The Word Problem for Finitely Presented Quandles is Undecidable

James Belk[1] and Robert W. McGrail[1]

The Laboratory for Algebraic and Symbolic Computation,
Reem-Kayden Center for Science and Computation,
Bard College,
Annandale-on-Hudson, NY 12504
belk@bard.edu, mcgrail@bard.edu

Abstract. This work presents an algorithmic reduction of the word problem for recursively presented groups to the word problem for recursively presented quandles. The faithfulness of the reduction follows from the conjugation quandle construction on groups. It follows that the word problem for recursively presented quandles is not effectively computable, in general. This article also demonstrates that a recursively presented quandle can be encoded as a recursively presented rack. Hence the word problem for recursively presented racks is also not effectively computable.

1 Introduction

The theory of quandles [8] has been the almost exclusive domain of knot theorists. Logical and computational questions about quandles have generally focused on the application of quandles as a strong invariant of three-dimensional knots. Researchers have given far less attention to logical and computational aspects of the theory of quandles from the perspective of universal algebra [1].

A logician might ask whether the first-order theory of quandles is decidable [5]. That is, does there exist an algorithm to decide whether a well-formed, first-order sentence is a theorem of the theory of quandles? This appears to be an open question; no one seems to have made an attempt to answer it as of the time of the writing of this article. This is not surprising since a definitive answer would hardly be useful to those principally concerned with knot theory and other domains within topology.

Logical questions more mildly relevant to knot theory might focus on the algebra of quandles. For example, is the pure equational theory of quandles decidable? In other words, does there exist an effective procedure for deciding whether an identity over the quandle signature is valid for all quandles? It just so happens that such a procedure follows directly from [8]. In that seminal work Joyce proved that, for a set of generators A, the free quandle on a A can be embedded into a quandle structure over the group operations of the free group [14] on A. Hence, any quandle identity can be translated into a logically equivalent

group identity. Since the pure equational theory of groups is decidable [9], the same holds for quandles.

Along these lines, is the general word problem [4] for recursively presented quandles also decidable? This article demonstrates that this is not the case. In particular, the authors show that there exists a **finitely presented** quandle with undecidable word problem.

This sections below describe a construction that, given a recursively (finitely) presented group $\mathbf{G}$ [3], produces a recursively (finitely) presented quandle $\mathbf{Q_G}$ [8, 1]. Using two standard constructions, namely the *group quandle* as well as the group of *inner automorphisms* of a quandle, it is shown that $\mathbf{G}$ is isomorphic to a subgroup of $\mathbf{Inn}(\mathbf{Q_G})$, the group of inner automorphisms of $\mathbf{Q_G}$. This provides a new "representation theory" for groups. Moreover, it follows that for any group expression w over the generators of $\mathbf{G}$, $\mathbf{G} \models w = e$ if and only if $\mathbf{Q_G} \models x^w = x$, where x is a generator for $\mathbf{Q_G}$ indeterminate over $\mathbf{G}$ and x^w stands for a fixed quandle expression over the generators of $\mathbf{Q_G}$ constructed by induction over the structure of the expression w.

Hence, any procedure that decides the word problem over $\mathbf{Q_G}$ must also decide the word problem over $\mathbf{G}$. In particular, any finitely presented group $\mathbf{G}$ with undecidable word problem gives rise to a finitely presented quandle $\mathbf{Q_G}$ with undecidable word problem. Since such a group exists [13], a finitely presented quandle with undecidable word problem must also exist.

2 The Theory of Quandles

A quandle $\mathbf{Q} = (Q, *, /)$ is an algebra over the signature $\{*, /\}$, both binary function symbols, satisfying the following identities:

Idempotence: $\forall x(x * x = x)$;
Right Cancellation: $\forall x \forall y((x * y)/y = x)$ and $\forall x \forall y((x/y) * y = x)$; and
Right Self-Distributivity: $\forall x \forall y \forall z((x * y) * z = (x * z) * (y * z))$.

The theory of quandles was introduced by Joyce [8] and the material from this section is taken from that source.

The formulation of the theory of quandles above – a list of identities and hence axioms free of existential quantifiers and logical connectives – and the logical notation that follows is from the points of view of universal algebra [1] and model theory [2], respectively.

2.1 The Inner Automorphism Group of a Quandle

For an element q of a quandle $\mathbf{Q} = (Q, *, /)$, consider the induced mappings $r_q, R_q : Q \to Q$ via right translation. That is,

$$r_q(p) = p * q$$

and

$$R_q(p) = p/q$$

for $p \in Q$. By the right self-distributivity axiom, $r_q(p_1 * p_2) = (p_1 * p_2) * q = (p_1 * q) * (p_2 * q) = r_q(p_1) * r_q(p_2)$, so each r_q is a quandle homomorphism. Moreover, these maps are permutations on the set Q. Indeed, the right cancellation axioms ensure that $R_q = r_q^{-1}$. Hence each r_q is a quandle automorphism of $\mathbf{Q}$. Let $\mathbf{Inn}(\mathbf{Q})$ stand for the subgroup of $\mathbf{Sym_Q}$, the symmetric group on the elements of $\mathbf{Q}$, generated by $\{r_q | q \in Q\}$. This is called the group of **inner automorphisms** of $\mathbf{Q}$.

2.2 The Group Quandle

Given a group $\mathbf{G} = (G, e, (-)^{-1}, \cdot)$ [14], one may define a quandle structure as follows. For $a, b \in G$ define $* : G \times G \to G$ by

$$a * b = b^{-1}ab$$

and $/ : G \times G \to G$ by

$$a/b = bab^{-1}$$

Then $\mathbf{Conj}(\mathbf{G}) = (G, *, /)$ is quandle. Indeed, suppose $a, b, c \in G$. Idempotence is a consequence of

$$\begin{aligned} a * a &= a^{-1}aa \\ &= (a^{-1}a)a \\ &= a. \end{aligned}$$

Also

$$\begin{aligned} (a * b)/b &= b(b^{-1}ab)b^{-1} \\ &= (bb^{-1})a(bb^{-1}) \\ &= a. \end{aligned}$$

By a similar argument $(a/b) * b = a$. Finally,

$$\begin{aligned} (a * b) * c &= (b^{-1}ab) * c \\ &= c^{-1}(b^{-1}ab)c \\ &= (c^{-1}b^{-1})a(bc) \\ &= (c^{-1}b^{-1})(cc^{-1})a(cc^{-1})(bc) \\ &= (c^{-1}b^{-1}c)(c^{-1}ac)(c^{-1}bc) \\ &= (c^{-1}bc)^{-1}(c^{-1}ac)(c^{-1}bc) \\ &= (b * c)^{-1}(a * c)(b * c) \\ &= (a * c) * (b * c). \end{aligned}$$

A quandle formed in this way from a group and its operations is called a **group quandle**.

3 The Quandle $\mathbf{Q_G}$

Let $\mathbf{G} = \langle A|W\rangle$ be a recursively presented group. Here A is a recursive set of generators and W is a recursive set of words over the group signature and the generators A. Then by the definition of freeness, there exists a unique surjective group homomorphism $\pi_{\mathbf{G}} : \mathbf{FG}(A) \to \mathbf{G}$ from the free group $\mathbf{FG}(A)$ that fixes the generators A.

For the duration of this article, x is a fresh generator. That is, $x \notin A$. Let w be a word over the group signature $\{e, (-)^{-1}, \cdot\}$ and the generators A and let q be a word over the quandle signature $\{*, /\}$ and the generators $A \cup \{x\}$. Define the syntactic form q^w over the quandle signature and the generators $A \cup \{x\}$ by induction on the structure of the word w [6]:

$$q^w = \begin{cases} q & \text{if } w = \epsilon; \\ q & \text{if } w = e; \\ q * a & \text{if } w = a \in A; \\ (q^{w_1})^{w_2} & \text{if } w = w_1 w_2; \\ q & \text{if } w = e^{-1}; \\ q/a & \text{if } w = a^{-1} \text{ and } a \in A; \\ (q^{{w_2}^{-1}})^{{w_1}^{-1}} & \text{if } w = (w_1 w_2)^{-1}; \text{ and} \\ q^{w_1} & \text{if } w = (w_1^{-1})^{-1}. \end{cases} \tag{1}$$

For example, given $a_1, a_2, a_3 \in A$,

$$\begin{aligned} x^{(a_1 a_3^{-1})a_2} &= (x^{(a_1 a_3^{-1})})^{a_2} \\ &= ((x^{a_1})^{a_3^{-1}})^{a_2} \\ &= ((x * a_1)^{a_3^{-1}})^{a_2} \\ &= ((x * a_1)/a_3)^{a_2} \\ &= ((x * a_1)/a_3) * a_2. \end{aligned}$$

Given the group presentation $\mathbf{G} = \langle A|W\rangle$, form the recursively presented quandle

$$\mathbf{Q_G} = \langle A \cup \{x\} |\ a^g = a; a \in A \cup \{x\}, g \in W\rangle.$$

For instance, consider the group presentation for the group of symmetries of a triangle,

$$\mathbf{S_3} = \langle a, b | a^2, b^3, abab\rangle.$$

Then $\mathbf{Q_{S_3}} = \langle a, b, x | E_{S_3}\rangle$ where E_{S_3} is the following set of equations:

$$\begin{array}{rrr} (a*a)*a = a, & (b*a)*a = b, & (x*a)*a = x, \\ ((a*b)*b)*b = a, & ((b*b)*b)*b = b, & ((x*b)*b)*b = x, \\ (((a*a)*b)*a)*b = a, & (((b*a)*b)*a)*b = b, & (((x*a)*b)*a)*b = x. \end{array}$$

3.1 Representing G in $\mathbf{Inn}(\mathbf{Q_G})$

Consider the group $\mathbf{Inn}(\mathbf{Q_G})$ arising from the construction of Section 2.1. Let

$$\rho : \mathbf{FG}(A) \to \mathbf{Inn}(\mathbf{Q_G})$$

be the unique group homomorphism that satisfies $\rho_a = r_a$ for $a \in A$. Since ρ is a group homomorphism into $\mathbf{Sym_{Q_G}}$, it induces an action [16] of the group $\mathbf{FG}(A)$ on the underlying set of $\mathbf{Q_G}$. The following lemma demonstrates that this action directly corresponds to the definition of q^w from the previous section.

Lemma 1. *For each $w \in \mathbf{FG}(A)$ and $q \in \mathbf{Q_G}$, $\rho_w(q) = q^w$ in $\mathbf{Q_G}$.*

Proof. This follows by induction on the structure of the word w. In the first type of base case, w is ϵ, e, or e^{-1} and

$$\rho_w(q) = q = q^w.$$

The remaining base cases are $w = a$ and $w = a^{-1}$. In the former case,

$$\begin{aligned}\rho_w(q) &= \rho_a(q)\\ &= r_a(q)\\ &= q * a\\ &= q^a\\ &= q^w,\end{aligned}$$

and in the latter case,

$$\begin{aligned}\rho_w(q) &= \rho_{a^{-1}}(q)\\ &= \rho_a^{-1}(q)\\ &= r_a^{-1}(q)\\ &= R_a(q)\\ &= q/a\\ &= q^{a^{-1}}\\ &= q^w.\end{aligned}$$

Now assume for $w_1, w_2 \in \mathbf{FG}(A)$ that for any $p \in \mathbf{Q_G}$, $\rho_{w_1}(p) = p^{w_1}$ and $\rho_{w_2}(p) = p^{w_2}$. If $w = w_1 w_2$ then

$$\begin{aligned}\rho_w(q) &= \rho_{w_1 w_2}(q)\\ &= (\rho_{w_2} \circ \rho_{w_1})(q)\\ &= \rho_{w_2}(\rho_{w_1}(q))\\ &= \rho_{w_2}(q^{w_1})\\ &= (q^{w_1})^{w_2}\\ &= q^{w_1 w_2}\\ &= q^w.\end{aligned}$$

For $w = (w_1 w_2)^{-1}$,

$$\begin{aligned}
\rho_w(q) &= \rho_{(w_1 w_2)^{-1}}(q) \\
&= \rho_{w_2^{-1} w_1^{-1}}(q) \\
&= (\rho_{w_1^{-1}} \circ \rho_{w_2^{-1}})(q) \\
&= \rho_{w_1^{-1}}(\rho_{w_2^{-1}}(q)) \\
&= \rho_{w_1^{-1}}(q^{w_2^{-1}}) \\
&= (q^{w_2^{-1}})^{w_1^{-1}} \\
&= q^{(w_1 w_2)^{-1}} \\
&= q^w.
\end{aligned}$$

The final case is $w = (w_1^{-1})^{-1}$. Here

$$\begin{aligned}
\rho_w(q) &= \rho_{(w_1^{-1})^{-1}}(q) \\
&= \rho_{w_1}(q) \\
&= q^{w_1} \\
&= q^{(w_1^{-1})^{-1}} \\
&= q^w.
\end{aligned}$$

Since this constitutes an exhaustive set of cases on the structure of the word w, $\rho_w(q) = q^w$ follows by structural induction.

Lemma 2. *For each $g \in W$, ρ_g is the identity mapping on $\mathbf{Q_G}$.*

Proof. By Lemma 1, for each $q \in \mathbf{Q_G}$ and $w \in \mathbf{FG}(A)$, $\rho_w(q) = q^w$. In particular, for $g \in W$, $\rho_g(a) = a^g = a$ for all $a \in A \cup \{x\}$. Hence ρ_g is a quandle automorphism of $\mathbf{Q_G}$ that fixes the generators $A \cup \{x\}$. This implies that ρ_g is the identity map on $\mathbf{Q_G}$.

Lemma 3. $\mathbf{ker}\ \pi_{\mathbf{G}} \leq \mathbf{ker}\ \rho$.

Proof. By Lemma 2, $\mathbf{ker}\ \rho$ is a normal subgroup of $\mathbf{FG}(A)$ that contains the set W. However, $\mathbf{ker}\ \pi_{\mathbf{G}}$ is the minimal normal subgroup of $\mathbf{FG}(A)$ containing W, so $\mathbf{ker}\ \pi_{\mathbf{G}} \leq \mathbf{ker}\ \rho$.

As a consequence of Lemma 3, ρ corresponds to a well-defined group homomorphism from $\mathbf{G}$ to $\mathbf{Inn}(\mathbf{Q_G})$.

Theorem 1 (Quandle Representation Theory for Groups, Part I). *Given any recursively presented group $\mathbf{G} = \langle A|W\rangle$, there exists a unique group homomorphism $\rho : \mathbf{G} \to \mathbf{Inn}(\mathbf{Q_G})$ satisfying $\rho_g(q) = q^g$ for all $g \in \mathbf{G}$ and $q \in \mathbf{Q_G}$.*

In particular, this gives rise to an encoding of identities over $\mathbf{G}$ as identities over $\mathbf{Q_G}$, which will be instrumental in reducing the decidability of the word problem for groups to the word problem for quandles in Theorem 3.

Corollary 1. *For $w \in \mathbf{FG}(A)$, if $\mathbf{G} \models w = e$, then $\mathbf{Q_G} \models x^w = x$.*

4 The Embedding ρ

The main goal of this section is to show that the reverse implication to Corollary 1 also holds, so that the homomorphism ρ is an embedding of $\mathbf{G}$ into $\mathbf{Q_G}$. Toward that end, this section constructs two groups which, through use of the group quandle construction, will make this implication more clear.

4.1 The Group $\mathbf{G}_x$

Consider the recursively presented group below.

$$\mathbf{G}_x = \langle A \cup \{x\} |\ ag = ga; a \in A \cup \{x\}, g \in W \rangle$$

Let q be a word over the quandle signature and the letters $A \cup \{x\}$. Define $\phi(q)$ over the group signature and the letters $A \cup \{x\}$ by structural induction over the quandle signature as follows:

$$\phi(q) = \begin{cases} a, & \text{if } q = a \in A \cup \{x\}; \\ \phi(q_2)^{-1}\phi(q_1)\phi(q_2), & \text{if } q = q_1 * q_2; \text{ and} \\ \phi(q_2)\phi(q_1)\phi(q_2)^{-1}, & \text{if } q = q_1/q_2. \end{cases} \tag{2}$$

Note that the definition of $\mathbf{Conj}(\mathbf{G_x})$ requires that $\mathbf{Conj}(\mathbf{G_x}) \models q = q'$ if and only if $\mathbf{G}_x \models \phi(q) = \phi(q')$.

Lemma 4. *For q a word over the quandle signature and the letters $A \cup \{x\}$ and w a word of positive length over the group signature and the letters A, $\mathbf{G}_x \models \phi(q^w) = w^{-1}\phi(q)w$.*

Proof. The proof proceeds by induction on the structure of the word $w \neq \epsilon$ over the generators A and the group signature. If w is e or e^{-1},

$$\phi(q^w) = \phi(q) = w^{-1}\phi(q)w.$$

For $w = a \in A$,

$$\begin{aligned} \phi(q^w) &= \phi(q^a) \\ &= \phi(q * a) \\ &= \phi(a)^{-1}\phi(q)\phi(a) \\ &= a^{-1}\phi(q)a \\ &= w^{-1}\phi(q)w, \end{aligned}$$

and for $w = a^{-1}$,

$$\begin{aligned} \phi(q^w) &= \phi(q^{a^{-1}}) \\ &= \phi(q/a) \\ &= \phi(a)\phi(q)\phi(a)^{-1} \\ &= a\phi(q)a^{-1} \\ &= w^{-1}\phi(q)w, \end{aligned}$$

which rounds out the base cases.

In the first inductive case, $w = w_1 w_2$. Here

$$\begin{aligned}\phi(q^w) &= \phi(q^{w_1 w_2}) \\ &= \phi((q^{w_1})^{w_2}) \\ &= w_2^{-1}\phi(q^{w_1})w_2 \\ &= w_2^{-1}(w_1^{-1}\phi(q)w_1)w_2 \\ &= (w_1 w_2)^{-1}\phi(q)(w_1 w_2) \\ &= w^{-1}\phi(q)w.\end{aligned}$$

Given $w = (w_1 w_2)^{-1}$,

$$\begin{aligned}\phi(q^w) &= \phi(q^{(w_1 w_2)^{-1}}) \\ &= \phi((q^{w_2^{-1}})^{w_1^{-1}}) \\ &= (w_1^{-1})^{-1}\phi(q^{w_2^{-1}})w_1^{-1} \\ &= (w_1^{-1})^{-1}((w_2^{-1})^{-1}\phi(q)w_2^{-1})w_1^{-1} \\ &= (w_2^{-1}w_1^{-1})^{-1}\phi(q)w_2^{-1}w_1^{-1} \\ &= ((w_1 w_2)^{-1})^{-1}\phi(q)(w_1 w_2)^{-1} \\ &= w^{-1}\phi(q)w.\end{aligned}$$

In the final inductive case, $w = (w_1^{-1})^{-1}$,

$$\begin{aligned}\phi(q^w) &= \phi(q^{(w_1^{-1})^{-1}}) \\ &= \phi(q^{w_1}) \\ &= w_1^{-1}\phi(q)w_1 \\ &= ((w_1^{-1})^{-1})^{-1}\phi(q)(w_1^{-1})^{-1} \\ &= w^{-1}\phi(q)w.\end{aligned}$$

Since the collection of cases for $w \neq \epsilon$ is exhaustive, the lemma follows by induction on the structure of w.

Corollary 2. *For $a \in A \cup \{x\}$ and w a word over the group signature and the letters A, $\mathbf{Conj}(\mathbf{G_x}) \models a^w = a$ if and only if $\mathbf{G}_x \models aw = wa$.*

Lemma 5. *For $w \in \mathbf{FG}(A)$, if $\mathbf{Q_G} \models x^w = x$, then $\mathbf{G}_x \models xw = wx$.*

Proof. Note that for each $g \in W$ and $a \in A \cup \{x\}$, $\mathbf{G}_x \models ag = ga$. By Corollary 2, $\mathbf{Conj}(\mathbf{G_x}) \models a^g = a$. Of course, this means that there exists a unique quandle homomorphism $\psi : \mathbf{Q_G} \to \mathbf{Conj}(\mathbf{G_x})$ that fixes the generators $A \cup \{x\}$. Then given $w \in \mathbf{FG}(A)$ such that $\mathbf{Q_G} \models x^w = x$, it must follow that $\mathbf{Conj}(\mathbf{G_x}) \models x^w = x$. However, the latter assertion is equivalent to $\mathbf{G}_x \models xw = wx$ also by Corollary 2.

4.2 The Free Product $\mathbf{G} * \langle x \rangle$

Next, consider the free product of $\mathbf{G}$ and the infinite cycle group $\langle x \rangle$

$$\mathbf{G} * \langle x \rangle = \langle A \cup \{x\} |\ W \rangle.$$

Lemma 6. *For $w \in \mathbf{FG}(A)$, if $\mathbf{Q_G} \models x^w = x$, then $\mathbf{G} * \langle x \rangle \models xw = wx$.*

Proof. Since for each $g \in W$, $\mathbf{G} * \langle x \rangle \models g = e$, it certainly follows that $\mathbf{G} * \langle x \rangle \models ag = ga$ for $a \in A \cup \{x\}$. Therefore, there exists a unique group homomorphism $\theta : \mathbf{G}_x \to \mathbf{G} * \langle x \rangle$ that fixes the elements of $A \cup \{x\}$. Given that $\mathbf{Q_G} \models x^w = x$, then $\mathbf{G}_x \models xw = wx$ by Lemma 5. The assertion $\mathbf{G} * \langle x \rangle \models xw = wx$ follows by application of θ.

The structure $\mathbf{G} * \langle x \rangle$ arises from the coproduct of $\mathbf{G}$ and $\langle x \rangle$ in the category of groups [10]. Let $\iota : \mathbf{G} \to \mathbf{G} * \langle x \rangle$ be the canonical injection of $\mathbf{G}$ into $\mathbf{G} * \langle x \rangle$, $\iota_{\mathbf{FG}(A)} : \mathbf{FG}(A) \to \mathbf{FG}(A \cup \{x\})$ be the group homomorphism induced by the inclusion of A in $A \cup \{x\}$, and $\pi_{\mathbf{G}_x} : \mathbf{FG}(A \cup \{x\}) \to \mathbf{G}_x$ be the natural projection. Since the composite maps $\iota_{\mathbf{G}} \circ \pi$ and $\theta \circ \pi_{\mathbf{G}_x} \circ \iota_{\mathbf{FG}(A)}$ agree on the generators A

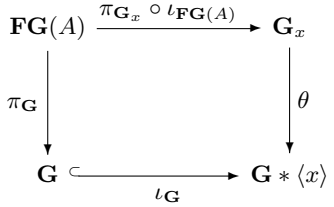

Fig. 1. Commuting Square

of $\mathbf{FG}(A)$, the square of Figure 1 commutes.

The free product construction guarantees that, for any $w \in \mathbf{G}$, if $wx = xw$ in $\mathbf{G} * \langle x \rangle$, then $w = e$ in $\mathbf{G} * \langle x \rangle$ and so also in $\mathbf{G}$. This proves the following.

Corollary 3. *For $w \in \mathbf{FG}(A)$, if $\mathbf{Q_G} \models x^w = x$, then $\mathbf{G} \models w = e$.*

Lemma 7. $\mathbf{ker}\ \rho \leq \mathbf{ker}\ \pi_{\mathbf{G}}$.

Proof. Suppose $w \in \mathbf{ker}\ \rho$. Then $\rho_w = id_{\mathbf{Q_G}}$ so certainly $x^w = \rho_w(x) = id(x) = x$ in $\mathbf{Q_G}$. By Corollary 3, $w = e$ in $\mathbf{G}$. In other words, $w \in \mathbf{ker}\ \pi_{\mathbf{G}}$.

Theorem 2 (Quandle Representation Theory for Groups, Part II). *For every recursively presented group $\mathbf{G} = \langle A | W \rangle$, $\mathbf{G} \leq \mathbf{Inn}(\mathbf{Q_G})$.*

Proof. By Lemmas 3 and 7, $\mathbf{ker}\ \rho = \mathbf{ker}\ \pi_{\mathbf{G}}$. This implies that the induced group homomorphism $\rho : \mathbf{G} \to \mathbf{Inn}(\mathbf{Q_G})$ of Theorem 1 is injective. In other words, $\mathbf{G}$ is isomorphic to a subgroup of $\mathbf{Inn}(\mathbf{Q_G})$.

4.3 The Word Problem for Quandles

Theorem 3. *If* $\mathbf{Q_G}$ *has decidable word problem then so does* $\mathbf{G}$*.*

Proof. This is accomplished via a reduction of the word problem for $\mathbf{G}$ to the word problem for $\mathbf{Q_G}$ [4]. For any word w over the group operations and the generators of $\mathbf{G}$, replace the equation $w = e$ with the quandle equation $x^w = x$ according to the construction of Section 3. By Corollaries 1 and 3, $\mathbf{G} \models w = e$ if and only if $\mathbf{Q_G} \models x^w = x$. Consequently, any algorithm that determines the latter for all w also determines the former for all w.

In [13], Novikov contructs a finitely presented group $\mathbf{G}$ with an undecidable word problem. It follows from Theorem 3 and elementary use of propositional contrapositive that the finitely presented quandle $\mathbf{Q_G}$ must also have an undecidable word problem.

Corollary 4. *There exists a finitely presented quandle with undecidable word problem.*

5 Racks

A rack $\mathbf{R} = (R, *, /)$ [15] is an algebra over the quandle signature $\{*, /\}$ that satisfies all of the quandle axioms with the possible exception of idempotence. In other words, racks satisfy the axioms below:

Right Cancellation: $\forall x \forall y((x * y)/y = x)$ and $\forall x \forall y((x/y) * y = x)$; and
Right Self-Distributivity: $\forall x \forall y \forall z((x * y) * z = (x * z) * (y * z))$.

It turns out that every finitely presented quandle is also a finitely presented rack: Given a finite quandle presentation $\mathbf{Q} = \langle A|E\rangle$, the finite rack presentation

$$\mathbf{R_Q} = \langle A|E \cup \{a * a = a, a/a = a|a \in A\}\rangle$$

represents the same algebra. As a consequence, if the finitely presented quandle $\mathbf{Q}$ has undecidable word problem then so does the finitely presented rack $\mathbf{R_Q}$. Theorem 4 below follows directly from this relationship and Corollary 4.

Theorem 4. *The general word problem for finitely presented racks is undecidable.*

6 Conclusion and Future Work

A natural trajectory for this work is to explore other self-distributive theories through further encodings. In particular, there is much that is not known about the hardness of left-distributive algebras [12]. These algebras arise from elementary embeddings associated with a large cardinal assumption [11] in set theory [7].

References

1. Burris, S., Sankappanavar, H.P.: A Course in Universal Algebra. Springer Verlag, Berlin (1981)
2. Chang, C.C., Keisler, H.J.: Model Theory, Studies in Logic and the Foundations of Mathematics, vol. 73. North-Holland, Amsterdam, 3rd edn. (1992)
3. Coxeter, H.M.S., Moser, W.O.J.: Generators and Relations for Discrete Groups, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 14. Springer-Verlag, New York, 4th edn. (1980)
4. Evans, T.: The word problem for abstract algebras. Journal of the London Mathematical Society s1-26(1), 64–71 (1951)
5. Gödel, K.: Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I. Monatshefte für Mathematik und Physik 38, 173–198 (1931)
6. Hopcroft, J.E., Motwani, R., Ullman, J.D.: Introduction to Automata Theory, Languages, and Computation. Addison-Wesley, Reading, Massachusetts, 2nd edn. (2001)
7. Jech, T.: Set Theory. Springer Monographs in Mathematics, Springer, 3rd edn. (2003)
8. Joyce, D.: A classifying invariant of knots, the knot quandle. Journal of Pure and Applied Algebra 23, 37–66 (1982)
9. Knuth, D.E., Bendix, P.B.: Simple word problems in universal algebras. In: Leach, J. (ed.) Computational Algebra, pp. 263–297. Pergamon Press (1970)
10. Lane, S.M.: Categories for the Working Mathematician, Graduate Texts in Mathematics, vol. 5. Springer-Verlag, New York, 2nd edn. (1998)
11. Laver, R.: The algebra of elementary embeddings of a rank into itself. Advances in Mathematics 110(2), 334–346 (February 1995)
12. Laver, R.: The left-distributive law and the freeness of an algebra of elementary embeddings. Advances in Mathematics 91(2), 209–231 (February 1995)
13. Nobikov, P.S.: On the algorithmic unsolvability of the word problem in group theory. Proceedings of the Steklov Institute of Mathematics 44, 1–143 (1955)
14. Rotman, J.: An Introduction to the Theory of Groups, Graduate Texts in Mathematics, vol. 148. Springer-Verlag, New York, 4th edn. (1999)
15. Rourke, C., Fenn, R.: Racks and links in codimension 2. Journal of Knot Theory and Its Ramifications 1(4), 343–406 (1992)
16. Smith, J.H.D.: Introduction to Abstract Algebra. Textbooks in Mathematics, Taylor and Francis Ltd (August 2008)

A Identities

The right cancellation rules have a very nice symmetry with respect to the operators $*$ and $/$. That is, exchanging the roles of $*$ and $/$ in one rule yields the other. This also holds for idempotence in the theory of quandles and the right self-distributivity rule in quandles and racks. A complete set of such rules are presented below.

A.1 Idempotence

Assuming the quandle identities, one may reason as follows:

$$x/x = (x * x)/x = x.$$

Hence, the $/$ operator is also idempotent according to the theory of quandles.

A.2 Right Distributivity

This section presents the remaining right distributive quandle and rack identities.

1. $(x * y)/z = (x/z) * (y/z)$: First note that by the second right cancellation rule and right self-distributivity,

$$\begin{aligned}(x * y) &= ((x/z) * z) * ((y/z) * z) \\ &= ((x/z) * (y/z)) * z.\end{aligned}$$

   Therefore by the first right cancellation rule,

$$\begin{aligned}(x * y)/z &= (((x/z) * (y/z)) * z)/z \\ &= (x/z) * (y/z).\end{aligned}$$

2. $(x/y) * z = (x * z)/(y * z)$: By right distributivity and the second right cancellation rule,

$$\begin{aligned}((x/y) * z) * (y * z) &= ((x/y) * y) * z \\ &= x * z.\end{aligned}$$

   This means that

$$\begin{aligned}(x/y) * z &= (((x/y) * z) * (y * z))/(y * z) \\ &= (x * z)/(y * z).\end{aligned}$$

3. $(x/y)/z = (x/z)/(y/z)$: By employing second right cancellation rule and the first right distributivity law of this section, one reasons

$$\begin{aligned}x/y &= ((x/z) * z)/((y/z) * z) \\ &= ((x/z)/(y/z)) * z.\end{aligned}$$

   Then the first cancellation rule ensures

$$\begin{aligned}(x/y)/z &= (((x/z)/(y/z)) * z)/z \\ &= (x/z)/(y/z).\end{aligned}$$

B $\mathbf{R_Q}$ is the Same Algebra as Q

Let $\mathbf{Q} = \langle A|E\rangle$ be a finite quandle presentation and

$$\mathbf{R_Q} = \langle A|E \cup \{a * a = a, a/a = a | a \in A\}\rangle$$

be a finite rack presentation.

The additional conditions on $\mathbf{R_Q}$ are both sufficient and necessary to the condition that $q * q = q$ and $q/q = q$ for all $q \in \mathbf{R_Q}$. The proof of such follows by structural induction on the quandle/rack expression q. The base cases in which

$q = a \in A$ are direct consequences of the new part of the rack presentation. Next suppose that $q = q_1 * q_2$ with induction hypotheses $q_1 * q_1 = q_1$, $q_1/q_1 = q_1$, $q_2 * q_2 = q_2$, and $q_2/q_2 = q_2$. Then

$$\begin{aligned} q * q &= (q_1 * q_2) * (q_1 * q_2) \\ &= (((q_1 * q_2)/q_2) * q_2) * (q_1 * q_2) \\ &= (((q_1 * q_2)/q_2) * q_1) * q_2 \\ &= (q_1 * q_1) * q_2 \\ &= q_1 * q_2 \\ &= q, \end{aligned}$$

which employs the second right cancellation rule, right self-distributivity, the first right cancellation rule, and the induction hypothesis on q_1, in that order. The case $q = q_1/q_2$ proceeds in a similar fashion. It follows that $\mathbf{R_Q}$ is idempotent and so a quandle.

Since $\mathbf{R_Q}$ is a quandle and satisfies the equations in E, there exists a unique quandle homomorphism $\alpha : \mathbf{Q} \to \mathbf{R_Q}$ that fixes the generators in A. Certainly $\mathbf{Q}$ is a rack and satisfies the equations in $E \cup \{a * a = a, a/a = a | a \in A\}$, so there exists a unique rack homomorphism $\beta : \mathbf{R_Q} \to \mathbf{Q}$ fixing the elements of A. Of course, a quandle homomorphism is also a rack homomorphism and a rack homomorphism between quandles is a quandle homomorphism. Hence, $\alpha \circ \beta : \mathbf{R_Q} \to \mathbf{R_Q}$ is a rack homomorphism that fixes the elements of A and $\beta \circ \alpha : \mathbf{Q} \to \mathbf{Q}$ is a quandle homomorphism that also fixes the generators of A. The universal mapping property on presentations implies that $\alpha \circ \beta = id_{\mathbf{R_Q}}$ and $\beta \circ \alpha = id_{\mathbf{Q}}$, so $\mathbf{R_Q}$ is, for all intents and purposes, the same algebra as $\mathbf{Q}$.