9.3, 9.6, 9.3, and 4.9, respectively. For $k = 4$, we have $A = \mathbb{Z}_3$, and the contribution is $\varepsilon(\mathbb{Z}_3, 1, 4) + \varepsilon(\mathbb{Z}_3, -1, 4) = 3 + 1 = 4$. For $k = 6$, we have $A = \mathbb{Z}_2$, and the contribution is $\varepsilon_{2,6} = 3$. For $k = 12$, we obtain one projection quandle of order 12. The total is $1 + 2 + 6 + 4 + 3 + 1 = 17$ quasi-affine quandles of order 12 up to isomorphism.

REFERENCES

[1] N. Andruskiewitsch, M. Graña, *From racks to pointed Hopf algebras*, Adv. Math. 178/2 (2003), 177–243.

[2] Y. Bae, *Coloring link diagrams by Alexander quandles*, J. Knot Theory Ramifications 21/10 (2012), 1250094, 13 pp.

[3] C. Bergman, *Universal algebra: Fundamentals and selected topics*, CRC Press, 2011.

[4] M. Bonatto, D. Stanovský, *Commutator theory for quandles*, in progress.

[5] L. Camacho, F. M. Dionísio, E. Picken, *Colourings and the Alexander polynomial*, Kyungpook Math. J. 56/3 (2016), 1017–1045.

[6] J. Demel, M. Demlová, V. Koubek, *Fast algorithms constructing minimal subalgebras, congruences, and ideals in a finite algebra.* Theor. Comput. Sci. 36 (1985), 203–216.

[7] P. Etingof, A. Soloviev, R. Guralnick, *Indecomposable set-theoretical solutions to the quantum Yang-Baxter equation on a set with a prime number of elements*, J. Algebra 242/2 (2001), 709–719.
[8] R. Freese, R. McKenzie, *Commutator theory for congruence modular varieties*, London Mathematical Society Lecture Note Series 125, Cambridge University Press, Cambridge, 1987.
[9] H. Holmes, *Left distributive algebras and knots,* Master's Thesis, Charles University in Prague, 2013. Available at `https://is.cuni.cz/webapps/zzp`
[10] X. Hou, *Automorphism groups of Alexander quandles*, J. Algebra 344 (2011), 373–385.
[11] X. Hou, *Finite modules over* $\mathbb{Z}[t, t^{-1}]$, J. Knot Theory Ramifications 21/8 (2012), 1250079, 28 pp.
[12] A. Hulpke, D. Stanovský, P. Vojtěchovský, *Connected quandles and transitive groups*, J. Pure Appl. Algebra 220 (2016), 735–758.
[13] P. Jedlička, A. Pilitowska, D. Stanovský, A. Zamojska-Dzienio, *The structure of medial quandles*, J. Algebra 443 (2015), 300–334.
[14] P. Jedlička, A. Pilitowska, A. Zamojska-Dzienio, *Free medial quandles*, to appear in Algebra Universalis.
[15] D. Joyce, *Classifying invariant of knots, the knot quandle*, J. Pure Appl. Algebra, 23 (1982), 37–65.
[16] K. Kearnes, *A quasi-affine representation*, Int. J. Algebra Comput. 5/6 (1995), 673–702.
[17] J. Matoušek, J. Nešetřil, *Invitation to Discrete Mathematics*, Clarendon Press, 1998.
[18] G. Murillo, S. Nelson, A. Thompson, *Matrices and finite Alexander quandles*, J. Knot Theory Ramifications 16/6 (2007), 769–778.
[19] R. W. Quackenbush, *Quasi-affine algebras*, Algebra Universalis 20/3 (1985), 318–327.
[20] A. Romanowska, J. D. H. Smith, *Modes*, World Scientific, 2002.
[21] J. J. Rotman, *An introduction to homological algebra*, 2nd Edition, Springer, 2009.
[22] D. Stanovský, *Abelian differential modes are quasi-affine*, Comment. Math. Univ. Carolin. 53/3 (2012), 461–473.
[23] J. Šťovíček, the referee report to [9], 2013.
[24] M. Stronkowski, D. Stanovský, *Embedding general algebras into modules*, Proc. Amer. Math. Soc. 138/8 (2010), 2687–2699.
[25] Á. Szendrei, *Modules in general algebra*, Contributions to general algebra 10 (Klagenfurt, 1997), Heyn, Klagenfurt (1998), 41–53.

(P.J.) Department of Mathematics, Faculty of Engineering, Czech University of Life Sciences, Kamýcká 129, 16521 Praha 6, Czech Republic

(A.P., A.Z.) Faculty of Mathematics and Information Science, Warsaw University of Technology, Koszykowa 75, 00-662 Warsaw, Poland

(D.S.) Department of Algebra, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 18675 Praha 8, Czech Republic

E-mail address: (P.J.) `jedlickap@tf.czu.cz`
E-mail address: (A.P.) `apili@mini.pw.edu.pl`
E-mail address: (D.S.) `stanovsk@karlin.mff.cuni.cz`
E-mail address: (A.Z.) `A.Zamojska-Dzienio@mini.pw.edu.pl`