CSPs and Connectedness: P/NP-Complete Dichotomy for Idempotent, Right Quasigroups

Robert W. McGrail, James Belk,
Solomon Garber, and Japheth Wood
Reem Kayden Center for Science
and Computation
Bard College
31 Campus Road
Annandle-on-Hudson, New York 12528

Benjamin Fish
Department of Mathematics,
Statistics, and Computer Science
University of Illinois at Chicago
322 Science and Engineering Offices
851 S. Morgan Street
Chicago, IL 60607-7045

***Abstract*—In the 1990's, Jeavons showed that every finite algebra corresponds to a class of constraint satisfaction problems. Vardi later conjectured that idempotent algebras exhibit P/NP dichotomy: Every non NP-complete algebra in this class must be tractable. Here we discuss how tractability corresponds to connectivity in Cayley graphs. In particular, we show that dichotomy in finite idempotent, right quasigroups follows from a very strong notion of connectivity. Moreover, P/NP membership is first-order axiomatizable in involutory quandles.**

I. Introduction

Constraint satisfaction problems have a wide range of applications, from artificial intelligence to combinatorics and complexity theory. The general constraint satisfaction problem (CSP) is NP-complete, but there are many restrictions that make certain CSPs tractable. Jeavons, Cohen, and Gyssens [8] noticed that all tractable CSPs involve closure under algebraic operations. It was later noticed that all CSPs can be viewed this way [7].

Furthermore, Feder and Vardi [5] conjectured that CSPs exhibit P/NP-complete dichotomy. Bulatov, Jeavons, and Krokhin proved that Feder and Vardi's conjecture is equivalent to showing that algebras that fail to admit NP-complete CSPs must only admit polynomial time CSPs [1].

A. Aim and Scope

There have been many advances toward a P/NP-complete dichotomy theorem for all algebras. Much of this progress has involved the discovery of conditions under which algebras are tractable, that is, admit only polynomial time CSPs. Such conditions include term-based tests. For example, the existence of a **unanimity operation** [7], a **generalized majority-minority operation** [10], a **semilattice operation** [8], or a **Malcev term** [2] for a given algebra guarantees tractability.

In this paper we introduce another term-based test for tractability for idempotent, right quasigroups. We show this is a special case of the Malcev term test. However, this approach is easier computationally since it involves a binary **Merling** term rather than a ternary Malcev term. Moreover, this test governs a P/NP-complete dichotomy result: If an idempotent, right quasigroup has a Merling term it is tractable. Otherwise, it is NP-complete.

A Merling term has a strong geometric dimension: its existence is tantamount to a strong notion of connectedness within the right Cayley graph. Furthermore, for the subclass of **involutory quandles**, one can replace the existence of a Merling term with the satisfiabilty of a certain fixed, first-order statement. In other words, tractability and, by association, the existence of a Malcev term for involutory quandles is **first-order axiomatizable**.

B. Brief Summary

We first establish the notion of a constraint satisfaction problem over an algebra in Section II. This allows us to speak of the tractability of algebras via their constraint satisfaction problems. In Section III we define Merling terms and prove that in idempotent right quasigroups, the existence of a Merling term is equivalent to the existence

of a Malcev term. Furthermore, in Section IV we show that idempotent, right quasigroups exhibit P/NP-complete dichotomy through an exploration of a geometrical interpretation of Merling terms. In Section V, we then narrow down idempotent, right quasigroups to a strict subclass of algebras, involutory quandles. We show that not only do involutory quandles exhibit this dichotomy, but this instance of P/NP-complete dichotomy is first-order axiomatizable.

II. Constraint Satisfaction Problems over Algebras

Our treatment of the constraint satisfaction problem closely follows [1]. A constraint over an algebra A is a pair $\langle (v_1, v_2, \ldots, v_n), A' \rangle$ where $v_1, v_2, \ldots, v_n$ are variables and A' is a subalgebra of A^n. Note that elements of A' are tuples of size n. These tuples represent the possible values the variables can take.

The components of a constraint satisfaction problem over an algebra A are instances and solutions. An instance is a triple

$$\mathcal{I} = (\mathcal{V}, A, \mathcal{C})$$

where $\mathcal{V}$ is a finite set of variables and $\mathcal{C}$ is a finite set of constraints over A with variables from $\mathcal{V}$. A solution to an instance $\mathcal{I}$ is a function $\sigma : \mathcal{V} \to A$ such that for each constraint

$$\langle (v_1, v_2, \ldots, v_n), A' \rangle \in \mathcal{C},$$

we have

$$(\sigma(v_1), \sigma(v_2), \ldots, \sigma(v_n)) \in A'.$$

The set of CSPs over an algebra A is denoted $\mathrm{CSP}(A)$.

The projection algebra U_2 on two elements plays an important role in this article. More generally, U_n is the algebra $(A, *)$ on the underlying set $A = \{0, 1, \ldots, n-1\}$ defined by $x * y = x$.

Example 1. *We typically present an algebra with one basic operation by giving its Cayley table. Here is the Cayley table for U_2:*

TABLE I. Cayley table for U_2

$*$	0	1
0	0	0
1	1	1

All subsets of U_n are also subalgebras since the projection operation forces all subsets to be closed under $*$.

Example 2. *An instance of the* 3−SAT *problem is a proposition in conjunctive normal form whose clauses each have three literals. For example, consider the following.*

$$(\neg x \vee y \vee z) \wedge (x \vee \neg y \vee w)$$

A solution is a truth assignment to the variables in the clauses that satisfies the proposition. Any truth assignment that makes both z and w true satisfies this formula.

3−SAT *can also be formulated as a CSP over U_2. The instance is the triple $(\mathcal{V}, \{0,1\}, \mathcal{C})$ where $\mathcal{V}$ is the set of variables that appear in the proposition, 0 represents false and 1 represents true, and $\mathcal{C}$ is the set of constraints of the following form: For each clause, whose variables are x_1, x_2, and x_3, there is a constraint $\langle (x_1, x_2, x_3), \{0,1\}^3 - \{(a_1, a_2, a_3)\} \rangle$ where (a_1, a_2, a_3) is the only truth assignment to (x_1, x_2, x_3) that makes the clause false.*

For example, the constraint corresponding to the clause $\neg x \vee y \vee z$ is

$$\langle (x, y, z), \{0,1\}^3 - \{(1,0,0)\} \rangle.$$

Note that since all subsets of U_2^3 are also subalgebras of U_2^3, all of the constraints for 3−SAT *are subalgebras of U_2^3. Hence* 3−SAT *is a problem in* $\mathrm{CSP}(U_2)$.

An algebra A is NP-complete if $\mathrm{CSP}(A)$ contains an NP-complete problem. A is tractable if all problems in $\mathrm{CSP}(A)$ have polynomial-time solutions.

Example 3. 3−SAT *is a known NP-complete problem and* $\mathrm{CSP}(U_2)$ *contains* 3−SAT*, so U_2 is NP-complete.*

III. Tractability and Right Cancellation

Definition 4. *An idempotent, right quasigroup $(Q, *, /)$ is a set Q together with two binary basic operations $*, / : Q^2 \to Q$ satisfying the following axioms:*

Idempotence: $\forall x (x * x = x)$.

Right Cancellation I: $\forall xy ((x * y)/y = x)$.

Right Cancellation II: $\forall xy ((x/y) * y = x)$.

Note that U_n is an idempotent, right quasigroup when we define the $/$ operation to be the same as the $*$ operation. In particular, U_n is an NP-complete idempotent, right quasigroup for $n \geq 2$, since it admits the NP-complete CSP 3−SAT.

$$t(x_1, x_2, \ldots, x_k) \quad = \quad (\ldots((x_i \circ_1 t_1(x_1, x_2, \ldots, x_k)) \circ_2 t_2(x_1, x_2, \ldots, x_k)) \ldots) \circ_n t_n(x_1, x_2, \ldots, x_k)$$

Fig. 1. Structure of $t(x_1, x_2, \ldots, x_k)$.

$$r(x_1, x_2, \ldots, x_k) \quad = \quad (\ldots((x_i \circ_1 t_1(x_1, x_2, \ldots, x_k)) \circ_2 t_2(x_1, x_2, \ldots, x_k)) \ldots) \circ_i t_i(x_1, x_2, \ldots, x_k)$$

Fig. 2. Structure of $r(x_1, x_2, \ldots, x_k)$.

$$m(x, y) \quad = \quad (\ldots((x \circ_1 t_1(x, y)) \circ_2 t_2(x, y)) \ldots) \circ_n t_n(x, y)$$

Fig. 3. Structure of $m(x, y)$.

$$\begin{aligned} s(x, y, z) \quad &= \quad (\ldots((x \circ_1 t_1(y, z)) \circ_2 t_2(y, z)) \ldots) \circ_n t_n(y, z) \\ p(x, y, z) \quad &= \quad (\ldots((s(x, y, z) \circ_n^{-1} z) \circ_{n-1}^{-1} z) \ldots) \circ_1^{-1} z \end{aligned}$$

Fig. 4. Definition of $s(x, y, z)$ and $p(x, y, z)$.

A. Malcev and Merling Terms

In [2], the authors proved that an algebra with a Malcev term is tractable. A *Malcev term* over an algebra A is a ternary term $p(x, y, z)$ such that $p(x, y, y) = x$ and $p(x, x, y) = y$ in A [3]. In order to determine that an algebra is tractable, it is sufficient to find a Malcev term for that algebra.

In idempotent, right quasigroups, however, we do not need to find a Malcev term. Instead we only need to find a *Merling term*:

Definition 5. *A binary term $m(x, y)$ over the right quasigroup signature is a Merling term for the quandle Q if $m(x, y) = x$ in U_2 but $m(x, y) = y$ in Q.*

Note that a Merling term t for Q ensures that Q and U_2 have **independent varieties** [11]. The following technical result will prove useful in multiple contexts.

Lemma 6. *Let $t(x_1, x_2, \ldots, x_k)$ be a term over $\{*, /\}$. Then the term operation on U_m associated to t is a projection operation. That is, for some $i = 1, 2, \ldots, k$, $t(x_1, x_2, \ldots, x_k) = x_i$ in U_m. Moreover, t takes a form as in Figure 1 for some terms $t_1, t_2, \ldots, t_n$.*

Proof: We prove this claim by induction on the term structure of $t(x_1, x_2, \ldots, x_k)$. The result is immediate in most basic case in which the term $t(x_1, x_2, \ldots, x_k)$ is a variable x_i for some $1 \leq i \leq k$.

In the general case, $t(x_1, x_2, \ldots, x_k)$ takes the form $t(x_1, x_2, \ldots, x_k) = r(x_1, x_2, \ldots, x_k) \circ s(x_1, x_2, \ldots, x_k)$ where $\circ$ is either $*$ or $/$. By the induction hypothesis, one of $r(x_1, x_2, \ldots, x_k) = x_i$ holds in U_m for some $1 \leq i \leq k$. In U_m, $x * y = x$ and $x/y = x$ for all x, y. Hence $t(x_1, x_2, \ldots, x_k) = r(x_1, x_2, \ldots, x_k) \circ s(x_1, x_2, \ldots, x_k) = r(x_1, x_2, \ldots, x_k) = x_i$.

Also by the induction hypothesis, r takes the form of Figure 2. Letting $n = i + 1$, $\circ_n = \circ$, and $t_n(x_1, x_2, \ldots, x_k) \circ s(x_1, x_2, \ldots, x_k)$ places t in the desired form. ■

Theorem 7. *Let Q be an idempotent, right quasigroup. Then Q has a Merling term if and only if it has a Malcev term.*

Proof: Let $m(x, y)$ be a Merling term for Q. Then according to Lemma 6, $m(x, y) = x$ in U_2 and m takes the form shown in Figure 3 where for all $1 \leq i \leq n$, $\circ_i$ is in $\{*, /\}$ and t_i is a binary term. Construct $s(x, y, z)$ and $p(x, y, z)$ as in Figure 4 where $\circ_i^{-1}$ is $/$ when $\circ_i$ is $*$ and $\circ_i^{-1}$ is $*$ when $\circ_i$ is $/$. The idempotence of $*$ and $/$ ensure that any term operation defined over these operators is also idempotent. Hence for each of the terms operations $t_i(x, y)$, $t_i(y, y) = y$ is a theorem of the first order theory of idempotent, right quasigroups. Using this fact along with right cancellation, for $x, y \in Q$, one can reason as in Figure 5. Also from idempotence, for $x, y \in Q$ comes the derivation of Figure 6. Thus, p is a Malcev term for Q.

Now let $p(x, y, z)$ be a Malcev term for Q, i.e. $p(x, x, y) = y$ and $p(x, y, y) = x$ in Q. Switching x and y in the second identity, $p(x, x, y) = y$ and $p(y, x, x) = y$ in Q.

By Lemma 6, one of the identities $p(x, y, z) = x$, $p(x, y, z) = y$ or $p(x, y, z) = z$ holds in U_2. Suppose $p(x, y, z) = x$ or $p(x, y, z) = y$ in U_2. Then $p(x, x, y) = x$ in U_2, and $p(x, x, y) = y$ in Q, so $m(x, y) = p(x, x, y)$ is a Merling term. Otherwise, $p(x, y, z) = z$ in U_2. Then $p(y, x, x) = x$ in U_2, and $p(y, x, x) = y$ in Q, so $m(x, y) = p(y, x, x)$ is a Merling term. ■

$$\begin{aligned} p(x,y,y) &= (...((x \circ_1 t_1(y,y)) \circ_2 t_2(y,y)) \dots \circ_n t_n(y,y)) \circ_n^{-1} y) \circ_{n-1}^{-1} y) \dots \circ_1^{-1} y \\ &= (...((x \circ_1 y) \circ_2 y) \dots \circ_n y)) \circ_n^{-1} y) \circ_{n-1}^{-1} y) \dots \circ_1^{-1} y \\ &= x. \end{aligned}$$

Fig. 5. Derivation of $p(x,y,y) = x$.

$$\begin{aligned} p(x,x,y) &= (...((x \circ_1 t_1(x,y)) \circ_2 t_2(x,y)) \dots \circ_n t_n(x,y)) \circ_n^{-1} y) \circ_{n-1}^{-1} y) \dots \circ_1^{-1} y \\ &= (...(m(x,y) \circ_n^{-1} y) \circ_{n-1}^{-1} y) \dots \circ_1^{-1} y \\ &= (...(y \circ_n^{-1} y) \circ_{n-1}^{-1} y) \dots \circ_1^{-1} y \\ &= y. \end{aligned}$$

Fig. 6. Derivation of $p(x,x,y) = y$.

Corollary 8. *If an idempotent, right quasigroup has a Merling term, it is tractable.*

Proof: Let Q be an idempotent, right quasigroup with a Merling term. Then by Theorem 7, it has a Malcev term. By [2], Q is tractable. ■

Malcev terms are computationally difficult to calculate [13]. In general, the time it takes to find term functions is dependent on the arity of the operation. A well-designed search for a Merling term should be computationally easier than a comparably efficient search for a Malcev term, since the former only considers binary term functions while the latter searches the larger class of ternary term functions.

IV. Connectedness and Dichotomy

The existence of a Merling term corresponds to a strong notion of connectivity in Cayley graphs. In turn, this notion of connectivity reveals the desired dichotomy result.

A. Connectedness

Let A be an idempotent, right quasigroup. We define Cayley(A) to be the (right) Cayley graph of A [12]. That is, Cayley(A) is the graph where each element of A is assigned a vertex and there is an edge between x and y in Cayley(A) if there exists an element a in A such that $x * a = y$ or $x/a = y$. If Cayley(A) is connected, then we say A is connected.

Definition 9. *Let Q be an idempotent, right quasigroup.*

i) *Q is locally connected if every subalgebra $Q' \leq Q$ is connected.*

ii) *Q is totally connected if for all $n \in \mathbb{N}$, Q^n is locally connected.*

iii) *Q is uniformly connected if it has a Merling term.*

Note that an idempotent, right quasigroup is totally connected if and only if all of its subpowers are connected.

These are increasingly strong notions of connectedness. That is, each subsequent notion of connectedness implies those before it. Let Q be a right quasigroup. Then Q being locally connected implies Q is connected: If Q is locally connected, then trivially, Q is a subalgebra of itself and hence must be connected. If Q is totally connected, then $Q^1 = Q$ is locally connected. As will be shown in Theorem 11, if Q is uniformly connected, then it is totally connected. Another consequence of Theorem 11 is if Q is totally connected, then Q is also uniformly connected. In order to show this, however, we first need to show that uniformly connected implies connected:

Lemma 10. *If an idempotent, right quasigroup is uniformly connected, then it is connected.*

Proof: Let Q be an idempotent, right quasigroup with a Merling term $m(x,y)$. Since $m(x,y) = x$ in U_2, x appears left-most in $m(x,y)$. That is $m(x,y)$ must be of the form presented in Figure 3 where for all $1 \leq i \leq n$, $\circ_i$ is in $\{*, /\}$ and t_i is a binary term. Then, for $a, b \in Q$ there is a series of right translations from a to $m(a,b) = b$ in Q by the elements $t_1(a,b), t_2(a,b), \dots, t_n(a,b)$. Each right translation corresponds to an edge in Cayley(Q). This means that there is a path from a to b in Cayley(Q) for all a, b in Q. In other words, Cayley(Q) is connected, and hence Q is connected. ■

Now we can prove that uniformly connected and totally connected are equivalent:

Theorem 11. *An idempotent, right quasigroup is totally connected if and only if it has a Merling term.*

Proof: Let Q be a totally connected idempo-

tent, right quasigroup. Let $\mathcal{F}(2, Q)$ be the free term algebra on two generators over Q [14]. This algebra is founded over the binary terms $t(x, y)$ over the signature $\{*, /\}$. Two terms $t(x, y)$ and $s(x, y)$ are in the same equivalence class if Q satisfies

$$\forall xy(t(x, y) = s(x, y)).$$

Identifying the equivalence class of $t(x, y)$ in $\mathcal{F}(2, Q)$ with its term operation $t : Q^2 \to Q$, it follows via a routine verification that $\mathcal{F}(2, Q)$ is a subalgebra of $Q^{|Q|^2}$, and hence a subpower of Q.

Since Q is totally connected, its subpower $\mathcal{F}(2, Q)$ is necessarily connected. This means that there is a path in the (right) Cayley graph of $\mathcal{F}(2, Q)$ from the term x to the term y. This path corresponds to a sequence of right translations by binary terms $t_1(x, y), t_2(x, y), \ldots t_n(x, y)$. From these terms, form $m(x, y)$ as in Figure 3. Clearly, $m(x, y) = y$ in Q, since the right translations correspond to the path in $\mathcal{F}(2, Q)$ from x to y. Moreover, since x is the leftmost variable in the expression $m(x, y)$, $m(x, y) = x$ in U_2. Hence, $m(x, y)$ is a Merling term for Q.

Now let Q be an idempotent, right quasigroup with a Merling term $m(x, y)$. All algebras in the variety of Q must also satisfy $m(x, y) = y$ and so inherit this Merling term. Specifically, $m(x, y)$ is a Merling term for each $R \leq Q^n$ for all $n \in \mathbb{N}$. That is each subpower R of Q is uniformly connected, and hence is connected by Lemma 10. Thus, Q is totally connected. ■

B. P/NP Dichotomy

We now have the necessary results about connectivity to prove a tractability dichotomy in idempotent, right quasigroups. The next two lemmas prove one half of the dichotomy by providing a sufficient condition for an idempotent, right quasigroup to be NP-complete.

Lemma 12. *If an idempotent, right quasigroup Q is not totally connected, then U_2 is in its variety.*

Proof: Since Q is not totally connected, there is a power $R \leq Q^n$ that is not connected. Since R is not connected, there exist at least two distinct connected components of Cayley(R). Let C be one of these connected components. Define $h : R \to U_2$ by

$$h(z) = \begin{cases} 0 & \text{if } z \in C \\ 1 & \text{otherwise} \end{cases}$$

It is left to the reader to verify that this is indeed a right quasigroup homomorphism onto U_2. This places U_2 in the variety of Q. ■

Lemma 13. *If an algebra A has U_2 in its variety, then it is NP-complete.*

Proof: From Example 3, first note that U_2 is NP-complete.

Suppose U_2 is in the variety of A. Then A has a subpower $R \leq A^n$ such that there exists a surjective homomorphism $h : R \to U_2$. According to Corollary 7.3 of [1], R is NP-complete by virtue of its unary factor U_2. This means that there exists an NP-complete CSP over R. Any CSP over R is also a CSP over A, so CSP (A) is also NP-complete. Hence A is NP-complete. ■

Corollary 14 (Dichotomy Theorem)**.** *If an idempotent, right quasigroup Q is not NP-complete, it must be tractable.*

Equivalently, Q is NP-complete if and only if Q is not totally connected.

Proof: If Q is not NP-complete, then by the contrapositive of Lemma 13, Q does not have U_2 in its variety. Then by Lemma 12, Q is totally connected. By Theorem 11, Q has a Merling term and must be tractable by Corollary 8. ■

V. The Merling Condition and Involutory Quandles

It follows from Section IV that an idempotent, right quasigroup Q is NP-complete if and only if Q is not totally connected. In other words, tractable (not NP-complete) idempotent, right quasigroups must have Merling terms. Therefore, determining the P/NP-complete classification of idempotent, right quasigroups can be reduced to a term search. However, finding term functions is, in general, EXPTIME-complete [6]. On the other hand, given a first-order formula, checking whether or not the equation holds for an algebra takes polynomial time on the size of the algebra [4]. Hence it is preferable, whenever possible, to find a single, fixed first-order formula to determine whether an idempotent, right quasigroup is NP-complete or not. We introduce a candidate formula below and demonstrate that this formula is effective for a well-studied subclass of idempotent, right quasigroups.

Definition 15. *An algebra A is said to satisfy the Merling condition if*

$$A \models \forall xy(x * y = x \Rightarrow x = y).$$

Lemma 16. *If A is an algebra that satisfies the Merling condition, then A^n satisifies the Merling condition for all $n \in \mathbb{N}$.*

Proof: Let A be an algebra that satisfies the Merling condition. Suppose there exists $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in A^n$ such that $x * y = x$. Then for every $1 \leq i \leq n$, $x_i * y_i = x_i$. Since A satisfies the Merling condition, $x_i = y_i$ for all $1 \leq i \leq n$, which implies that $x = (x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) = y$. ■

A. Quandles

Joyce introduced the first-order theory of quandles in [9]. They originate from the "crossover algebra" of three-dimensional knots.

Definition 17. *A quandle $(Q, *, /)$ is a set Q together with two binary operations $*, / : Q^2 \to Q$ satisfying the following axioms:*

Idempotence: $\forall x(x * x = x)$.

Right Cancellation I: $\forall xy((x * y)/y = x)$.

Right Cancellation II: $\forall xy((x/y) * y = x)$.

Right Self-Distributivity: $\forall xyz((x*y)*z = (x*z) * (y * z))$.

Of course, quandles form a subclass of idempotent, right quasigroups and so also exhibit P/NP-complete dichotomy.

Theorem 18. *If a finite quandle Q does not satisfy the Merling condition, then U_2 is a subalgebra of Q.*

Proof: Suppose that a quandle Q does not satisfy the Merling condition, but U_2 is not a subalgebra for the sake of contradiction. Then there exist two distinct elements x, y in Q such that $x * y = x$. Define $v_0 = x$ and $v_i = y * v_{i-1}$.

TABLE II. PARTIAL $*$ CAYLEY TABLE FOR Q

$*$	y	v_0	v_1	v_2	$\ldots$	v_{n-1}
y	y	v_1	v_2	v_3	$\ldots$	v_n
v_0	v_0	v_0	v_0	v_0	$\ldots$	v_0
v_1	v_1		v_1	v_1	$\ldots$	v_1
v_2	v_2			v_2	$\ldots$	v_2
$\vdots$	$\vdots$				$\ddots$	$\vdots$
v_{n-1}	v_{n-1}				$\ldots$	v_{n-1}

We need to show that for all i in $\mathbb{N}$, $v_i * y = v_i$. We proceed by induction on i. The base case is $i = 0$, and indeed $v_0 * y = x * y = x = v_0$. Now suppose $v_{i-1} * y = v_{i-1}$ for some i. From self-distributivity and idempotence, $v_i * y = (y * v_{i-1}) * y = (y * y) * (v_{i-1} * y) = y * v_{i-1} = v_i$.

We also need to show that for a given i in $\mathbb{N}$ that for all $j \geq i$, $v_i * v_j = v_i$. We proceed by induction on $j \geq i$. In the simplest case $j = i$, so $v_i * v_j = v_i * v_i = v_i$. Now assume that $j > i$ and $v_i * v_{j-1} = v_i$. Then since $v_i * y = v_i$, $v_i * v_j = (v_i * v_{j-1}) * (y * v_{j-1}) = (v_i * y) * v_{j-1} = v_i * v_{j-1} = v_i$.

Now we prove that for $n \in \mathbb{N}$, $v_n \neq y$ and $v_i \neq v_j$ whenever $0 \leq i < j \leq n$. We proceed by induction on n. The base case is when $n = 0$. Trivially, $v_0 = x$ does not equal y and there are no instances of $0 \leq i < j \leq 0$ to consider. Now suppose v_0 through v_{n-1} are all distinct for some n and $v_i \neq y$ for all $i < n$. $v_{n-1} * y = v_{n-1}$, $v_{n-1} * v_{n-1} = v_{n-1}$, and $y * v_{n-1} = v_n$, so if $v_n = y$, then $\{y, v_{n-1}\} = U_2$, a contradiction, so $v_n \neq y$. If $v_n = v_i$ for some $i < n$, then $y * v_{n-1} = v_i * v_{n-1}$. From right cancellation, $y = v_i$, a contradiction, so $v_n \neq v_i$ for all $i < n$. Hence v_n is distinct from all v_i for $i < n$.

However, then Q contains $\{v_i\}_{i=0}^{n}$ for all $n \in \mathbb{N}$, so Q is infinite, a contradiction. Hence U_2 must be a subalgebra of Q. ■

Corollary 19. *If U_2 is a subpower of a finite quandle then it is also a subalgebra.*

Proof: Let U_2 be a subalgebra of Q^n. Then there exist distinct x and y in $U_2 \leq Q^n$ such that $x * y = x$. Hence Q^n does not satisfy the Merling condition. By Lemma 16, Q does not satisfy the Merling condition. Then by Theorem 18, U_2 is a subalgebra of Q. ■

B. Involutory Quandles

Definition 20. *An involutory quandle $(Q, *)$ is a set Q together with a binary basic operation $* : Q^2 \to Q$ satisfying the following axioms:*

Idempotence: $\forall x(x * x = x)$.

Right Cancellation: $\forall xy((x * y) * y = x)$.

Right Self-Distributivity: $\forall xyz((x*y)*z = (x*z) * (y * z))$.

Note that an involutory quandle is a quandle where $*$ and $/$ define the same operation.

The Merling condition axiomatizes the P/NP-complete dichotomy that involutory quandles inherit from idempotent, right quasigroups. We already have most of the proof. Namely, if an involutory quandle Q does not satisfy the Merling condition, then U_2 is a subalgebra of Q. But CSP (U_2) is NP-complete, so Q must also be NP-complete. Otherwise, we will want it to be totally connected, as we know totally connected quandles

are tractable, since they have Malcev terms. We leverage the fact that the Merling condition is inherited by powers since this allows us to reduce the problem to showing that the Merling condition implies connectedness.

Theorem 21. *If a finite, involutory quandle Q satisfies the Merling condition, then Q is connected.*

Proof: Suppose Q is not connected for sake of contradiction. Then there are two distinct elements x and y of Q in two different connected components of Cayley(Q). Define $x_0 = x$, $x_{2i-1} = x_{2i-2} * y$, and $x_{2i} = x_{2i-1} * x$.

TABLE III. PARTIAL $*$ CAYLEY TABLE FOR Q

$*$	x	y
x_0	x_0	x_1
x_1	x_2	
x_2		x_3
x_3	x_4	
x_4		x_5
$\vdots$	$\vdots$	$\vdots$

It is shown below that, for each $j \in \mathbb{N}$, the elements $x_0, x_1, \ldots, x_j$ are distinct. This proceeds by induction on j. For $j = 0$ this is certainly true since there is just one element to consider. When $j = 1$, there are just two elements x_0 and x_1 and $x_1 = x_0 * y$. If $x_1 = x_0$ then $x = x_0 = x_1 = x * y$, then $x = y$ by the Merling condition. But x and y are distinct, a contradiction, so x_0 and x_1 are distinct.

Now let $i \geq 1$ and suppose $x_0, x_1, \ldots, x_i$ are all distinct. Let $j = i+1$ and assume that for some $0 \leq k \leq i$ that $x_j = x_k$. We consider the cases in which $j > 1$ is even or odd.

- $j = i + 1$ **is even:** Then we may partition the possible values of k into the following four categories.
  - $k = 0$: Then if $x_j = x_k$, $x_i * x = x_{i+1} = x_j = x_k = x_0 = x = x*x = x_0*x$. By right cancellation, $x_i = x_0$. Since $j = i + 1$ is even, i is odd and so $i > 0$.
  - k is odd and $0 < k < i - 1$: Then $x_i * x = x_{i+1} = x_j = x_k$ so that $x_i = (x_i * x) * x = x_k * x = x_{k+1}$. Since $k < i - 1$, $k + 1 < i$.
  - k is even and $0 < k < i$: Then $x_i * x = x_{i+1} = x_j = x_k = x_{k-1} * x$. Right cancellation ensures that $x_i = x_{k-1}$. Also, $0 < k - 1 < k \leq i$.
  - $k = i$; Then $x_i * x = x_{i+1} = x_j = x_k = x_i$. Since Q satisfies the Merling condition, $x_i = x = x_0$.

  In each case, the assumption that $x_j = x_k$ forces $x_i = x_l$ for some $0 \leq l < i$. This contradicts the assumption that $x_0, x_1, \ldots, x_i$ are distinct. Hence, for $j > 1$ even, $x_j \neq x_k$.
- $j = i+1$ **is odd:** Here is an exhaustive list of cases for k.
  - $k = 0$: Then $x_i * y = x_{i+1} = x_j = x_0$ which means $x_i = (x_i * y) * y = x_0 * y = x_1$. Since $j > 1$ is odd, $i + 1 = j > 2$. Thus, $i \geq 2 > 1$.
  - k is odd and $0 < k < i$: Then $x_i * y = x_{i+1} = x_j = x_k = x_{k-1} * y$. By right cancellation, $x_i = x_{k-1}$ but $k - 1 < k < i$.
  - k is even and $0 < k < i - 1$: Then $k + 1$ is odd so $x_{k+1} = x_k * y$. Therefore, $x_{k+1} * y = (x_k * y) * y = x_k = x_j = x_{i+1} = x_i * y$. Right cancellation yields $x_i = x_{k+1}$ but since $k < i - 1$, $k + 1 < i$.
  - $k = i$; Then $x_i * y = x_{i+1} = x_j = x_k = x_i$. Since Q satisfies the Merling condition, $x_i = y$. However, x_i is in the same connected component as x but y is in a different connected component from x.

  In each subcase, the assumption that $x_j = x_k$ generates a contradiction. The first three subcases lead to a contradiction of the induction hypothesis while the last merges two distinct connected components of Q into one. Since the set of subcases cover all possibilities for k, it follows that $x_j \neq x_k$ when $j > 1$ is odd.

This means that the finite Q contains the infinite set $\{x_j | j \in \mathbb{N}\}$, which is an obvious contradiction. Hence, the assumption that Q is disconnected was in error. ∎

Corollary 22. *If an involutory quandle satisfies the Merling condition it is tractable. If it does not satisfy the Merling condition it is NP-complete.*

Proof: Let Q be an involutory quandle. Suppose Q satisfies the Merling condition. Note that the Merling condition is inherited by subalgebras, so by Lemma 16 and Theorem 21, all subpowers of Q are connected, i.e., Q is totally connected. Thus by Corollary 14, Q is tractable. If Q does not satisfy the Merling condition, then by Theorem 18 and Lemma 13, Q is NP-complete. ∎

VI. Future Work

One obvious line of research is to see whether Corollary 22 can be extended to the following, or to all idempotent, right quasigroups, for that matter.

Conjecture 23. *A quandle is tractable if it satisfies the Merling condition and NP-complete otherwise.*

Another direction to consider is to have the results of this article inform the search for "interesting" finite algebras. We consider an algebra to be interesting when it is not readily classifiable as tractable or NP-complete. Of course, non trivial right-cancelable operations should be avoided. We close with a candidate theory for further exploration.

Definition 24. *A Quay algebra is a set Q together with a binary operation $* : Q^2 \to Q$ satisfying the following axioms:*

$$\forall x(x * x = x).$$

$$\forall xyz(((x * z) * y) * z = x * (y * z)).$$

The second axiom is a theorem of involutory quandles. However, Quay algebras satisfy neither right cancellation nor right self-distributivity. They are a rich class of algebras which include the class of involutory quandles and the class of semilattices.

Lemma 25. *All involutory quandles are Quay algebras.*

Proof: Let Q be an involutory quandle. So Q is idempotent. Q also satisfies the conditions $(x * y) * y = x$ and $(x * y) * z = (x * z) * (y * z)$, which give $((x*z)*y)*z = ((x*z)*z)*(y*z) = x*(y*z)$. Therefore, by definition, Q is a Quay algebra. ■

Definition 26. *A semilattice is an algebraic structure $(S, *)$ together with a binary operation *, such that:*

$$\forall x(x * x = x).$$

$$\forall xy(x * y = y * x).$$

$$\forall xyz((x * y) * z = x * (y * z)).$$

Lemma 27. *All semilattices are Quay algebras.*

Proof: Let S be a semilattice. So S is idempotent. S also satisfies the conditions $x*y = y*x$ and $(x*y)*z = x*(y*z)$, which give $((x*z)*y)*z = ((x*y)*z)*z = (x*y)*z = x*(y*z)$. Therefore, by definition, S is a Quay algebra. ■

From [8], semilattices are tractable. Thus we have some Quay algebras that are tractable and some that are NP-complete.

A. Acknowledgements

The authors would like to acknowledge Peter Golbus and Mona Merling for their early contributions to this research program and Brita Brudvig, Aleksandr Chakarov, Max Jeter, Benjamin Selfridge, and Liwen Song for their assistance at later stages.

We also thank M.E. Adams, Kira Adiracheva, Joel Berman, David Hobby, J.B. Nation, Donald Silberger, Jonathan D.H. Smith, and Michal Stronkowski for providing valuable feedback.

References

[1] A. Bulatov, P. Jeavons, and A. Krokhin. Classifying the complexity of constraints using finite algebras. *SIAM Journal on Computing.*, 34(3):720–742, April 2005.

[2] Andrei Bulatov and Víctor Dalmau. A simple algorithm for Mal'tsev constraints. *SIAM J. Comput.*, 36(1):16–27, July 2006.

[3] S. Burris and H.P. Sankappanavar. *A Course in Universal Algebra*. Graduate texts in mathematics. Springer-Verlag, 1981.

[4] Heinz-Dieter Ebbinghaus and Jorg Flum. *Finite Model Theory*. University of Freiburg, Freiburg, 1995.

[5] Tomás Feder and Moshe Y. Vardi. The computational structure of monotone monadic SNP and constraint satisfaction: A study through datalog and group theory. *SIAM Journal on Computing*, 28(1):57–104, February 1999.

[6] Ralph Freese and Matthew A. Valeriote. On the complexity of some Maltsev conditions. *International Journal of Algebra & Computation*, 19(1):41 – 77, 2009.

[7] Peter Jeavons, David Cohen, and Martin Cooper. Constraints, consistency, and closure. *Artificial Intelligence*, 101:101–1, 1998.

[8] Peter Jeavons, David Cohen, and Marc Gyssens. Closure properties of constraints. *J. ACM*, 44(4):527–548, July 1997.

[9] David Joyce. A classifying invariant of knots; the knot quandle. *Journal of Pure and Applied Algebra*, (23):37–65, 1982.

[10] Ho Weng Kin. Generalized majority-minority operations are tractable. In *Proceedings of the 20th Annual IEEE Symposium on Logic in Computer Science*, LICS '05, pages 438–447, Washington, DC, USA, 2005. IEEE Computer Society.

[11] Tomás Kowalski, Francesco Paoli, and Antonio Ledda. On independent varieties and some related notions. *Algebra Universalis.*, 70(2):107–136, October 2013.

[12] W. Magnus, A. Karrass, and D. Solitar. *Combinatorial Group Theory: Presentations Of Groups In Terms Of Generators And Relations*. Dover Books on Mathematics. Dover Publications, 2004.

[13] Lee Spector, David M. Clark, Ian Lindsay, Bradford Barr, and Jon Klein. Genetic programming for finite algebras. In *Proceedings of the 10th annual conference on Genetic and evolutionary computation*, GECCO '08, pages 1291–1298, New York, NY, USA, 2008. ACM.

[14] J. Wood. Subtraces and shadow chains. *Algebra Universalis.*, 41(3):233–237, August 1999.