Quantified Constraint Satisfaction on Monoids*

Hubie Chen[1] and Peter Mayr[2]

1 **University of the Basque Country (UPV/EHU), E-20018 San Sebastián, Spain; and**
IKERBASQUE, Basque Foundation for Science, E-48011 Bilbao, Spain
hubie.chen@ehu.es

2 **Department of Mathematics, University of Colorado Boulder, Campus Box 395, Boulder, CO 80309-0395, USA**
peter.mayr@colorado.edu

Abstract

We contribute to a research program that aims to classify, for each finite structure, the computational complexity of the quantified constraint satisfaction problem on the structure. Employing an established algebraic viewpoint to studying this problem family, whereby this classification program can be phrased as a classification of algebras, we give a complete classification of all finite monoids.

1998 ACM Subject Classification F.4.1 Mathematical Logic

Keywords and phrases quantified constraint satisfaction, universal algebra, computational complexity

Digital Object Identifier 10.4230/LIPIcs.CSL.2016.15

1 Introduction

Problem frameworks. The *constraint satisfaction problem (CSP)* is a generic combinatorial problem where an input consists of a set of constraints on a set of variables, and the question is to determine whether or not there is an assignment to the variables satisfying all of the constraints. The CSP can be formulated logically as the problem of deciding, given an *existential conjunctive sentence* and a finite structure, whether or not the sentence evaluates to true on the structure. By an *existential conjunctive sentence*, we mean a first-order sentence built from atoms, conjunction ($\wedge$), and existential quantification ($\exists$).

It is well-known that the CSP is NP-complete in general. However, one can define, for each finite structure $\mathbb{B}$, the problem CSP($\mathbb{B}$) to be the restricted version of the CSP where the structure is fixed as $\mathbb{B}$, and in this way obtain a rich family of problems, some of which are polynomial-time decidable and hence escape the general intractability of the CSP. This family includes a variety of well-established combinatorial problems, such as graph homomorphism problems (for examples, *2-colorability*, *3-colorability*, and various generalizations thereof); Boolean satisfiability problems (for examples, *2-SAT* and *Horn-SAT*); and algebraic equations problems.

A natural generalization of the CSP is the *quantified constraint satisfaction problem (QCSP)*, where the task is to decide whether or not a *quantified conjunctive sentence* holds true on a structure. By a *quantified conjunctive sentence*, we mean a first-order sentence built

* The first author was supported by the Spanish Project MINECO COMMAS TIN2013-46181-C2-R, Basque Project GIU15/30, and Basque Grant UFI11/45; the second by the Austrian Science Fund (FWF): P24285.

from atoms, conjunction ($\wedge$), and both quantifiers ($\exists, \forall$); so, the QCSP may be described as the generalization of the CSP where both quantifiers are permitted, as opposed to just existential quantifiers. It is well-known that the QCSP is PSPACE-complete in general. For each finite structure $\mathbb{B}$, one may also define QCSP($\mathbb{B}$) to be the restricted version of the QCSP where the structure is fixed as $\mathbb{B}$. The resulting problem family includes quantified generalizations of the mentioned combinatorial problems. (For a broader perspective on model checking various fragments of first-order logic on fixed finite structures, we refer the reader to [18].)

Classification. The problem families CSP($\mathbb{B}$) and QCSP($\mathbb{B}$) give rise to fundamental classification programs, in which researchers aim to describe the complexity of each of the problems in the respective families. Perhaps the best-known result in this vein is Schaefer's dichotomy theorem [22], which shows for each two-element structure $\mathbb{B}$, the problem CSP($\mathbb{B}$) is polynomial-time decidable if the structure $\mathbb{B}$ satisfies one of six presented conditions, and is NP-complete otherwise. Schaefer also claimed without proof a partial classification of the problems QCSP($\mathbb{B}$), over all two-element structures $\mathbb{B}$; a complete classification was presented and proved in the book [12]. Current research on the CSP [16, 1] and the QCSP [7, 19, 8, 9, 17, 6] aims to understand the behavior of all finite structures with respect to each of these two problem families, without any universe size restriction of the type employed by Schaefer. At the present juncture, it seems fair to suggest that the family QCSP($\mathbb{B}$) is less understood than the family CSP($\mathbb{B}$). For examples of evidence, we observe that the classification of CSP($\mathbb{B}$) over all undirected graphs is a classical result due to Hell and Nesetril [14], but no such classification is known for QCSP($\mathbb{B}$) (although partial results exist [20, 9]); also, the classification of CSP($\mathbb{B}$) over all three-element structures was given by Bulatov [5], but no such classification is known for QCSP($\mathbb{B}$) (see [7, 8] for partial results).

A significant stimulus for these classification programs was the introduction of an algebraic approach [3] that permits the deployment of notions, concepts, and results from universal algebra. A cornerstone of this algebraic approach is the passage from a structure $\mathbb{B}$ to an algebra, the so-called algebra of *polymorphisms* of $\mathbb{B}$. It is known that, intuitively speaking, this algebra retains the relevant information about the complexity of the structure, in the precise sense that two structures $\mathbb{B}, \mathbb{B}'$ sharing the same algebra enjoy that the problems CSP($\mathbb{B}$) and CSP($\mathbb{B}'$) are interreducible [3], and similarly that the problems QCSP($\mathbb{B}$) and QCSP($\mathbb{B}'$) are interreducible [2]. (Here, we mean *interreducible* with respect to many-one polynomial-time reduction). In fact, each of the described classification programs on structures can be rephrased as a classification program on algebras (see [3]).

An initial basic result of the algebraic approach to the CSP states that, for each structure $\mathbb{B}$, there exists a structure $\mathbb{B}'$ whose algebra is *idempotent*, such that CSP($\mathbb{B}$) and CSP($\mathbb{B}'$) are interreducible [3]. An algebra is *idempotent* if each operation f thereof is idempotent in that $f(a, \ldots, a) = a$ holds for each element a. On the algebraic side, this result implies that one can restrict to studying and to classifying idempotent algebras in order to carry out the classification program on the problem family CSP($\mathbb{B}$). In contrast to this state of affairs for the CSP, the QCSP has not seen any such result that allows attention to be restricted to idempotent algebras, although attempts have been made to understand this discrepancy [11]. Despite the lack of such a result for the QCSP, we believe it fair to claim that the development of the algebraic approach for the QCSP has focused on idempotent algebras [7, 8, 9, 6]. Non-idempotent algebras hence constitute a *terra incognita* in QCSP research.

Contribution. The present article was motivated by the desire to initiate a systematic study of the *terra incognita* of non-idempotent algebras, with respect to QCSP complexity. In this article, we investigate the class of finite monoids. Recall that a *semigroup* is an algebra comprised of a set equipped with an associative binary operation; a *monoid* is a semigroup whose operation has an identity element.

Our main theorem is the complete classification of finite monoids with respect to QCSP complexity. We identify a simply stated algebraic condition on monoids, and show that each monoid satisfying this condition has a polynomial-time tractable QCSP; we show that all other monoids have an NP-complete QCSP. (See Theorem 7 for a precise statement.) We remark that the fact that each monoid has a QCSP in NP is due to previous work (see Theorem 6). We elected to focus on classifying monoids since their CSP complexity was already understood—indeed, semigroups were historically one of the first classes of algebras to be understood for the CSP [4]—and also because this would permit the usage of the established structure theory of semigroups. Indeed, our work opens up an interface between quantified constraint satisfaction and semigroup theory that, we believe, presents new perspectives on each of these two fields. One intriguing aspect of our dichotomy theorem is this: the algebraic condition that we identify concerns whether or not the monoid is generated by a particular subset of its elements. At the same time, the size of generating sets for algebras was previously linked to QCSP complexity, in particular, to the study of which problems QCSP($\mathbb{B}$) are in NP [8, 9].

2 Preliminaries

2.1 General preliminaries

When $\mathcal{A}, \mathcal{B}$ are decision problems such that there is a polynomial-time many-one reduction from $\mathcal{B}$ to $\mathcal{A}$, we write $\mathcal{B} \leq_p^m \mathcal{A}$. When I is an instance of a decision problem and I' is also an instance of a decision problem, we say that I and I' are *decision-equivalent* when I is a *yes* instance iff I' is a *yes* instance.

2.2 Semigroups

We recall some notation and basic facts for semigroups that will be used in this paper (see [15]). A *semigroup* $\mathbf{S} = \langle S, \cdot \rangle$ is a non-empty set S with an associative binary operation $\cdot$, the multiplication. A *subsemigroup* of $\mathbf{S}$ is a non-empty subset $T \subseteq S$ that is closed under multiplication. An element $x \in S$ is *idempotent* if $x^2 = x$. We will use the fact that, when $\mathbf{S}$ is a finite monoid of size n, for each element $x \in S$, it holds that $x^{n!}$ is idempotent. If $\mathbf{S}$ contains an element 1 such that $x \cdot 1 = 1 \cdot x = x$ for all $x \in S$, we call 1 the *identity* of $\mathbf{S}$ and $\mathbf{S}$ a *monoid*. If $\mathbf{S}$ has no identity, we can adjoin an extra element 1 to S to form a monoid $\mathbf{S}^1$. For that, let S^1 denote $S \cup \{1\}$ and extend the multiplication of $\mathbf{S}$ by $1 \cdot x = x \cdot 1 = x$ for all $x \in S^1$. If $\mathbf{S}$ already contains an identity, let $\mathbf{S}^1 = \mathbf{S}$. An element $a \in S$ is *regular* if there exists $x \in S$ such that $axa = a$. A semigroup is *zero* if its multiplication is constant.

Let $\mathbf{S}$ be a semigroup. An *ideal* is a non-empty subset $I \subseteq S$ such that $SI := \{si \ : \ s \in S, i \in I\} \subseteq I$ and $IS := \{is \ : \ s \in S, i \in I\} \subseteq I$. The ideal generated by an element $a \in S$ is hence S^1aS^1. The equivalence relation $\mathcal{J}$ on S is defined by $a \mathcal{J} b$ iff $S^1aS^1 = S^1bS^1$. The equivalence classes of the equivalence relation $\mathcal{J}$ are called $\mathcal{J}$*-classes*, and the $\mathcal{J}$-class containing the element a is denoted by J_a. There is a natural partial order on $\mathcal{J}$-classes, given by $J_a \leq J_b$ iff $S^1aS^1 \subseteq S^1bS^1$.

A *right ideal* of $\mathbf{S}$ is a non-empty subset $A \subseteq S$ such that $AS \subseteq A$. The right ideal generated by an element $a \in S$ is aS^1. The equivalence relation $\mathcal{R}$ on S is defined by $a\mathcal{R}b$ iff $aS^1 = bS^1$. In an analogous fashion, we define *left ideals* and the equivalence $\mathcal{L}$.

Given an ideal I of a semigroup $\mathbf{S} = \langle S, \cdot \rangle$, the *Rees quotient* $\mathbf{S}/I$ is the semigroup on $(S \setminus I) \cup \{0\}$ with multiplication

$$xy := \begin{cases} x \cdot y & \text{if } x, y \in S \text{ and } x \cdot y \in S \setminus I, \\ 0 & \text{otherwise.} \end{cases}$$

For a group $\mathbf{G}$, sets I, Λ and a $\Lambda \times I$-matrix P with entries in $G \cup \{0\}$ the *Rees matrix semigroup* $\mathbf{M} := M^0(\mathbf{G}, I, \Lambda, P)$ is defined on the set

$$M^0 = \{(i, g, \lambda) \ : \ i \in I, g \in G, \lambda \in \Lambda\} \cup \{0\}$$

with multiplication

$$(i, g, \lambda)(j, h, \mu) := \begin{cases} (i, gP_{\lambda,j}h, \mu) & \text{if } P_{\lambda,j} \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

for all $(i, g, \lambda), (j, h, \mu) \in M^0$ and by $x0 = 0x = 0$ for all $x \in M^0$. The *Rees matrix semigroup* $\mathbf{M} := M(\mathbf{G}, I, \Lambda, P)$ is defined similarly on $M = \{(i, g, \lambda) \ : \ i \in I, g \in G, \lambda \in \Lambda\}$ when P has entries in G.

We collect some well-known facts on $\mathcal{J}$-classes of finite semigroups from Section 3 of [15] in the following lemma.

▶ **Lemma 1.** *Let $\mathbf{S}$ be a finite semigroup and $a \in S$.*

1. *If a is not regular, then J_a is not minimal and $(S^1aS^1)/\bigcup\{J_x \ : \ J_x < J_a\}$ is a zero semigroup.*
2. *If a is regular and J_a not minimal, then $(S^1aS^1)/\bigcup\{J_x \ : \ J_x < J_a\}$ is isomorphic to a Rees matrix semigroup $M^0(\mathbf{G}, I, \Lambda, P)$ for some group $\mathbf{G}$, index sets I, Λ and a $\Lambda \times I$-matrix P with entries in $G \cup \{0\}$ such that every row and every column contains an element from G.*
3. *If J_a is the minimal $\mathcal{J}$-class, then it is isomorphic to a Rees matrix semigroup $M(\mathbf{G}, I, \Lambda, P)$ for some group $\mathbf{G}$, index sets I, Λ and a $\Lambda \times I$-matrix P with entries in G.*

Let $\mathbf{S}$ be a semigroup. Then $\mathbf{S}$ is a *block group* if for all idempotents $e, f \in S$:

$$ef = e, fe = f \Rightarrow e = f,$$
$$ef = f, fe = e \Rightarrow e = f.$$

Equivalently, $\mathbf{S}$ is a block group if every $\mathcal{L}$-class and every $\mathcal{R}$-class of $\mathbf{S}$ contains at most one idempotent. We will make use of the following facts on block groups.

▶ **Lemma 2.** *Let $\mathbf{S}$ be a finite block group with $a \in S$ regular.*

1. *If J_a is not minimal, then $(S^1aS^1)/\bigcup\{J_x \ : \ J_x < J_a\}$ is isomorphic to a Rees matrix semigroup $M^0(\mathbf{G}, I, I, P)$ for some group $\mathbf{G}$, an index set I and the identity matrix P.*
2. *If J_a is the smallest $\mathcal{J}$-class, then it forms a group $\mathbf{G}$.*
3. *There exist unique idempotents $e \in R_a$, $f \in L_a$ such that $ea = af = a$.*

Proof. Item (1) follows from Lemma 1 (2): $(S^1aS^1)/\bigcup\{J_x \ : \ J_x < J_a\}$ is some $M^0(\mathbf{G}, I, \Lambda, P)$. Note that whenever $P_{\lambda,i} \neq 0$ for some $i \in I, \lambda \in \Lambda$, then $e = (i, P^{-1}_{\lambda,i}, \lambda)$ is idempotent. Suppose $f = (j, P^{-1}_{\lambda,j}, \lambda)$ for $j \in I$ is idempotent as well. Then $ef = e$ and $fe = f$. Since $\mathbf{S}$ is

a block group this implies $e = f$ and $i = j$. Consequently $P_{\lambda,j} = 0$ for all $j \neq i$. Hence every row of P (and similarly every column) contains at most one non-zero entry. Together with Lemma 1 (2) it follows that every row and every column of P contains exactly one entry from G, the remaining being 0. Hence $|I| = |\Lambda|$. By reordering rows and columns and normalizing P, we obtain that $(S^1aS^1)/\bigcup\{J_x \ : \ J_x < J_a\}$ is isomorphic to $M^0(\mathbf{G}, I, I, P)$ with P the identity matrix.

By a similar argument Lemma 1 (3) implies item (2). We have that J_a is isomorphic to $M(\mathbf{G}, I, \Lambda, P)$ for some group $\mathbf{G}$, index sets I, Λ and a $\Lambda \times I$-matrix P with entries in G. Since $\mathbf{S}$ is a block group, P contains at most one entry in every row and column. So $|I| = |\Lambda| = 1$ and $M(\mathbf{G}, I, \Lambda, P)$ is isomorphic to $\mathbf{G}$.

For (3) we may identify the elements of J_a with $\{(i, g, j) \ : \ i, j \in I, g \in G\}$ by (1), (2), respectively. Let $a = (i, g, j)$ for some $i, j \in I, g \in G$. Then $e := (i, 1, i)$, $f := (j, 1, j)$ are the unique idempotents in R_a, L_a, respectively. Clearly $ea = af = a$. ◀

2.3 Algebra and constraint satisfaction

An *algebra* $\mathbf{A} = \langle A, F\rangle$ is a non-empty set A paired with a set of finitary operations F on A. A subset $R \subseteq A^n$ is an n-ary *relation* on A. A k-ary operation $f\colon A^k \to A$ *preserves* or *is a polymorphism of* an n-ary relation R if for any choice of k tuples $(a_1^1, \ldots, a_n^1), \ldots, (a_1^k, \ldots, a_n^k) \in R$, it holds that the tuple $(f(a_1^1, \ldots, a_1^k), \ldots, f(a_n^1, \ldots, a_n^k))$ is in R. We say that a relation is *preserved* by an algebra if it is preserved by all operations of the algebra, and we say that a relational structure is *preserved* by an algebra if each of its relations is preserved by the algebra. (We remark that, algebraically, a non-empty relation is preserved by an algebra iff it is the universe of a subalgebra of a power of the algebra.) Here, a *relational signature* is a set of *relation symbols*, each having an associated arity, and a *relational structure* $\mathbb{B}$ over a relational signature σ provides a non-empty set B and an interpretation $R^{\mathbb{B}} \subseteq B^k$ for each relation symbol $R \in \sigma$; here, k denotes the arity of R. We assume that each relational signature is finite, and that each relation of a relational structure is represented using a list of its tuples. If an algebra $\mathbf{A}$ preserves a relational structure $\mathbb{B}$, then the universe of $\mathbb{B}$ is a subset of the universe of $\mathbf{A}$. For a more detailed study on which relational structures are preserved by semigroups we refer to [21].

In this article, we deal with relational first-order logic. Define a *qcsp-sentence* to be a first-order sentence of the form $Q_1 v_1 \ldots Q_n v_n \phi$ where each Q_i is a quantifier in $\{\forall, \exists\}$; the v_i are variables, assumed to be pairwise distinct; and ϕ is a conjunction of atoms. By an *atom*, we refer to the application $R(w_1, \ldots, w_k)$ of a relation symbol to a tuple of variables. Define a *csp-sentence* to be a qcsp-sentence in which all quantifiers are existential.

When $\mathbf{A}$ is an algebra, we define the problem QCSP($\mathbf{A}$) as follows. An instance of QCSP($\mathbf{A}$) is pair $(\Phi, \mathbb{B})$ where $\mathbb{B}$ is a relational structure preserved by $\mathbf{A}$ and Φ is a qcsp-sentence over the signature of $\mathbb{B}$. The question is to decide whether or not $\mathbb{B} \models \Phi$. When $\mathbf{A}$ is an algebra, the problem CSP($\mathbf{A}$) is defined to be the restriction of QCSP($\mathbf{A}$) to instances $(\Phi, \mathbb{B})$ where Φ is a csp-sentence. Let $\mathbf{A}$ be an algebra, and let $(\exists x_1 \ldots \exists x_n \phi, \mathbb{B})$ be an instance of CSP($\mathbf{A}$); a mapping $f : \{x_1, \ldots, x_n\} \to B$ such that $\mathbb{B}, f \models \phi$ is called a *solution* of the instance. In the case that $\mathbf{A}$ is a semigroup, a solution is called *idempotent* if each element in its image is an idempotent of $\mathbf{A}$. A fact that we will tacitly use is the following.

▶ **Proposition 3.** *When* $\mathbf{S}$ *is a semigroup and* f *and* g *are solutions to an instance of* CSP($\mathbf{S}$)*, the assignment* fg *obtained by point-wise product is also a solution to the instance.*

We define QCSP($\mathbb{B}$) to be the problem of deciding, given a qcsp-sentence Φ over the signature of $\mathbb{B}$, whether or not $\mathbb{B} \models \Phi$; we define CSP($\mathbb{B}$) analogously, but with respect to csp-sentences.

The following is the statement of the classification of finite semigroups with respect to the CSP.

▶ **Theorem 4** ([4]). *Let* $\mathbf{S}$ *be a finite semigroup. If* $\mathbf{S}$ *is a block group, then* CSP($\mathbf{S}$) *is polynomial-time decidable; otherwise,* CSP($\mathbf{S}$) *is* NP*-complete.*

Let us now identify some results on quantified constraint satisfaction of which we will make use.

Let $\mathbf{A} = \langle A, F\rangle$ be an algebra. A *congruence* of $\mathbf{A}$ is an equivalence relation $\theta \subseteq A \times A$ that is preserved by $\mathbf{A}$. Suppose that θ is a congruence of $\mathbf{A}$. Denote the equivalence class of θ containing $a \in A$ by a^θ; then, for each $f \in F$, the operation f^θ given by $f^\theta(a_1^\theta, \ldots, a_k^\theta) = (f(a_1, \ldots, a_k))^\theta$ is well-defined. Define A^θ as $\{a^\theta \mid a \in A\}$ and F^θ as $\{f^\theta \mid f \in F\}$. A *homomorphic image* of $\mathbf{A}$ is an algebra of the form $\langle A^\theta, F^\theta\rangle$, where θ is a congruence of $\mathbf{A}$. The following result seems to have a folklore status in the area, but we are not aware of any proof in the literature, so we provide one here.

▶ **Lemma 5.** *Let* $\mathbf{A}$ *be an algebra, and let* $\mathbf{B}$ *be a homomorphic image of* $\mathbf{A}$*. Then* $\mathrm{QCSP}(\mathbf{B}) \leq_p^m \mathrm{QCSP}(\mathbf{A})$*.*

Proof. Let θ be a congruence of $\mathbf{A}$ such that $\mathbf{B}$ has the form $\langle A^\theta, F^\theta\rangle$. Let h be the mapping from A to B defined by $h(a) = a^\theta$. Let $(\Psi, \mathbb{B})$ be an instance of QCSP($\mathbf{B}$). For each relation $R^{\mathbb{B}}$ of $\mathbb{B}$, let k denote its arity, and define $R^{\mathbb{A}}$ as the relation $\{(a_1, \ldots, a_k) \in A^k \mid (h(a_1), \ldots, h(a_k)) \in R^{\mathbb{B}}\}$. Since the relations of $\mathbb{A}$ are preimages under the homomorphism h of the relations of $\mathbb{B}$, we have that $\mathbb{A}$ is preserved by $\mathbf{A}$. So the reduction outputs the instance $(\Psi, \mathbb{A})$ of QCSP($\mathbf{A}$).

We argue the correctness of this reduction as follows. Let Φ be a formula having the form $Q_1 v_1 \ldots Q_m v_m \phi$, where ϕ is a conjunction of atoms. It is straightforward to verify the following by induction on m: for any assignment g mapping variables to A, it holds that $\mathbb{A}, g \models \Phi$ iff $\mathbb{B}, h(g) \models \Phi$. Here, $h(g)$ denotes the composition of h and g. It follows that, when Φ is a qcsp-sentence, $\mathbb{A} \models \Phi$ iff $\mathbb{B} \models \Phi$. ◀

When $\mathbf{A}$ is an algebra, define $\mathrm{QCSP}_\forall(\mathbf{A})$ to be the restriction of QCSP($\mathbf{A}$) to instances $(\Phi, \mathbb{B})$ where Φ has at most one universally quantified variable.

▶ **Theorem 6** (follows from [7]). *Let* $\mathbf{S}$ *be a finite monoid. There exists a polynomial-time algorithm that, given as input an instance* $(\Phi, \mathbb{B})$ *of the problem* QCSP($\mathbf{S}$)*, outputs a set* $\mathcal{I}$ *of* $\mathrm{QCSP}_\forall(\mathbf{S})$ *instances such that* $(\Phi, \mathbb{B})$ *is a* yes *instance of* QCSP($\mathbf{S}$) *if and only if every instance in* $\mathcal{I}$ *is a* yes *instance of* $\mathrm{QCSP}_\forall(\mathbf{S})$*. Consequently, the problem* QCSP($\mathbf{S}$) *is in* NP*.*

This theorem can be established using Theorem 4.3 of [7]; let us explain how. Let e denote the identity element of the monoid $\mathbf{S}$; by [7, Theorem 4.3] each structure $\mathbb{B}$ that is preserved by a monoid $\mathbf{S}$ of size 2 is (in the language of [7]) $(1, e)$-collapsible. The same proof works for monoids of arbitrary sizes. It follows that deciding an instance of QCSP($\mathbf{S}$) is equivalent to checking if all of its $(1, e)$-collapsings are yes instances (see Definitions 3.1 and 3.11 of [7]), and these can be formulated as instances of $\mathrm{QCSP}_\forall(\mathbf{S})$. Note that the relation $\{e\}$ is preserved by $\mathbf{S}$, and so can be used in an atom to force a variable to take on the value e. Finally we have polynomially many instances of $\mathrm{QCSP}_\forall(\mathbf{S})$, each of which clearly are in NP. Hence QCSP($\mathbf{S}$) is in NP.

3 Dichotomy theorem statement

The following is the main classification result of this paper.

▶ **Theorem 7.** *Let* $\mathbf{S}$ *be a finite monoid.*

- *If* $\mathbf{S}$ *is a block group and generated by its regular elements, then the problem* QCSP($\mathbf{S}$) *is polynomial-time decidable.*
- *Otherwise, the problem* QCSP($\mathbf{S}$) *is* NP*-complete.*

We give a proof that makes forward references to the main theorems of the next two sections, Theorems 8 and 9.

Proof. By Theorem 6, the problem QCSP($\mathbf{S}$) is in NP. When $\mathbf{S}$ is a block group and generated by its regular elements, it follows from Theorem 9 that QCSP($\mathbf{S}$) is polynomial-time decidable. If $\mathbf{S}$ is not a block group, then QCSP($\mathbf{S}$) is NP-hard by Theorem 4; if $\mathbf{S}$ is not generated by its regular elements, then QCSP($\mathbf{S}$) is NP-hard by Theorem 8. ◀

We now describe how some concrete classes of monoids behave with respect to our dichotomy, but first, we need some more definitions. A semigroup is *inverse* if all its elements are regular and its idempotents commute. Hence inverse semigroups are in particular block groups. The prototypical example of an inverse semigroup is the *symmetric inverse semigroup* I_n on the set $\{1, \dots, n\}$ which is formed by all partial one-to-one maps on $\{1, \dots, n\}$ under composition. Partial functions f, g are composed by the standard product $\circ$ for relations: $(x, y) \in f \circ g$ if there exists $z \in \{1, \dots, n\}$ such that $(x, z) \in f$ and $(z, y) \in g$. For $f \in I_n$ let $f^{-1} = \{(y, x) \ : \ (x, y) \in f\}$. Then f is regular by $f \circ f^{-1} \circ f = f$. It is easy to see that the idempotents of I_n are exactly the restrictions of the identity map on $\{1, \dots, n\}$. In particular all idempotents commute. Hence I_n is an inverse semigroup. Since finite inverse semigroups with identity, in particular I_n for $n \in \mathbb{N}$, are block groups with all their elements regular, they have polynomial-time decidable QCSP by Theorem 7.

The *full transformation semigroup* T_n is formed by all (total) transformations on $\{1, \dots, n\}$ under composition. While it is well-known and easy to check that T_n is regular, it is not a block group for $n \geq 2$. To see the latter let e, f be the constant functions on $\{1, \dots, n\}$ with image $1, 2$, respectively. Clearly e, f are idempotent and satisfy $ef = e, fe = f$; but, $e \neq f$. Hence QCSP(T_n) is NP-complete for all $n \geq 2$ by Theorem 7.

We give an easy example of a block group that is not generated by its regular elements: A semigroup $\mathbf{S}$ is a *zero semigroup* if $0 \in S$ and the multiplication is constant, that is $xy = 0$ for all $x, y \in S$. For a zero semigroup $\mathbf{S}$ the monoid $\mathbf{S}^1$ has the idempotents $0, 1$ and is a block group. However if $|S| > 1$, then $\mathbf{S}^1$ is not generated by its regular elements $0, 1$. Hence QCSP($\mathbf{S}^1$) is NP-complete for all zero semigroups $\mathbf{S}$ of size at least 2 by Theorem 7 although CSP($\mathbf{S}^1$) is in P by Theorem 4 of Bulatov, Jeavons, and Volkov. To our knowledge this is the first explicit example of an algebra $\mathbf{S}$ where CSP($\mathbf{S}$) is tractable and QCSP($\mathbf{S}$) is NP-complete.

Finally we give an example of a non-regular block group that is generated by its regular elements. Denote a transformation $f \in T_4$ by its list of images, i.e., $f = [f(1), f(2), f(3), f(4)]$. Let $\mathbf{S}$ be the transformation semigroup generated by $a = [1, 2, 2, 4]$ and $b = [4, 4, 3, 4]$. From $ab = [4, 4, 2, 4]$ and $ba = [4, 4, 4, 4]$ we see that $S = \{a, b, ab, ba\}$. We adjoin an identity to $\mathbf{S}$ to obtain the monoid $\mathbf{S}^1$. Clearly a, b and ba are idempotent, in particular, regular. Hence $\mathbf{S}^1$ is generated by regular elements. However ab is not regular because $abxab = ba$ for any $x \in S^1$. By considering the products of idempotents it is easy to check that $\mathbf{S}^1$ is a block group. Thus QCSP($\mathbf{S}^1$) is polynomial-time decidable by Theorem 7.

4 Hardness

For the hardness part of Theorem 7 we will use the following result that covers a more general setting than monoids.

▶ **Theorem 8.** *Let* $\mathbf{S}$ *be a finite semigroup that is not generated by its regular elements. The problem* QCSP($\mathbf{S}$) *is* NP*-hard. In particular, there exists a structure* $\mathbb{B}'$ *that is preserved by* $\mathbf{S}$ *and which has one* 4*-ary relation such that* QCSP($\mathbb{B}'$) *is NP-complete.*

Proof. Let J_a denote a $\mathcal{J}$-class of $\mathbf{S}$ that is maximal over all $\mathcal{J}$-classes containing an element a that is not generated by the regular elements of $\mathbf{S}$. By Lemma 1 (1), J_a is not the minimal $\mathcal{J}$-class. Then $I := \{x \in S \ : \ J_a \not\leq J_x\}$ is non-empty, and is an ideal of $\mathbf{S}$. Consider the Rees quotient $\mathbf{S}/I$. Since QCSP($\mathbf{S}/I$) $\leq_p^m$ QCSP($\mathbf{S}$) by Lemma 5, it suffices to show that QCSP($\mathbf{S}/I$) is NP-hard. So we pass from $\mathbf{S}$ to $\mathbf{S}/I$ and assume $I = \{0\}$ in the following.

Define $F := \{x \in S \ : \ J_a < J_x\}$. We have that $F \cup J_a \cup \{0\}$ is a partition of S.

By assumption, F is generated by the regular elements of $\mathbf{S}$. In particular, a is not generated by F. We claim that

$$J_a \cap \langle F \rangle = \emptyset. \tag{1}$$

We argue this claim as follows. Suppose $b \in J_a \cap \langle F \rangle$. We have $u, v \in S^1$ such that $a = ubv$. Clearly $u, v \in F$, because $J_a^2 = \{0\}$ by Lemma 1 (1). But then $a = ubv$ is generated by F, which contradicts our assumption. Hence (1) is proved.

Let $\mathbb{B}$ be the relational structure with universe $\{0, 1\}$ and with the single relation $T^{\mathbb{B}} = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)$. The relational structure $\mathbb{B}$ is known to have an NP-hard CSP [22]. We claim that

$$\text{CSP}(\mathbb{B}) \leq_p^m \text{QCSP}(\mathbf{S}). \tag{2}$$

To this end, define the relational structure $\mathbb{B}'$ with universe S as follows. Set $T_b := \{(b, 0, 0), (0, b, 0), (0, 0, b)\}$ for $b \in J_a$ and

$$T'^{\mathbb{B}'} := \{(f, f, f, f) \ : \ f \in F\} \cup (0 \times S \times S \times S) \cup (\bigcup_{b \in J_a} \{b\} \times T_b).$$

By using (1) and the fact that $J_a^2 = \{0\}$, it is straightforward to verify that $T'^{\mathbb{B}'}$ is preserved by $\mathbf{S}$. We prove that CSP($\mathbb{B}$) $\leq_p^m$ QCSP($\mathbb{B}'$), which suffices to give (2).

Given an instance

$$\Phi = \exists x_1 \ldots \exists x_k \phi(x_1, \ldots, x_k) \tag{3}$$

of CSP($\mathbb{B}$) we construct an instance of QCSP($\mathbb{B}'$), as follows. Define

$$\Phi' = \forall y \exists x_1 \ldots \exists x_k \phi'(y, x_1, \ldots, x_k) \tag{4}$$

where ϕ' is obtained from ϕ by replacing every atom $T(x, x', x'')$ in ϕ by $T'(y, x, x', x'')$. The resulting instance of QCSP($\mathbb{B}'$) is Φ'.

Note that, on $\mathbb{B}'$, we have that $\phi'(s, \ldots, s)$ is true for every $s \in S \backslash J_a$. Further, when $b \in J_a$, the 0-1 assignments $f : \{x_1, \ldots, x_k\} \to \{0, 1\}$ such that $\mathbb{B}, f \models \phi(x_1, \ldots, x_k)$ correspond exactly to the 0-b assignments $f' : \{x_1, \ldots, x_k\} \to \{0, b\}$ such that $\mathbb{B}', f' \models \phi'(b, x_1, \ldots, x_k)$. Thus $\mathbb{B} \models \Phi$ if and only if $\mathbb{B}' \models \Phi'$. Hence we have (2) and that QCSP($\mathbf{S}$) is NP-hard. ◀

5 Tractability

In this section, we establish the following theorem.

▶ **Theorem 9.** *Let* $\mathbf{S}$ *be a finite monoid that is a block group and generated by its regular elements. Then* QCSP($\mathbf{S}$) *is in* P.

When $\mathbf{S}$ is a semigroup, we order assignments using the order of $\mathcal{J}$-classes of $\mathbf{S}$ as follows. Let $f, g : V \to S$ be assignments defined on the same set V of variables. We write $f \leq_{\mathcal{J}} g$ iff for all $v \in V$, it holds that $J_{f(v)} \leq J_{g(v)}$. Also, for $\mathcal{T} \in \{\mathcal{R}, \mathcal{L}\}$ we write $f \equiv_{\mathcal{T}} g$ iff for all $v \in V$, it holds that $T_{f(v)} = T_{g(v)}$.

▶ **Lemma 10** (follows from [4]). *Let* $\mathbf{S}$ *be a finite block group. There exists a polynomial-time algorithm that, when given as input an instance* $(\exists x_1 \ldots \exists x_k \phi, \mathbb{B})$ *of* CSP($\mathbf{S}$)*, either correctly reports that there is no solution, or outputs an idempotent solution* g *such that for any solution* h *of the instance:*

- *It holds that* $g \leq_{\mathcal{J}} h$.
- *If* h *is idempotent and* $h \leq_{\mathcal{J}} g$*, then* $h = g$.

That is, the solution is $\mathcal{J}$*-minimal, and is also the unique* $\mathcal{J}$*-minimal assignment among idempotent assignments.*

Although this lemma follows from [4], we give a proof for the sake of completeness.

Proof. Let $n := |S|$. The algorithm does the following: first, it runs *arc consistency*; see [10] for a description of this algorithm. In the case that arc consistency reports *no*, the algorithm reports no; otherwise, arc consistency returns sets $A_1, \ldots, A_k \subseteq S$, one for each variable $x_1, \ldots, x_k$. In this latter case, it is well-known and straightforward to verify that

1. when the instance is an instance of CSP($\mathbf{A}$), each set A_i is the universe of a subalgebra of $\mathbf{A}$;
2. for any solution $f : \{x_1, \ldots, x_k\} \to S$, it holds that $f(x_i) \in A_i$ (for each i); and,
3. for each atom $R(x_{i_1}, \ldots, x_{i_\ell})$ of ϕ, there exists a set of tuples $U \subseteq R^{\mathbb{B}}$ such that $(A_{i_1}, \ldots, A_{i_\ell}) = (\pi_1(U), \ldots, \pi_\ell(U))$, where π_j is the projection onto the jth coordinate.

Let $m \geq 1$ be a natural number. As shown in [4], as $\mathbf{S}$ is a block group, the value of $(y_1^{n!} \cdots y_m^{n!})^{n!}$ depends only on the set $\{y_1, \ldots, y_m\} \subseteq S$. Let $t : \wp(S) \setminus \{\emptyset\} \to S$ denote the map sending a non-empty set $\{y_1, \ldots, y_m\}$ to the value $(y_1^{n!} \cdots y_m^{n!})^{n!}$. The algorithm outputs the mapping $g : \{x_1, \ldots, x_k\} \to S$ given by $g(x_i) = t(A_i)$. It can be verified from item (3) that this mapping g is a solution.

Let h be any solution of the instance, and let $i \leq k$. By property (2), since $t(A_i)$ is defined as a product that involves all elements in A_i, we have that $g(x_i)$ is an element of the unique minimal $\mathcal{J}$-class of $\mathbf{S}$ that intersects A_i non-trivially and hence $J_{g(x_i)} \leq J_{h(x_i)}$. Consequently, it holds that $g \leq_{\mathcal{J}} h$. For the second claim, it suffices to show that $J_{g(x_i)} \cap A_i$ only contains one idempotent. Since $\mathbf{S}$ is a block group, the product of any pair of distinct idempotents from a $\mathcal{J}$-class lies outside of that $\mathcal{J}$-class, by Lemma 2. So, if $J_{g(x_i)} \cap A_i$ contained two distinct idempotents, their product would be an element of A_i (by property (1)) in a strictly lower $\mathcal{J}$-class of $\mathbf{S}$, a contradiction to the minimality of the $\mathcal{J}$-class $J_{g(x_i)}$ in A_i. ◀

For the rest of the section, we assume that $\mathbf{S}$ *is a finite monoid that is a block group.* We also assume that $|S| > 1$; note that Theorem 9 holds trivially in the case that $|S| = 1$. In the following, when presenting instances of CSP($\mathbf{S}$) and QCSP($\mathbf{S}$), we permit the use of atoms of the form $v = a$, where v is a variable and a is an idempotent element of $\mathbf{S}$; this is

justified by the fact that, when a is an idempotent element, the relation $\{a\}$ is preserved by the semigroup $\mathbf{S}$.

▶ **Lemma 11.** *There exists a polynomial-time algorithm that, given an instance of* $\mathrm{QCSP}_\forall(\mathbf{S})$ *having exactly one universal quantifier, computes a decision-equivalent instance of* $\mathrm{QCSP}_\forall(\mathbf{S})$ *whose sentence has the form* $\forall y \exists w_1 \dots \exists w_m \phi$*, that is, having exactly one universal quantifier that appears before the existential quantifiers.*

Proof. Let $(\Phi, \mathbb{B})$ be an instance of $\mathrm{QCSP}_\forall(\mathbf{S})$ where Φ has the form

$$\exists x_1 \dots \exists x_k \forall y \exists z_1 \dots \exists z_\ell \phi(x_1, \dots, x_k, y, z_1, \dots, z_\ell).$$

Let $T \subseteq S$. We say that a mapping $f\colon \{x_1, \dots, x_k\} \to S$ *tolerates* T if for any extension $f' : \{x_1, \dots, x_k, y\} \to S$ of f where $f'(y) \in T$, it holds that $\mathbb{B}, f' \models \exists z_1 \dots \exists z_\ell \phi$. Note that there exists an assignment that tolerates all of S if and only if $(\Phi, \mathbb{B})$ is a *yes* instance of $\mathrm{QCSP}_\forall(\mathbf{S})$. Also, note that when this condition holds, the $\mathrm{CSP}(S)$ instance $(\Phi_1, \mathbb{B})$, where

$$\Phi_1 = \exists x_1 \dots \exists x_k \exists y \exists z_1 \dots \exists z_\ell (y = 1 \wedge \phi),$$

is a *yes* instance.

The algorithm does the following. It applies the algorithm of Lemma 10 to the $\mathrm{CSP}(\mathbf{S})$ instance $(\Phi_1, \mathbb{B})$; if the result is *no*, then a *no* instance of $\mathrm{QCSP}_\forall(\mathbf{S})$ having the desired form is output. Otherwise, let h' be the resulting solution for $(\Phi_1, \mathbb{B})$, and define h to be the restriction of h' to $\{x_1, \dots, x_k\}$; the algorithm outputs the $\mathrm{QCSP}_\forall(\mathbf{S})$ instance

$$(\forall y \exists x_1 \dots \exists x_k \exists z_1 \dots \exists z_\ell (x_1 = h(x_1) \wedge \dots \wedge x_k = h(x_k) \wedge \phi), \mathbb{B}).$$

Observe that this instance is decision-equivalent to the instance

$$(\exists x_1 \dots \exists x_k \forall y \exists z_1 \dots \exists z_\ell (x_1 = h(x_1) \wedge \dots \wedge x_k = h(x_k) \wedge \phi), \mathbb{B}).$$

We argue the correctness of the algorithm by proving that, if there exists an assignment $f : \{x_1, \dots, x_k\} \to S$ that tolerates S, then the assignment h tolerates S. As f tolerates S, there exists an extension $f' : \{x_1, \dots, x_k, y, z_1, \dots, z_\ell\} \to S$ such that $f'(y) = 1$ and such that f' is a solution to the $\mathrm{CSP}(\mathbf{S})$ instance $(\Phi_1, \mathbb{B})$. We obtain that $i' = (f'h')^{|S|!}$ is also a solution to $(\Phi_1, \mathbb{B})$, where here the product is defined point-wise. As i' is an idempotent solution and has $i' \leq_\mathcal{J} h'$, we have $i' = h'$. Letting i denote the restriction of i' to $\{x_1, \dots, x_k\}$, we then have $i = h$. Since f tolerates S and h tolerates $\{1\}$, we have that fh and hence $h = i = (fh)^{|S|!}$ tolerates S. ◀

Theorem 6 and the just-established lemma allow us to restrict attention to the case of $\mathrm{QCSP}(\mathbf{S})$ where there is just one universally quantified variable, and this variable is the first (left-most) variable to appear in the quantifier prefix. We now establish two lemmas that will aid us in reasoning about such instances. Before doing so, however, we establish some terminology. Let $(\Phi = \exists y \exists z_1 \dots \exists z_\ell \phi(y, z_1, \dots, z_\ell), \mathbb{B})$ be an instance of $\mathrm{CSP}(\mathbf{S})$. Relative to such an instance, let us call an assignment $g : \{z_1, \dots, z_\ell\} \to S$ an *extension* of an element $s \in S$ if, when one takes the assignment sending the first variable y to s and extends by g, the result is a solution. When $e \in S$ is an idempotent and the algorithm of Lemma 10 returns a solution on the instance $(\exists y \exists z_1 \dots \exists z_\ell (y = e \wedge \phi), \mathbb{B})$ of $\mathrm{CSP}(\mathbf{S})$, we refer to the restriction of this solution to $\{z_1, \dots, z_\ell\}$ as the *canonical extension* of e.

▶ **Lemma 12.** *Let* $(\Phi = \exists y \exists z_1 \dots \exists z_\ell \phi(y, z_1, \dots, z_\ell), \mathbb{B})$ *be an instance of* $\mathrm{CSP}(\mathbf{S})$*. Suppose that each element of* S *has an extension, and let* $a \in S$ *be regular. By Lemma 2, there are uniquely determined idempotents* $e \in R_a, f \in L_a$*; let* g_e*,* g_f *denote their canonical extensions. Then* a *has an extension* g_a *such that* $g_e \equiv_\mathcal{R} g_a \equiv_\mathcal{L} g_f$*.*

Proof. By assumption a has some extension h. Since $eaf = a$, by Lemma 2, $g_a := g_e h g_f$ is also an extension of a with $g_a \leq_{\mathcal{J}} g_e$ and $g_a \leq_{\mathcal{J}} g_f$. Since a and e are $\mathcal{R}$-related, there exists an element $b \in J_a$ with $ab = e$. Let i be an extension of b. Then $(g_a i)^{n!}$ is an idempotent extension of e with $(g_a i)^{n!} \leq_{\mathcal{J}} g_e$. Since g_e is the unique $\mathcal{J}$-minimal extension of e by assumption, it follows that $(g_a i)^{n!} = g_e$. Together with $g_a = g_e h g_f$ this yields $g_a \equiv_{\mathcal{R}} g_e$. Similarly we obtain $g_a \equiv_{\mathcal{L}} g_f$. Thus the lemma is proved. ◀

▶ **Lemma 13.** *There exists a polynomial-time algorithm that, given a regular element $a \in S$, and an instance $(\Phi = \exists y \exists z_1 \ldots \exists z_\ell \phi(y, z_1, \ldots, z_\ell), \mathbb{B})$ of $\mathrm{CSP}(\mathbf{S})$, either reports that a has an extension, or that there exists an element without an extension.*

Proof. Let us assume that every element has an extension. Let e, f be the idempotents described in the statement of Lemma 12. For every $u \in \{1, \ldots, \ell\}$, it holds that the elements $g_e(z_u), g_f(z_u), g_a(z_u)$ are contained in the same $\mathcal{J}$-class, say, J_u. Since $\mathbf{S}$ is a block group and J_u contains a regular element (even an idempotent), by Lemma 2 we can identify J_u with $\{(i, g, j) \ : \ i, j \in I_u, g \in G_u\}$ for some index set I_u and some group $\mathbf{G}_u$. Since $g_e(z_u), g_f(z_u)$ are idempotent, they are of the form $(i_u, 1, i_u), (j_u, 1, j_u)$, respectively, for $i_u, j_u \in I$ and 1 the identity of $\mathbf{G}_u$. By Lemma 12, we have $g_u \in G_u$ such that $g_a(z_u) = (i_u, g_u, j_u)$.

Let $b \in J_a$ be such that $ab = e$. By Lemma 12, b has an extension such that $g_a g_b = g_e$, implying $g_b(z_u) = (j_u, g_u^{-1}, i_u)$. Thus we have that

$$\phi(a, (i_1, g_1, j_1), \ldots, (i_\ell, g_\ell, j_\ell)) \wedge \phi(b, (j_1, g_1^{-1}, i_1), \ldots, (j_\ell, g_\ell^{-1}, i_\ell)) \tag{5}$$

holds on $\mathbb{B}$.

We argued that if every element has an extension, then there exist elements $g_1, \ldots, g_\ell$ satisfying (5). The algorithm claimed in the lemma thus does the following. It checks to see if e and f have extensions (using Lemma 10); if not, it reports that there exists an element without an extension. Otherwise, let g_e, g_f be the canonical extensions of e and f, respectively, and let b be as described. The groups $\mathbf{G}_1, \ldots, \mathbf{G}_\ell$ and the indices $i_1, \ldots, i_\ell, j_1, \ldots, j_\ell$ are uniquely determined by g_e and g_f.

We will argue that determining the existence of elements $g_1, \ldots, g_\ell$ as in (5) is a CSP over a coset generating operation, i.e., its relations are closed under the operation $xy^{-1}z$. This CSP can be solved in polynomial time by Theorem 33 of [13], in particular, by using the known fact (which is straightforwardly verified) that a relation closed under the operation $xy^{-1}z$ of a group is a coset of a subgroup of the group. (Note that Theorem 33 of [13] deals with a single group $\mathbf{G}$; it can be employed for our purposes here by simply taking $\mathbf{G}$ to be the product of all groups $\mathbf{G}_i$ that may arise, and then identifying an element g of a group $\mathbf{G}_i$ with the element of $\mathbf{G}$ equal to g at the coordinate corresponding to $\mathbf{G}_i$, and as equal to the identity element of the respective group everywhere else.) This argument will thus conclude the proof of the Lemma; if such elements $g_1, \ldots, g_\ell$ exist, then a has an extension, otherwise some element does not have an extension.

Let ψ be an arbitrary constraint of ϕ, and assume that, for $u \in \{1, \ldots, \ell\}$, it holds that $r_u, s_u, t_u \in G_u$ are such that, on $\mathbb{B}$, the following hold:

$$\psi(a, (i_1, r_1, j_1), \ldots, (i_\ell, r_\ell, j_\ell)), \psi(a, (i_1, s_1, j_1), \ldots, (i_\ell, s_\ell, j_\ell)), \psi(a, (i_1, t_1, j_1), \ldots, (i_\ell, t_\ell, j_\ell)).$$

It follows that, on $\mathbb{B}$, the following hold:

$$\psi(a, (i_1, r_1, j_1), \ldots, (i_\ell, r_\ell, j_\ell)), \psi(b, (j_1, s_1^{-1}, i_1), \ldots, (j_\ell, s_\ell^{-1}, i_\ell)), \psi(a, (i_1, t_1, j_1), \ldots, (i_\ell, t_\ell, j_\ell)).$$

Since ψ is preserved by the semigroup multiplication and $aba = a$ by Lemma 2 (3), we obtain that

$$\psi(a, (i_1, r_1 s_1^{-1} t_1, j_1), \ldots, (i_\ell, r_\ell s_\ell^{-1} t_\ell, j_\ell))$$

holds on $\mathbb{B}$. Similarly, we have $bab = b$ which yields that

$$\psi(b, (i_1, t_1^{-1}s_1r_1^{-1}, j_1), \ldots, (i_\ell, t_\ell^{-1}s_\ell r_\ell^{-1}, j_\ell))$$

holds on $\mathbb{B}$. So the induced constraints are closed under $xy^{-1}z$. ◀

Proof of Theorem 9. Let $\mathbf{S}$ be a monoid that is a block group and generated by its regular elements. We have that CSP($\mathbf{S}$) is polynomial-time decidable by Theorem 4. Thus, by Theorem 6 and Lemma 11, it suffices to prove polynomial-time decidability of the restriction of QCSP$_\forall$($\mathbf{S}$) to instances with exactly one universal quantifier that appears before the existential quantifiers. Let $I = (\Psi = \forall y \exists z_1 \ldots \exists z_\ell \phi, \mathbb{B})$ be such an instance, and define I' to be the instance $(\Phi = \exists y \exists z_1 \ldots \exists z_\ell \phi, \mathbb{B})$ of CSP($\mathbf{S}$). The algorithm first checks that each idempotent has an extension with respect to I'; if this is not the case, the algorithm returns *no*. Since $\mathbf{S}$ is generated by its regular elements, I is a *yes* instance if and only if each regular element $a \in S$ has an extension with respect to I' (recall Proposition 3). Checking the latter condition can be done by looping over each regular element $a \in S$ and invoking the algorithm of Lemma 13. ◀

6 Conclusion

We investigated the complexity of quantified constraint satisfaction problems from monoids. While QCSP($\mathbb{B}$) for an arbitrary relational structure may be PSPACE-complete, QCSP($\mathbf{S}$) for a monoid $\mathbf{S}$ is always in NP. In our main result Theorem 7 we established a dichotomy between tractable and NP-complete QCSP for all finite monoids via some simple algebraic conditions. Note for any semilattice $\mathbf{S}$ without unit Börner et al showed that QCSP($\mathbf{S}$) is PSPACE-complete [2, Theorem 6.1]. A complete characterization of the complexity of QCSP for all semigroups remains open.

Combining the results of [4, 2] and the present paper we can compare the complexity of constraint satisfaction and quantified constraint satisfaction for the same fixed semigroup $\mathbf{S}$. We observe the following behavior:

1. **a.** CSP($\mathbf{S}$) in P and QCSP($\mathbf{S}$) in P if $\mathbf{S}$ is a block group, a monoid and generated by its regular elements;
   b. CSP($\mathbf{S}$) in P and QCSP($\mathbf{S}$) is NP-complete if $\mathbf{S}$ is a block group, a monoid and not generated by its regular elements;
   c. CSP($\mathbf{S}$) in P and QCSP($\mathbf{S}$) is PSPACE-complete if $\mathbf{S}$ is a semilattice without 1;
2. **b.** CSP($\mathbf{S}$) is NP-complete and QCSP($\mathbf{S}$) is NP-complete if $\mathbf{S}$ is not a block group but a monoid;
   c. CSP($\mathbf{S}$) is NP-complete and QCSP($\mathbf{S}$) is PSPACE-complete if $\mathbf{S}$ is not a block group but has a semilattice without 1 as homomorphic image.

The case (2a) that CSP($\mathbf{S}$) is NP-complete and QCSP($\mathbf{S}$) is in P cannot occur and is omitted. The cases above can be attained by concrete monoids given in Section 3 except for examples witnessing PSPACE-completeness. Note that clearly (1c) occurs because semilattices without 1 exist. For (2c) we consider an idempotent semigroup $\mathbf{S}$ with elements a, b, e, f such that

$$a^2 = a, ax = e \text{ for all } x \neq a,$$
$$b^2 = b, bx = f \text{ for all } x \neq b,$$
$$ex = e, fx = f \text{ for all } x \in S.$$

Then $ef = e \neq f = fe$ implies that $\mathbf{S}$ is not a block group. Further $I = \{e, f\}$ is an ideal with quotient $\mathbf{S}/I$ isomorphic to a 3-element semilattice without 1. Thus $\mathbf{S}$ witnesses case (2c).

References

1 Libor Barto and Marcin Kozik. Constraint satisfaction problems solvable by local consistency methods. *J. ACM*, 61(1):Art. 3, 19, 2014. doi:10.1145/2556646.

2 Ferdinand Börner, Andrei A. Bulatov, Hubie Chen, Peter Jeavons, and Andrei A. Krokhin. The complexity of constraint satisfaction games and QCSP. *Inform. and Comput.*, 207(9):923–944, 2009. doi:10.1016/j.ic.2009.05.003.

3 Andrei Bulatov, Peter Jeavons, and Andrei Krokhin. Classifying the complexity of constraints using finite algebras. *SIAM J. Comput.*, 34(3):720–742, 2005. doi:10.1137/S0097539700376676.

4 Andrei Bulatov, Peter Jeavons, and Mikhail Volkov. Finite semigroups imposing tractable constraints. In *Semigroups, algorithms, automata and languages (Coimbra, 2001)*, pages 313–329. World Sci. Publ., River Edge, NJ, 2002. doi:10.1142/9789812776884_0011.

5 Andrei A. Bulatov. A dichotomy theorem for constraint satisfaction problems on a 3-element set. *J. ACM*, 53(1):66–120, 2006. doi:10.1145/1120582.1120584.

6 Catarina Carvalho, Florent R. Madelaine, and Barnaby Martin. From complexity to algebra and back: Digraph classes, collapsibility, and the PGP. In *30th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2015, Kyoto, Japan, July 6-10, 2015*, pages 462–474, 2015.

7 Hubie Chen. The complexity of quantified constraint satisfaction: collapsibility, sink algebras, and the three-element case. *SIAM J. Comput.*, 37(5):1674–1701, 2008. doi:10.1137/060668572.

8 Hubie Chen. Quantified constraint satisfaction and the polynomially generated powers property. *Algebra Universalis*, 65(3):213–241, 2011. doi:10.1007/s00012-011-0125-4.

9 Hubie Chen. Meditations on quantified constraint satisfaction. In *Logic and program semantics*, volume 7230 of *Lecture Notes in Comput. Sci.*, pages 35–49. Springer, Heidelberg, 2012. doi:10.1007/978-3-642-29485-3_4.

10 Hubie Chen, Victor Dalmau, and Berit Grußien. Arc consistency and friends. *J. Logic Comput.*, 23(1):87–108, 2013. doi:10.1093/logcom/exr039.

11 Hubie Chen, Florent Madelaine, and Barnaby Martin. Quantified constraints and containment problems. *Log. Methods Comput. Sci.*, 11(3):3:9, 28, 2015.

12 Nadia Creignou, Sanjeev Khanna, and Madhu Sudan. *Complexity classifications of Boolean constraint satisfaction problems*. SIAM Monographs on Discrete Mathematics and Applications. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2001. doi:10.1137/1.9780898718546.

13 Tomás Feder and Moshe Y. Vardi. The computational structure of monotone monadic SNP and constraint satisfaction: a study through Datalog and group theory. *SIAM J. Comput.*, 28(1):57–104 (electronic), 1999. doi:10.1137/S0097539794266766.

14 Pavol Hell and Jaroslav Nešetřil. On the complexity of H-coloring. *J. Combin. Theory Ser. B*, 48(1):92–110, 1990. doi:10.1016/0095-8956(90)90132-J.

15 John M. Howie. *Fundamentals of semigroup theory*, volume 12 of *London Mathematical Society Monographs. New Series*. The Clarendon Press, Oxford University Press, New York, 1995. Oxford Science Publications.

16 Paweł Idziak, Petar Marković, Ralph McKenzie, Matthew Valeriote, and Ross Willard. Tractability and learnability arising from algebras with few subpowers. *SIAM J. Comput.*, 39(7):3023–3037, 2010. doi:10.1137/090775646.

17 Florent Madelaine and Barnaby Martin. QCSP on partially reflexive cycles – the wavy line of tractability. In *Computer science – theory and applications*, volume 7913 of *Lecture Notes in Comput. Sci.*, pages 322–333. Springer, Heidelberg, 2013. doi:10.1007/978-3-642-38536-0_28.

18 Florent R. Madelaine and Barnaby Martin. On the complexity of the model checking problem. *CoRR*, abs/1210.6893, 2012.

19 Barnaby Martin. QCSP on partially reflexive forests. In *Principles and Practice of Constraint Programming – CP 2011 – 17th International Conference, CP 2011, Perugia, Italy, September 12-16, 2011. Proceedings*, pages 546–560, 2011.

20 Barnaby Martin and Florent Madelaine. Towards a trichotomy for quantified H-coloring. In *Logical Approaches to Computational Barriers, Second Conference on Computability in Europe (CiE)*, pages 342–352, 2006.

21 Peter Mayr. On finitely related semigroups. *Semigroup Forum*, 86(3):613–633, 2013. doi:10.1007/s00233-012-9455-6.

22 Thomas J. Schaefer. The complexity of satisfiability problems. In *Conference Record of the Tenth Annual ACM Symposium on Theory of Computing (San Diego, Calif., 1978)*, pages 216–226. ACM, New York, 1978.