Complexity of quantified constraint satisfaction on monoids

Peter Mayr

CU Boulder

Joint work with Hubie Chen

Mathematics
UNIVERSITY OF COLORADO **BOULDER**

The quantified constraint satisfaction problem (QCSP)

QCSP: decide if $\mathbf{B} \models \Phi$

where

- $\mathbf{B}$ finite relational structure of finite signature
- $\Phi = Q_1 x_1 \dots Q_n x_n \bigwedge$ atomic formulas over $\mathbf{B}$
- each $Q_i \in \{\forall, \exists\}$, both quantifiers allowed

The quantified constraint satisfaction problem (QCSP)

QCSP: decide if $\mathbf{B} \models \Phi$

where

- $\mathbf{B}$ finite relational structure of finite signature
- $\Phi = Q_1 x_1 \dots Q_n x_n \bigwedge$ atomic formulas over $\mathbf{B}$
- each $Q_i \in \{\forall, \exists\}$, both quantifiers allowed

Example

Quantified Boolean Formulas (QBF):

- $\mathbf{B} = (\{0, 1\}, \text{clauses with 3 literals})$
- $\Phi = \exists x_1 \forall y_1 \exists x_2 \forall y_2 : (x_1 \vee y_1 \vee y_2') \wedge (x_2' \vee y_1' \vee y_2) \wedge \dots$

The quantified constraint satisfaction problem (QCSP)

QCSP: decide if $\mathbf{B} \models \Phi$

where

- $\mathbf{B}$ finite relational structure of finite signature
- $\Phi = Q_1 x_1 \dots Q_n x_n \; \bigwedge$ atomic formulas over $\mathbf{B}$
- each $Q_i \in \{\forall, \exists\}$, both quantifiers allowed

Example

Quantified Boolean Formulas (QBF):

- $\mathbf{B} = (\{0,1\}$, clauses with 3 literals$)$
- $\Phi = \exists x_1 \forall y_1 \exists x_2 \forall y_2 : (x_1 \vee y_1 \vee y_2') \wedge (x_2' \vee y_1' \vee y_2) \wedge \dots$

QCSP is PSPACE-complete.

Fixed template QCSP

QCSP($\mathbb{B}$), restricted version for fixed finite algebra $\mathbb{B}$:

Input: $(\mathbf{B}, \Phi)$ where $\mathbf{B}, \mathbb{B}$ have the same universe, $\mathbf{B}$ has finitely many relations, all closed under operations of $\mathbb{B}$

Problem: $\mathbf{B} \models \Phi$?

Fixed template QCSP

QCSP($\mathbb{B}$), restricted version for fixed finite algebra $\mathbb{B}$:

Input:	$(\mathbf{B}, \Phi)$ where $\mathbf{B}, \mathbb{B}$ have the same universe, $\mathbf{B}$ has finitely many relations, all closed under operations of $\mathbb{B}$
Problem:	$\mathbf{B} \models \Phi$?

1. Examples of $\mathrm{QCSP}(\mathbb{B})$ are in P, NP-complete, PSPACE-complete.
2. Complexity classification of $\mathrm{QCSP}(\mathbb{B})$ is not known to reduce to
   - dichotomy for CSP($\mathbb{B}$),
   - idempotent algebras $\mathbb{B}$.

Fixed template QCSP

QCSP($\mathbb{B}$), restricted version for fixed finite algebra $\mathbb{B}$:

Input: $(\mathbf{B}, \Phi)$ where $\mathbf{B}, \mathbb{B}$ have the same universe,
$\mathbf{B}$ has finitely many relations, all closed under operations of $\mathbb{B}$

Problem: $\mathbf{B} \models \Phi$?

1. Examples of $\mathrm{QCSP}(\mathbb{B})$ are in P, NP-complete, PSPACE-complete.
2. Complexity classification of $\mathrm{QCSP}(\mathbb{B})$ is not known to reduce to
   - dichotomy for CSP($\mathbb{B}$),
   - idempotent algebras $\mathbb{B}$.

Our goal

Study QCSP for non-idempotent algebras, in particular, semigroups.

CSP on semigroups

Theorem (Bulatov, Jeavons, Volkov, 2001)

Let $S = (S, \cdot)$ be a finite semigroup.

1. If S is a block group, then $\mathrm{CSP}(S)$ is in P.
2. Else $\mathrm{CSP}(S)$ is NP-complete.

S is a **block group** if for all idempotents $e, f \in S$

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

QCSP on semigroups

Theorem (Chen, M, CSL 2016)

Let S be a finite monoid.

- If S is a block group and generated by its regular elements, then $\mathrm{QCSP}(S)$ is in P.
- Else $\mathrm{QCSP}(S)$ is NP-complete.

$a \in S$ is **regular** if $\exists b \in S \colon aba = a$.

QCSP on semigroups

Theorem (Chen, M, CSL 2016)

Let S be a finite monoid.

- If S is a block group and generated by its regular elements, then $\mathrm{QCSP}(S)$ is in P.
- Else $\mathrm{QCSP}(S)$ is NP-complete.

$a \in S$ is **regular** if $\exists b \in S \colon aba = a$.

Theorem (Chen, M)

Let S be a finite semigroup without 1 such that

1. S is commutative or
2. S is completely regular.

Then $\mathrm{QCSP}(S)$ is PSPACE-complete.

From tractable CSP to NP-complete QCSP

Example

$S\ldots$ a zero semigroup with 1 adjoined

$\cdot$	0	a	1
0	0	0	0
a	0	0	a
1	0	a	1

1. $\mathrm{CSP}(S)$ is in P.
2. $\mathrm{QCSP}(S)$ is NP-complete.

Proof: NP-hardness

Recall: If S is not a block group, then $\mathrm{CSP}(S)$ is NP-hard (Bulatov, Jeavons, Volkov, 2001).

Lemma (Chen, M, 2016)

If a semigroup S is not generated by its regular elements, then $\mathrm{QCSP}(S)$ is NP-hard.

Proof: NP-hardness

Recall: If S is not a block group, then $\mathrm{CSP}(S)$ is NP-hard (Bulatov, Jeavons, Volkov, 2001).

Lemma (Chen, M, 2016)

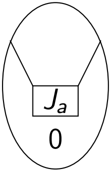
If a semigroup S is not generated by its regular elements, then $\mathrm{QCSP}(S)$ is NP-hard.

Proof.

S has homomorphic image $\bar{S} := S/0$:

$a \in S$ ... maximal with respect to $\leq_{\mathcal{J}}$, not generated by regulars

0 ... elements $\not\geq_{\mathcal{J}} a$



Proof: NP-hardness

Recall: If S is not a block group, then $\mathrm{CSP}(S)$ is NP-hard (Bulatov, Jeavons, Volkov, 2001).

Lemma (Chen, M, 2016)

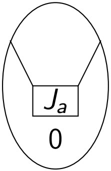
If a semigroup S is not generated by its regular elements, then $\mathrm{QCSP}(S)$ is NP-hard.

Proof.

S has homomorphic image $\bar{S} := S/0$:

$a \in S$ ... maximal with respect to $\leq_{\mathcal{J}}$, not generated by regulars

0 ... elements $\not\geq_{\mathcal{J}} a$



Encode 1-in-3 SAT (NP-hard) into $\mathrm{QCSP}(\bar{S})$. □

Homomorphic images

Easy fact

For $\theta \in \mathrm{Con}(\mathbb{B})$, $\mathrm{QCSP}(\mathbb{B}/\theta)$ has polytime reduction to $\mathrm{QCSP}(\mathbb{B})$.

Proof: NP

Lemma (Chen, 2008)

For any monoid S, $\mathrm{QCSP}(S)$ is in NP.

Proof: NP

Lemma (Chen, 2008)

For any monoid S, $\mathrm{QCSP}(S)$ is in NP.

Proof.

Instances for monoids are **collapsible**:

$$\forall y_1 \exists x_1 \dots \forall y_n \exists x_n \colon \phi(x_1, \dots, x_n, y_1, \dots, y_n)$$

iff for every $i \leq n$:

$$\exists x_1 \dots \exists x_{i-1} \forall y_i \exists x_i \dots \exists x_n \colon \phi(x_1, \dots, x_n, 1, \dots, 1, y_i, 1 \dots, 1).$$

Proof: NP

Lemma (Chen, 2008)

For any monoid S, $\mathrm{QCSP}(S)$ is in NP.

Proof.

Instances for monoids are **collapsible**:

$$\forall y_1 \exists x_1 \dots \forall y_n \exists x_n \colon \phi(x_1, \dots, x_n, y_1, \dots, y_n)$$

iff for every $i \leq n$:

$$\exists x_1 \dots \exists x_{i-1} \forall y_i \exists x_i \dots \exists x_n \colon \phi(x_1, \dots, x_n, 1, \dots, 1, y_i, 1 \dots, 1).$$

The latter yields $n|S|$ CSP-instances in the relational language expanded by constants. □

Proof: tractability

Lemma (Chen, M, 2016)

Let S be a block group with 1 that is generated by its regular elements. Then $\mathrm{QCSP}(S)$ is in P.

Proof.

1. Collapsibility reduces any instance to several with single $\forall$-quantifier:

$$\exists x_1 \dots x_m \forall y \exists z_1 \dots z_n \colon \phi(x_1 \dots x_m, y, z_1 \dots z_n)$$

Proof: tractability

Lemma (Chen, M, 2016)

Let S be a block group with 1 that is generated by its regular elements. Then $\mathrm{QCSP}(S)$ is in P.

Proof.

1. Collapsibility reduces any instance to several with single $\forall$-quantifier:

$$\exists x_1 \dots x_m \forall y \exists z_1 \dots z_n \colon \phi(x_1 \dots x_m, y, z_1 \dots z_n)$$

2. By CSP-algorithm find idempotents $e_1 \dots e_m, f_1 \dots f_n \in S$ such that

$$\phi(e_1 \dots e_m, 1, f_1 \dots f_n)$$

Proof: tractability

Lemma (Chen, M, 2016)

Let S be a block group with 1 that is generated by its regular elements. Then $\mathrm{QCSP}(S)$ is in P.

Proof.

1. Collapsibility reduces any instance to several with single $\forall$-quantifier:

$$\exists x_1 \dots x_m \forall y \exists z_1 \dots z_n \colon \phi(x_1 \dots x_m, y, z_1 \dots z_n)$$

2. By CSP-algorithm find idempotents $e_1 \dots e_m, f_1 \dots f_n \in S$ such that

$$\phi(e_1 \dots e_m, 1, f_1 \dots f_n)$$

3. Reduce further to a sentence starting with $\forall$:

$$\forall y \exists z_1 \dots z_n \colon \phi(e_1 \dots e_m, y, z_1 \dots z_n)$$

4. Given a $\mathrm{QCSP}(S)$-instance

$$\forall y \exists z_1 \dots \exists z_n \; \psi(y, z_1, \dots, z_n), \tag{1}$$

for any regular $a \in S$, deciding

$$\exists z_1 \dots \exists z_n \; \psi(a, z_1, \dots, z_n) \tag{2}$$

is in P.
Not possible for arbitrary $y = a$ but a combination of CSP-algorithms for block groups and idempotent group reducts works for regular a.

4. Given a $\mathrm{QCSP}(S)$-instance

$$\forall y \exists z_1 \dots \exists z_n \; \psi(y, z_1, \dots, z_n), \tag{1}$$

for any regular $a \in S$, deciding

$$\exists z_1 \dots \exists z_n \; \psi(a, z_1, \dots, z_n) \tag{2}$$

is in P.
Not possible for arbitrary $y = a$ but a combination of CSP-algorithms for block groups and idempotent group reducts works for regular a.

5. Since S is generated by regular elements and ψ is invariant under $\cdot$, (2) suffices for (1). □

A bigger picture

Fact (Wiegold)

Sizes of generating sets for S^n are ...

1. at most **polynomial** in n for finite monoids S (**PGP**);
2. at least **exponential** in n for semigroups S without 1 (**EGP**).

A bigger picture

Fact (Wiegold)

Sizes of generating sets for S^n are ...

1. at most **polynomial** in n for finite monoids S (**PGP**);
2. at least **exponential** in n for semigroups S without 1 (**EGP**).

Theorem (Zhuk, 2015)

Every finite algebra either has the PGP or EGP.

A bigger picture

Fact (Wiegold)

Sizes of generating sets for S^n are ...

1. at most **polynomial** in n for finite monoids S (**PGP**);
2. at least **exponential** in n for semigroups S without 1 (**EGP**).

Theorem (Zhuk, 2015)

Every finite algebra either has the PGP or EGP.

Theorem (Carvalho, Martin, Zhuk, 2017)

Let $\mathbb{B}$ be a finite idempotent algebra. Then

1. $\mathrm{QCSP}(\mathbb{B})$ is in NP if $\mathbb{B}$ has PGP;
2. $\mathrm{QCSP}(\mathbb{B})$ (allowing structures of infinite signature) is coNP-hard else.