FREE MEDIAL QUANDLES

PŘEMYSL JEDLIČKA, AGATA PILITOWSKA, AND ANNA ZAMOJSKA-DZIENIO

Abstract. This paper brings the construction of free medial quandles as well as free n-symmetric medial quandles and free m-reductive medial quandles.

1. Introduction

A *medial quandle* Q (or sometimes an *abelian quandle*) is a binary algebra $(Q,*)$, satisfying, for every $x,y,z,u \in Q$,

- $x*x=x$; (idempotency)
- $(x*y)*(z*u)=(x*z)*(y*u)$; (mediality)
- there exists a unique $v \in Q$ such that $x*v=z$. (left quasigroup)

An important example of a medial quandle is an abelian group A with an operation $*$ defined by $a*b=(1-h)(a)+h(b)$, where h is an automorphism of A. This construction is called an *affine* quandle (or sometimes an *Alexander quandle*) and denoted by $\mathrm{Aff}(A,h)$. In the literature [3, 4], the group A is usually considered to be a $\mathbb{Z}[t,t^{-1}]$-module, where $t\cdot a=h(a)$, for each $a\in A$. We shall adopt this point of view here as well and we usually write $\mathrm{Aff}(A,r)$ instead, where r is a ring element.

Medial quandles lie in the intersection of the class of quandles and the class of *modes* [12]. Recent development in quandle theory is motivated by knot theory (see e.g. [1]). The *knot quandle* is a very powerful knot invariant. Quandles have also applications in differential geometry [10] and graph theory [2]. Modes are general idempotent and entropic algebras (algebras with a commutative clone of term operations). Mediality is an other name for entropicity in the binary case. For a more detailed history of medial quandles we refer to [6].

Medial quandles do not form a variety of binary algebras, unless we introduce an additional binary operation $\backslash$ and the identities

$$x\backslash(x*y)\approx y \qquad \text{and} \qquad x*(x\backslash y)\approx y$$

to define the left quasigroup property equationally. When studying varieties, free algebras play an important role. They are the most general objects in the variety in the sense that the only equations that hold between their elements are those that follow from the defining identities. There are two natural applications then. First, the equational theories can be characterized directly from the algebraic structure of free algebras. It is well known that the lattice of all subvarieties of a variety $\mathcal{V}$ is dually isomorphic to the lattice of fully invariant congruences of the free $\mathcal{V}$-algebra on (infinite) countably many generators. Second, the knowledge of free algebras generated by finitely many elements allows one to construct *normal forms* i.e. uniquely determined words which represent the equivalence classes of equal words in free algebras. Then one can work on the *word problem*.

The structure of free medial quandles remained open for a long time. There were only results about more general classes, i.e. general free modes were investigated by Stronkowski [14] and

Date: December 15, 2015.

2010 *Mathematics Subject Classification.* Primary: 20N02, 08B20.

Key words and phrases. Quandles, medial quandles, binary modes, free algebras.

general free quandles by Joyce [8] and Stanovský [13]. Or there were some special cases described, like *involutory* medial quandles, that means medial quandles satisfying additionally $x*(x*y) \approx y$.

Theorem 1.1 ([8, Theorem 10.5]). *Let $n \in \mathbb{N}$. Denote by F the subset of the quandle $\mathrm{Aff}(\mathbb{Z}^n, -1)$ consisting of those n-tuples where at most one coordinate is odd. Then $(F, *)$ is a free $(n+1)$-generated involutory medial quandle over $\{(0,\dots,0), (1,0,\dots,0), (0,1,0,\dots,0), \dots, (0,\dots,0,1)\}$.*

Here we generalize the result of Joyce but not directly. We choose the path started in [6] instead and we study certain permutation groups acting on quandles, called *displacement* groups. It turns out that, in the case of free medial quandles, these groups are free $\mathbb{Z}[t,t^{-1}]$-modules and we can construct the free medial quandles based on these modules. Another important result is that the free medial quandles embed into affine quandles. This shows that the variety of medial quandles is generated by affine quandles.

Next we focus on two special classes: n-symmetric and m-reductive medial quandles which play a significant role within the class of finite medial quandles. A quandle $(Q,*)$ is *n-symmetric*, if it satisfies the identity

$$\underbrace{x*(x*\cdots*(x}_{n-times}*y)\cdots) \approx y.$$

We construct here free n-symmetric medial quandles and we prove that free n-symmetric quandles embed into products of affine quandles over modules over Dedekind domains. This is useful especially when studying finite medial quandles since each finite left quasigroup is n-symmetric, for some natural number n.

A quandle $(Q,*)$ is *m-reductive*, if it satisfies the identity

$$(\cdots(x*\underbrace{y)*\cdots*y)*y}_{m-times} \approx y.$$

A quandle is called reductive if it is m-reductive, for some $m \in \mathbb{N}$. Reductivity turns out to be a very important notion in the study of medial quandles as each finite medial quandle embeds into a product of a reductive quandle and a quasigroup [7].

The paper contents four Sections. In Section 2 we recall and present some facts about general medial quandles. Section 3 contains the main results. Theorem 3.3 gives a description of the free medial quandles and Theorem 3.5 a construction of affine quandles into which the free quandles embed. Section 4 is devoted to n-symmetric and m-reductive free medial quandles. In both cases, the displacement group of the free algebra turns out to be a free $\mathbb{Z}[t]/(f)$-module, for a suitable polynomial f. The description of the free quandles in these varieties is analogous as for general medial quandles.

Note that when studying left quasigroups, important tools are the mappings $L_e : x \mapsto e*x$, called the left translations. We use also the right translations $R_e : x \mapsto x*e$. The idempotency and the mediality imply that both L_e and R_e are endomorphisms. The left quasigroup property means that L_e is an automorphism.

2. Preliminaries

This section recalls some important notions from [6] where the structure of medial quandles was described. Key ingredients are two permutation groups acting on quandles.

Definition 2.1. Let Q be a quandle. The *left multiplication group* of Q is the group

$$\mathrm{LMlt}(Q) = \langle L_x;\ x \in Q \rangle .$$

The *displacement group* is the group

$$\mathrm{Dis}(Q) = \left\langle L_x L_y^{-1};\ x,y \in Q \right\rangle .$$

It was proved in [5, Proposition 2.1] that the actions of both groups on Q have the same orbits. We use, in the sequel, the word *orbit* plainly without explicitly mentioning the acting groups. The orbit of Q containing x is denoted by Qx and the stabilizer subgroup of x is denoted by $\mathrm{Dis}(Q)_x$. For two permutations α, β, we write $\alpha^\beta = \beta\alpha\beta^{-1}$. The commutator is defined by $[\beta, \alpha] = \alpha^\beta\alpha^{-1}$. The identity permutation is denoted by 1.

It is also useful to understand the structure of the displacement group.

Lemma 2.2 ([5, Proposition 2.1])**.** $\mathrm{Dis}(Q) = \{L_{x_1}^{\varepsilon_1} L_{x_2}^{\varepsilon_2} \cdots L_{x_k}^{\varepsilon_k};\ x_i \in Q, \varepsilon_i = \pm 1, \sum \varepsilon_i = 0\}$.

From this lemma, we can clearly see that $\mathrm{Dis}(Q)$ is a normal subgroup of $\mathrm{LMlt}(Q)$. Moreover, in our context, the group is commutative.

Proposition 2.3 ([5, Proposition 2.4])**.** *Let Q be a quandle. Then Q is medial if and only if* $\mathrm{Dis}(Q)$ *is abelian.*

Since $\mathrm{Dis}(Q)$ is abelian, conjugations by elements from the same coset of $\mathrm{Dis}(Q)$ yield the same results.

Lemma 2.4. *Let Q be a medial quandle. Let $\alpha \in \mathrm{Dis}(Q)$ and $x, y \in Q$. Then $\alpha^{L_x} = \alpha^{L_y}$.*

Proof. $\alpha^{L_x} = L_x\alpha L_x^{-1} = L_x\alpha L_x^{-1}L_yL_y^{-1} = L_xL_x^{-1}L_y\alpha L_y^{-1} = \alpha^{L_y}$ due to the abelianess of $\mathrm{Dis}(Q)$. □

From now on, by writing α^L, we mean α^{L_x}, for an arbitrary $x \in Q$, since the conjugation does not depend on the element x.

It is easy to see that, for $\alpha \in \mathrm{Aut}(Q)$ and $x \in Q$, $L_{\alpha(x)} = L_x^\alpha$. In particular, for $\alpha = L_y$, we obtain $L_{y*x} = L_x^{L_y}$. This implies that $\mathrm{LMlt}(Q)$ has only few generators. On the other hand, DisQ, in spite of being a subgroup of $\mathrm{LMlt}(Q)$, has usually more generators than $\mathrm{LMlt}(Q)$.

Proposition 2.5. *Let Q be a medial quandle generated by $X \subset Q$ and choose $z \in X$. Then*

- *the group* $\mathrm{LMlt}(Q)$ *is generated by* $\{L_x;\ x \in X\}$*;*
- *the group* $\mathrm{Dis}(Q)$ *is generated by* $\{(L_xL_z^{-1})^{L^k};\ x \in X,\ k \in \mathbb{Z}\}$*.*

Proof. The generating set for $\mathrm{LMlt}(Q)$ is obtained by the induction using $L_{x*y} = L_xL_yL_x^{-1}$ and $L_{x\backslash y} = L_x^{-1}L_yL_x$.

Suppose now $\alpha \in \mathrm{Dis}(Q)$. By Lemma 2.2 and the previous observation we can suppose $\alpha = L_{x_1}^{\varepsilon_1}L_{x_2}^{\varepsilon_2}\cdots L_{x_n}^{\varepsilon_n}$, where $x_i \in X$ and $\varepsilon_i = \pm 1$ with $\sum \varepsilon_i = 0$, for $1 \le i \le n$. We prove the claim by an induction on n. For $n = 2$ the claim is true.

Let the induction hypothesis holds for all words of length at most $n-2$. If $\varepsilon_1 = \varepsilon_n$ then clearly $w = w_1w_2$ with $w_i \in \mathrm{Dis}(Q)$ and we use the induction hypothesis. Let now $\varepsilon_1 = 1$ and $\varepsilon_n = -1$. Then $w = L_{x_1}w'L_{x_n}^{-1}$ and w' is, by the induction hypothesis, a product of elements from $\{(L_xL_z^{-1})^{L^k};\ x \in X,\ k \in \mathbb{Z}\}$. But

$$w = L_{x_1}w'L_{x_1}^{-1}L_{x_1}L_z^{-1}L_zL_{x_n}^{-1} = (w')^L(L_{x_1}L_z^{-1})(L_{x_n}L_z^{-1})^{-1}$$

proving the claim. The argument is similar for $\varepsilon_1 = -1$ and $\varepsilon_n = 1$. □

This result cannot be much improved – it is shown in Proposition 3.2 that the displacement group of a free medial quandle is not finitely generated.

The abelian group $\mathrm{Dis}(Q)$ can be easily endowed with the structure of a $\mathbb{Z}[t, t^{-1}]$-module, it suffices to pick an automorphism of $\mathrm{Dis}(Q)$. A natural choice is the inner automorphism $\alpha \mapsto \alpha^L$. Hence, from now on, the group $\mathrm{Dis}(Q)$ is treated, depending on the situation, either as a permutation group acting on Q or as an R-module, where R is a suitable image of $\mathbb{Z}[t, t^{-1}]$, with the action of t defined by $\alpha^t = \alpha^L$. Note that, for $f \in \mathbb{Z}[t, t^{-1}]$, $\alpha^f = \alpha^{f(L)}$.

Example 2.6. Let $f = (1-t)^2$. Then $\alpha^f = \alpha^{1-2t+t^2} = \alpha^{f(L)} = \alpha^{1-2L+L^2} = \alpha(\alpha^L)^{-2}\alpha^{L^2}$.

It was proved in [6, Proposition 3.2] that, for any $x \in Q$, the orbit Qx is affine over $\mathrm{Dis}(Q)/\mathrm{Dis}(Q)_x$ and we can naturally identify the sets Qx and $\mathrm{Dis}(Q)/\mathrm{Dis}(Q)_x$ by defining the group operation on Qx as:

$$\alpha(x) + \beta(x) = \alpha\beta(x) \qquad \text{and} \qquad -\alpha(x) = \alpha^{-1}(x).$$

The group so defined is denoted by $\mathrm{Orb}_Q(x)$ and called the *orbit group* for Qx. Moreover, $\mathrm{Dis}(Q)_x$ is a submodule of $\mathrm{Dis}(Q)$: suppose $\alpha(x) = x$; then $\alpha^t(x) = L_x\alpha L_x^{-1}(x) = x$. This means that $\mathrm{Dis}(Q)/\mathrm{Dis}(Q)_x$ is a $\mathbb{Z}[t,t^{-1}]$-module and we can call $\mathrm{Orb}_Q(x)$ the *orbit module* for Qx.

3. Free medial quandle

In this section we present the free medial quandles. Regarding the generating set, we see that, in any quandle Q, for all $x, y \in Q$, $y * x \in Qx$ as well as $y\backslash x \in Qx$. Hence each orbit has to contain at least one generator.

Lemma 3.1. *Let Q be a quandle generated by $X \subset Q$. Then the set $X \cap Qx$ is nonempty, for each $x \in Q$.*

The following proposition characterizes the free medial quandles. Formally, it is pronounced as a sufficient condition only but we can see in Theorem 3.3 that such an object exists, making the condition necessary too.

Proposition 3.2. *Let F be a medial quandle generated by a set $X \subset F$. Choose $z \in X$ arbitrarily. Then F is free over X if the following conditions are satisfied:*

1. *each element of X lies in a different orbit;*
2. *$\mathrm{Dis}(F)$ is a free $\mathbb{Z}[t,t^{-1}]$-module with $\{L_xL_z^{-1};\ x \in X \setminus \{z\}\}$ as a free basis;*
3. *the action of $\mathrm{Dis}(F)$ on F is free.*

Proof. Observe first that, for any $y \in F$, there exists exactly one $x \in X$ and exactly one $\alpha \in \mathrm{Dis}(F)$ such that $y = \alpha(x)$. Indeed, the existence of x, comes from Lemma 3.1, and its uniqueness from (1). The uniqueness of α is due to (3).

Let Q be a medial quandle and let $Y \subset Q$. Let ψ be a mapping $X \to Y$. We prove that ψ can be extended to a homomorphism $\Psi : F \to Q$. We define first a $\mathbb{Z}[t,t^{-1}]$-module homomorphism $\Phi : \mathrm{Dis}(F) \to \mathrm{Dis}(Q)$ on the basis of $\mathrm{Dis}(F)$ by setting $\Phi(L_xL_z^{-1}) = L_{\psi(x)}L_{\psi(z)}^{-1}$. Note that $\Phi(\alpha^L) = \Phi(\alpha^t) = \Phi(\alpha)^t = \Phi(\alpha)^L$. Now set

$$\Psi(\alpha(x)) = \Phi(\alpha)(\psi(x)), \qquad \text{for all } \alpha \in \mathrm{Dis}(F) \text{ and } x \in X.$$

Mapping Ψ is well defined since every element of F has a unique representation by α and x.

$$\Psi(\alpha(x)) * \Psi(\beta(y)) = \Phi(\alpha)(\psi(x)) * \Phi(\beta)(\psi(y)) = L_{\Phi(\alpha)(\psi(x))}\Phi(\beta)(\psi(y)) = L_{\psi(x)}^{\Phi(\alpha)}\Phi(\beta)(\psi(y)) =$$
$$\Phi(\alpha)L_{\psi(x)}\Phi(\alpha^{-1})\Phi(\beta)L_{\psi(x)}^{-1}L_{\psi(x)}L_{\psi(y)}^{-1}(\psi(y)) = \Phi(\alpha)(\Phi(\alpha^{-1}\beta))^L L_{\psi(x)}L_{\psi(y)}^{-1}(\psi(y)) =$$
$$\Psi(\alpha(\alpha^{-1}\beta)^L L_xL_y^{-1}(y)) = \Psi(\alpha L_x\alpha^{-1}\beta(y)) = \Psi(L_{\alpha(x)}\beta(y)) = \Psi(\alpha(x) * \beta(y))$$

and Ψ is a homomorphism that extends ψ. □

In the sequel, we use the following notation: let X be a set. We choose $z \in X$ arbitrarily and we denote by X^- the set $X \setminus \{z\}$. We often do not specify the element z since we actually rarely need it explicitly. Let now R be a ring and consider the free R-module of rank $|X^-|$, i.e. $M = \bigoplus_{x \in X^-} R$. We then choose a free basis of M, let us say $\{e_i;\ i \in X^-\}$, and by defining $e_z = 0 \in M$, we have defined e_i as an element of M, for each $i \in X$.

Theorem 3.3. *Let X be a set and let $z \in X$. Denote by X^- the set $X \smallsetminus \{z\}$. Let $M = \bigoplus_{x\in X^-} \mathbb{Z}[t,t^{-1}]$. Let $\{e_i;\ i \in X^-\}$ be a free basis of M. Moreover, let $e_z = 0 \in M$. Let us denote by F the set $M \times X$ equipped with the operation*

$$(a,i)*(b,j) = ((1-t)\cdot a + t\cdot b + e_i - e_j, j).$$

Then $(F,*)$ is a free medial quandle over $\{(0,i);\ i \in X\}$.

Proof. The idempotency is evident. The mediality is proved by the observation that

$$((a,i)*(b,j))*((c,k)*(d,n)) = ((1-t)^2\cdot a+(t-t^2)\cdot(b+c)+t^2\cdot d+(1-t)\cdot e_i+t\cdot(e_j+e_k)-(1+t)\cdot e_n, n).$$

The left-quasigroup operation is given by the formula

$$(a,i)\backslash(b,j) = ((1-t^{-1})\cdot a + t^{-1}\cdot(b+e_j-e_i), j).$$

Hence F is a medial quandle.

We know now that F is a medial quandle and we want to prove its freeness by Proposition 3.2.

We start with analyzing the structure of $\mathrm{Dis}(F)$.

$$\begin{aligned} L_{(a,i)}L^{-1}_{(b,j)}((c,k)) &= (a,i)*((b,j)\backslash(c,k)) = (a,i)*((1-t^{-1})\cdot b + t^{-1}\cdot(c+e_k-e_j), k) = \\ &((1-t)\cdot a + (t-1)\cdot b + c + e_k - e_j + e_i - e_k, k) = (c + (1-t)\cdot(a-b) + e_i - e_j, k). \end{aligned}$$

In particular, $L_{(0,i)}L^{-1}_{(0,z)}((c,k)) = (c+e_i,k)$. Now we prove by induction that

$$\left(L_{(0,i)}L^{-1}_{(0,z)}\right)^{L^n}((c,j)) = (c+t^n\cdot e_i, j), \qquad \text{for each } i\in X^-, j\in X \text{ and } n\in\mathbb{Z}.$$

The case $n=0$ was already proved. Now suppose $n>0$.

$$\begin{aligned} &\left(L_{(0,i)}L^{-1}_{(0,z)}\right)^{L^n}((c,j)) = L_{(0,z)}\left(L_{(0,i)}L^{-1}_{(0,z)}\right)^{L^{n-1}} L^{-1}_{(0,z)}((c,j)) = \\ &L_{(0,z)}\left(L_{(0,i)}L^{-1}_{(0,z)}\right)^{L^{n-1}}((t^{-1}\cdot(c+e_j),j)) = L_{(0,z)}((t^{-1}\cdot(c+e_j)+t^{n-1}\cdot e_i, j)) = (c+t^n\cdot e_i, j). \end{aligned}$$

The case $n<0$ is analogous. Moreover, from this we see that $(L_{(0,i)}L^{-1}_{(0,z)})^f\ ((c,j)) = (c+f\cdot e_i, j)$, for any $c\in M$, $f\in\mathbb{Z}[t,t^{-1}]$ and $i,j\in X$.

Let $\left((f_i)_{i\in X^-}, j\right)$ be in F. We now prove that this element lies in the subquandle generated by $\{(0,i);\ i\in X\}$. But it is not difficult to see that

$$\left((f_i)_{i\in X^-}, j\right) = \prod_{i\in X^-}\left(L_{(0,i)}L^{-1}_{(0,z)}\right)^{f_i}\ ((0,j)).$$

The product is finite since only finitely many f_i are non-zero. Hence $\langle\{(0,i);\ i\in X\}\rangle = F$. Moreover, we see that different generators lie in different orbits.

Since the set $\left\{\left(L_{(0,i)}L^{-1}_{(0,z)}\right)^{L^n}; i\in X, n\in\mathbb{Z}\right\}$ generates $\mathrm{Dis}(F)$, due to Proposition 2.5, we see that $\mathrm{Dis}(F)$ acts freely on every orbit of F. That means also that $\mathrm{Dis}(F)$ is isomorphic to M and $\{L_{(0,i)}L_{(0,z)};\ i\in X^-\}$ is clearly its free basis. According to Proposition 3.2, F is free over $\{(0,i);\ i\in X\}$. □

In [6], the structure of medial quandles was represented using a heterogeneous structure called the indecomposable affine mesh. We do not recall the definition here as it is not needed, we just remark that the free medial quandle now constructed is the sum of the affine mesh

$$\Big(\big(\bigoplus_{x\in X^-}\mathbb{Z}[t,t^{-1}]\big)_{i\in X};\ (1-t)_{i,j\in X};\ (e_i-e_j)_{i,j\in X}\Big).$$

Following universal algebra terminology, subquandles of affine quandles are called *quasi-affine*. Every (both sided) cancellative medial quandle is quasi-affine – to see this we can either use a result by Kearnes [9] for idempotent cancellative algebras having a central binary operation or a result by Romanowska and Smith (see e.g. [12]) for cancellative modes. Nevertheless, a direct proof is simple.

Proposition 3.4. *Let Q be a cancellative medial quandle. Then Q embeds into any of its orbits.*

Proof. R_x is an endomorphism of Q, for each $x \in Q$. The right cancellativity ensures that R_x is injective. Hence, for each $x \in Q$, R_x embeds Q into Qx. $\square$

The free medial quandle, we have constructed, is cancellative and therefore it can be represented as a subquandle of an affine quandle.

Theorem 3.5. *Let X be a set. The free medial quandle over X is isomorphic to a subquandle of the affine quandle $M = \mathrm{Aff}(\bigoplus_{x\in X^-} \mathbb{Z}[t,t^{-1}], t)$.*

Proof. Let $\Lambda : \bigoplus_{x\in X^-} \mathbb{Z}[t,t^{-1}] \to \bigoplus_{x\in X^-} \mathbb{Z}$ be the group homomorphism induced by the evaluation homomorphism $\mathbb{Z}[t,t^{-1}] \to \mathbb{Z};\ t \mapsto 1$. Denote by $Q = \{a \in M;\ \Lambda(a) = e_i, \text{ for some } i \in X\}$. Then, Q is a subquandle of M, since

$$\Lambda(L_a(b)) = \Lambda((1-t)\cdot a + t\cdot b) = 0\cdot\Lambda(a) + 1\cdot\Lambda(b) = \Lambda(b)$$

and analogously $\Lambda(L_a^{-1}(b)) = \Lambda(b)$. We shall prove that Q is a free quandle over $\{e_x;\ x \in X\}$.

Take the quandle F from Theorem 3.3. Note that the orbit $F(0,z)$ is isomorphic to M through the bijection $(a,z) \mapsto a$. Now consider the embedding $R_{(0,z)} : F \to F(0,z)$. Clearly $R_{(0,z)}((0,i)) = (e_i, 0)$. Therefore the subquandle of M generated by $Y = \{e_x;\ x \in X\}$ is free.

The only thing left to prove is to show that $Q = \langle Y\rangle$. Clearly $Y \subset Q$ and Q is a subquandle of M, hence $Q \supseteq \langle Y\rangle$.

On the other hand, for $Q \subseteq \langle Y\rangle$, we notice that $Q = \{a \in M;\ a \equiv e_i \pmod{1-t}, \text{ for some } i \in X\}$. Moreover, we have $(L_{e_x}L_{e_z}^{-1})^{L^n} : Q \to Q;\ u \mapsto u + (1-t)t^n \cdot e_x$, with an analogous proof as in Theorem 3.3. Then $(L_{e_x}L_{e_z}^{-1})^{f(L)}(u) = u + (1-t)f\cdot e_x$, for each $f \in \mathbb{Z}[t,t^{-1}]$. Now, for each element $a \in Q$, we have $a = e_i + (1-t)g$, for some $i \in X$ and $g = (g_x)_{x\in X^-} \in M$. Hence, we have

$$a = \prod_{x\in X^-} \left(L_{e_x}L_{e_z}^{-1}\right)^{g_x(L)}(e_i).$$

Therefore $a \in \langle Y\rangle$. $\square$

Example 3.6. We describe now the free medial quandle on three generators. Let $X = \{0,1,2\}$, let $e_1 = (1,0)$, $e_2 = (0,1)$ and $e_0 = (0,0)$. Now $M = \mathrm{Aff}(\mathbb{Z}[t,t^{-1}] \times \mathbb{Z}[t,t^{-1}], t)$ and $\Lambda : \mathbb{Z}[t,t^{-1}] \times \mathbb{Z}[t,t^{-1}] \to \mathbb{Z}^2$ is the group homomorphism induced by the evaluation homomorphism $\mathbb{Z}[t,t^{-1}] \to \mathbb{Z}$; $t \mapsto 1$. Denote by $Q = \{a \in M;\ \Lambda(a) \in \{(0,0),(1,0),(0,1)\}\}$. By Theorem 3.5, Q is a subquandle of M and it is the free quandle generated by the set $\{(0,0),(1,0),(0,1)\}$. For example, the element $a = (1-t, 1+t-t^2)$ lies in Q since $\Lambda(a) = (0,1)$. Now a can be represented as $(0,1)+(1-t)(1,t) = (0,1)+(1-t)\cdot(1,0)+(1-t)t\cdot(0,1) = (L_{(1,0)}L_{(0,0)}^{-1})(L_{(0,1)}L_{(0,0)}^{-1})^L(0,1) = (L_{e_1}L_{e_0}^{-1})(L_{e_2}L_{e_0}^{-1})^L(e_2)$.

4. Free quandles in subvarieties

In this section we study free n-symmetric and free m-reductive medial quandles. Both types of varieties have a similar property: they can be characterized by an identity on $\mathrm{Dis}(Q)$.

Definition 4.1. Let $I \subset \mathbb{Z}[t,t^{-1}]$. We say that a medial quandle Q is an I-quandle, if $\alpha^f = 1$, for each $\alpha \in \mathrm{Dis}(Q)$ and $f \in I$.

If I is an ideal of $\mathbb{Z}[t,t^{-1}]$ and a $\mathbb{Z}[t,t^{-1}]$-module M satisfies the identity $f\cdot a = 0$, for each $a \in M$ and $f \in I$, then M can be viewed as a module over $\mathbb{Z}[t,t^{-1}]/I$.

In our context, the set I shall usually be a principal ideal, that means $I = (f)$, for some $f \in \mathbb{Z}[t,t^{-1}]$. We than write that Q is an f-quandle, rather than $\{f\}$-quandle or (f)-quandle.

If, moreover, $f = \sum_{r=0}^{n} c_r t^r$ and the coefficient c_0 is invertible then $\mathbb{Z}[t,t^{-1}]/f \cong \mathbb{Z}[t]/f$ since $t^{-1} \equiv -\big(\sum_{r=1}^{n} c_r t^{r-1}\big)\cdot c_0^{-1} \pmod f$. We use these remarks since working with the ring $\mathbb{Z}[t]/f$ is often easier than working with the ring $\mathbb{Z}[t,t^{-1}]$.

We prepared the framework of I-quandles to work with symmetric and reductive medial quandles at once. First note that if Q is an I-quandle then clearly $\mathrm{Orb}_Q(x)^I = \{\alpha^f(x) \mid \alpha \in \mathrm{Dis}(Q),\ f \in I\} = \{x\}$. On the other hand, let $\alpha^f(x) = x$ for arbitrary $\alpha \in \mathrm{Dis}(Q)$, $f \in I$ and each $x \in Q$. Hence the action of α^f on Q is trivial and this means $\alpha^f = 1$ since $\mathrm{Dis}(Q)$ is faithful. This immediately gives the following lemma.

Lemma 4.2. *Let Q be a medial quandle and let $I \subset \mathbb{Z}[t,t^{-1}]$. Then Q is an I-quandle if and only if $\mathrm{Orb}_Q(x)^I = \{x\}$, for each $x \in Q$.*

Recall that a quandle Q is n-symmetric, if $L_x^n = 1$, for each $x \in Q$.

Proposition 4.3. *A medial quandle Q is n-symmetric if and only if Q is a $(\sum_{r=0}^{n-1} t^r)$-quandle.*

Proof. According to [6, Proposition 7.2], a medial quandle Q is n-symmetric if and only if, for each $x \in Q$

$$\sum_{r=0}^{n-1} (1-\varphi)^r \alpha(x) = x,$$

where $\varphi : Qx \to Qx$ is defined by $\alpha(x) \mapsto [\alpha, L](x)$.

Then $(1-\varphi)(\alpha(x)) = \alpha(x) - [\alpha, L](x) = \alpha[L,\alpha](x) = \alpha^L(x) = \alpha^t(x)$ and therefore it means that $\alpha^{\sum_{r=0}^{n-1} t^r}(x) = x$, for each $x \in Q$. Hence, according to Lemma 4.2, Q is n-symmetric if and only if it is a $(\sum_{r=0}^{n-1} t^r)$-quandle. $\square$

Recall that a quandle Q is m-reductive, if $R_x^m(y) = x$, for all $x, y \in Q$.

Proposition 4.4. *A medial quandle Q is m-reductive if and only if it is a $(1-t)^{m-1}$-quandle.*

Proof. According to [6, Proposition 6.2], a medial quandle Q is m-reductive if and only if $\varphi^{m-1}\alpha(x) = x$, for each $x \in Q$, where $\varphi : Qx \to Qx$ is defined by $\alpha(x) \mapsto [\alpha, L](x)$.

Then $\varphi(\alpha(x)) = [\alpha, L](x) = \alpha(\alpha^{-1})^L(x) = \alpha^{(1-t)}(x)$ and therefore it means that $\alpha^{(1-t)^{m-1}}(x) = x$, for each x. Hence, according to Lemma 4.2, Q is m-reductive if and only if it is a $(1-t)^{m-1}$-quandle. $\square$

Both the mentioned polynomials, i.e. $\sum_{r=0}^{n-1} t^r$ and $(1-t)^{m-1}$ have the property that the leading as well as the absolute coefficients are invertible.

In this case, not only $\mathrm{Dis}(Q)$ can be treated as a $\mathbb{Z}[t]/f$-module but it has less generators even as a group.

Proposition 4.5. *Let $f = \sum_{r=0}^{s} c_r t^r$ be a polynomial with c_0 and c_k invertible and let Q be an f-quandle generated by $X \subset Q$. Let $z \in X$ be an arbitrary element. Then $\mathrm{Dis}(Q)$ is generated by $\{(L_x L_z^{-1})^{L^r};\ x \in X \smallsetminus \{z\}$ and $0 \le r < s\}$.*

Proof. According to Proposition 2.5, the group $\mathrm{Dis}(Q)$ is generated by $(L_x L_z^{-1})^{L^k}$, for $x \in X \smallsetminus \{z\}$ and $k \in \mathbb{Z}$. But now

$$(L_x L_z^{-1})^{L^{-1}} = (L_x L_z^{-1})^{t^{-1}} = (L_x L_z^{-1})^{-(\sum_{r=0}^{s-1} c_{r+1} t^r) c_0^{-1}} = \prod_{r=0}^{s-1} \left((L_x L_z^{-1})^{L^r}\right)^{-c_{r+1} c_0^{-1}},$$

$$(L_x L_z^{-1})^{L^s} = (L_x L_z^{-1})^{t^s} = (L_x L_z^{-1})^{-(\sum_{r=0}^{s-1} c_r t^r) c_s^{-1}} = \prod_{r=0}^{s-1} \left((L_x L_z^{-1})^{L^r}\right)^{-c_r c_s^{-1}}.$$

Similarly for all $(L_x L_z^{-1})^{L^r}$, where $r < -1$ or $r > s$. $\square$

The structure of free medial f-quandles can be described exactly in the same way as the structure of general free medial quandles.

Proposition 4.6. *Let $f \in \mathbb{Z}[t]$ be a polynomial with the leading and the absolute coefficients invertible. Let F be an f-quandle generated by a set $X \subset F$. Choose $z \in X$ arbitrarily. Then F is a free f-quandle over X if the following conditions are satisfied:*

1. *each element of X lies in a different orbit;*
2. $\mathrm{Dis}(F)$ *is a free $\mathbb{Z}[t]/f$-module with $\{L_x L_z^{-1};\ x \in X \smallsetminus \{z\}\}$ as a free basis;*
3. *the action of* $\mathrm{Dis}(F)$ *on F is free.*

Proof. The proof is nearly the same as the proof of Proposition 3.2. The only difference is that displacements groups appearing here are $\mathbb{Z}[t]/f$-modules. $\square$

Theorem 4.7. *Let $f \in \mathbb{Z}[t]$ be a polynomial with the leading and the absolute coefficients invertible. Let X be a set. Let $M = \bigoplus_{s \in X^-} \mathbb{Z}[t]/f$. Let us denote by F the set $M \times X$ equipped with the operation*

$$(a, i)*(b, j) = ((1-t)\cdot a + t\cdot b + e_i - e_j, j).$$

Then $(F, *)$ is a free f-quandle over $\{(0, i);\ i \in X\}$.

Proof. The proof is nearly the same as of Theorem 3.3, with the usage of Proposition 4.6. The only thing to show is that $\alpha^f = 1$, for all $\alpha \in \mathrm{Dis}(F)$. But this follows from $\mathrm{Dis}(F) \cong M$. $\square$

Non-trivial reductive medial quandles are never right-cancellative since the multiplication by $(1-t)$ is not injective. On the other hand, free n-symmetric quandles are cancellative and we can embed them in their orbits. Moreover, the polynomial $\sum t^r$ is a product of cyclotomic polynomials.

Theorem 4.8. *Let X be a set. Let $n \in \mathbb{N}$ and let $\sum_{r=0}^{n-1} t^r = \prod_{j \in \mathcal{J}} f_j$, where f_j are irreducible in $\mathbb{Z}[t]$ and $M_j = \mathrm{Aff}(\bigoplus_{x \in X^-} \mathbb{Z}[t]/f_j, t)$, for each $j \in \mathcal{J}$. Each free n-symmetric medial quandle is isomorphic to the subquandle of $\prod_{j \in \mathcal{J}} M_j$ generated by $\{(e_i)_{j \in \mathcal{J}};\ i \in X\}$.*

Proof. We show that the subquandle $Q = \{(a_j)_{j \in \mathcal{J}};\ \exists i \in X\ \forall j \in \mathcal{J}\ a_j \equiv e_i \pmod{(1-t)}\}$ of $\prod_{j \in \mathcal{J}} M_j$ is a free n-symmetric medial quandle over $\{(e_i, e_i, \ldots, e_i);\ i \in X\}$.

Denote by $f = \sum_{r=0}^{n-1} t^r$. It is well known that $t^n - 1 = (t-1)f = (t-1)\prod_{j \in \mathcal{J}} f_j$ and all the polynomials f_j are pairwise different. Therefore, according to the Chinese remainder theorem, $\mathbb{Z}[t]/f \cong \bigoplus_{j \in \mathcal{J}} \mathbb{Z}[t]/f_j$. The rest is the same as in Theorem 3.5. $\square$

Example 4.9. Consider $n = 2$, i.e. involutory medial quandles. Since $\mathbb{Z}[t]/(t+1) \cong \mathbb{Z}$ and $t \equiv -1 \pmod{(t+1)}$, according to Theorem 4.8, the free $|X|$-generated involutory medial quandle is isomorphic to the subquandle of $\mathrm{Aff}(\bigoplus_{x \in X^-} \mathbb{Z}, -1)$ that consists of those $|X^-|$-tuples congruent to some e_i modulo 2. This confirms the result of Joyce (Theorem 1.1).

Theorem 4.8 can be reformulated as follows: let ζ_k be the primitive k-th root of unity in $\mathbb{C}$. It is well known that $\mathbb{Z}[t]/(1+t+\cdots+t^{n-1}) \cong \prod_{k|n,k>1} \mathbb{Z}[\zeta_k]$. Hence the free $|X|$-generated n-symmetric quandle is the subquandle of $\prod_{k|n,k>1} \mathrm{Aff}(\bigoplus_{x \in X^-} \mathbb{Z}[\zeta_k], \zeta_k)$ generated by $\{(e_i, e_i, \ldots, e_i);\ i \in X\}$.

Example 4.10. Consider $|X| = 2$. Then the free 2-generated n-symmetric medial quandle F is the subquandle of $\prod_{k|n,k>1} \mathrm{Aff}(\mathbb{Z}[\zeta_k], \zeta_k)$ generated by $(0, \ldots, 0)$ and $(1, \ldots, 1)$. The subquandle F consists of those tuples $(a_k)_{k|n,k>1}$, that either $a_k \equiv 0 \pmod{(1-\zeta_k)}$, for all $k|n, k > 1$, or $a_k \equiv 1 \pmod{(1-\zeta_k)}$, for all $k|n, k > 1$.

Every finite quandle is n-symmetric, for some n. For studying finite medial quandles, it is nice to hear that we do not need always consider $\mathbb{Z}[t, t^{-1}]$-modules but we can sometimes restrain or focus to nicer rings, or even domains.

Corollary 4.11. *Let $n \in \mathbb{N}$. The variety of n-symmetric medial quandles is generated by quandles that are polynomially equivalent to modules over Dedekind domains.*

Proof. It is well known [15] that $\mathbb{Z}[\zeta_k]$ is a Dedekind domain, for each k. Free n-symmetric quandles embed into products of $\mathrm{Aff}(\bigoplus_{x\in X^-}\mathbb{Z}[\zeta_k],\zeta_k)$. Each of these affine quandles embeds into any of its orbits, i.e. into a module over $\mathbb{Z}[\zeta_k]$. $\square$

Note that applying our idea of I-quandles one obtains the description of free n-symmetric m-reductive medial quandles if we consider $I=\{\sum_{r=0}^{n-1}t^r,(1-t)^{m-1}\}$. In particular, the free 2-reductive n-symmetric medial quandle over X is isomorphic to $\bigoplus_{x\in X^-}\mathbb{Z}_n\times X$ with the operation $(a,i)*(b,j)=(b+e_i-e_j,j)$ [11, Proposition 2.4].

References

[1] J.S. Carter, *A survey of quandle ideas*, Introductory lectures on knot theory, Ser. Knots Everything 46, World Sci. Publ., Hackensack, NJ (2012), 22–53.

[2] J. Denes, A.D. Keedwell, *On P-quasigroups and decompositions of complete undirected graphs*, J. Combin. Theory Ser. B, 13 (1972), 270–275.

[3] X. Hou, *Automorphism groups of Alexander quandles*, J. Algebra 344 (2011), 373–385.

[4] X. Hou, *Finite modules over* $\mathbb{Z}[t,t^{-1}]$, J. Knot Theory Ramifications 21 (2012), no. 8, 1250079, 28 pp.

[5] A. Hulpke, D. Stanovský, P. Vojtěchovský, *Connected quandles and transitive groups*, J. Pure Appl. Algebra 220 (2016), 735–758.

[6] P. Jedlička, A. Pilitowska, D. Stanovský, A. Zamojska-Dzienio, *The structure of medial quandles*, J. Algebra 443 (2015), 300–334.

[7] P. Jedlička, A. Pilitowska, A. Zamojska-Dzienio, *Subdirectly irreducible medial quandles*, submitted. Available at `http://arxiv.org/abs/1511.06529`.

[8] D. Joyce, *Classifying invariant of knots, the knot quandle*, J. Pure Applied Algebra 23 (1982), 37–65.

[9] K. Kearnes, *A quasi-affine representation*, Internat. J. Algebra Comput. 5 (1995), 673–702.

[10] O. Loos, *Symmetric spaces*, J. Benjamin New York, 1969.

[11] A. Romanowska, B. Roszkowska, *Representations of n-cyclic groupoids,* Algebra Universalis 26 (1989), 7–15.

[12] A. Romanowska, J.D.H. Smith, *Modes,* World Scientific, Singapore, 2002.

[13] D. Stanovský, *Left symmetric left distributive operations on a group*, Algebra Universalis 54(1) (2005), 97–103.

[14] M. Stronkowski, *Free modes*, Comment. Math. Univ. Carolinae 47, no. 4 (2006), 561–568.

[15] O. Zariski, P. Samuel, *Commutative algebra*, vol. I, Springer-Verlag, Berlin, 1975.

(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

E-mail address: (P.J.) jedlickap@tf.czu.cz

E-mail address: (A.P.) apili@mini.pw.edu.pl

E-mail address: (A.Z.) A.Zamojska-Dzienio@mini.pw.edu.pl