Complexity of quantified constraint satisfaction on monoids

Peter Mayr

CU Boulder

Joint work with Hubie Chen
The quantified constraint satisfaction problem (QCSP)

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

where
- $\mathcal{B}$ finite relational structure of finite signature
- $\Phi = Q_1 x_1 \ldots Q_n x_n \land$ atomic formulas over $\mathcal{B}$
- each $Q_i \in \{\forall, \exists\}$, both quantifiers allowed
The quantified constraint satisfaction problem (QCSP)

QCSP: decide if $B \models \Phi$

where

- $B$ finite relational structure of finite signature
- $\Phi = Q_1x_1 \ldots Q_nx_n \land$ atomic formulas over $B$
- each $Q_i \in \{\forall, \exists\}$, both quantifiers allowed

Example

Quantified Boolean Formulas (QBF):

- $B = (\{0, 1\},$ clauses with 3 literals$)$
- $\Phi = \exists x_1 \forall y_1 \exists x_2 \forall y_2 : (x_1 \lor y_1 \lor y'_2) \land (x'_2 \lor y'_1 \lor y_2) \land \ldots$
The quantified constraint satisfaction problem (QCSP)

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

where

- $\mathcal{B}$ finite relational structure of finite signature
- $\Phi = Q_1x_1 \ldots Q_nx_n \land$ atomic formulas over $\mathcal{B}$
- each $Q_i \in \{\forall, \exists\}$, both quantifiers allowed

Example

Quantified Boolean Formulas (QBF):

- $\mathcal{B} = (\{0, 1\},$ clauses with 3 literals$)$
- $\Phi = \exists x_1 \forall y_1 \exists x_2 \forall y_2 : (x_1 \lor y_1 \lor y'_2) \land (x'_2 \lor y'_1 \lor y_2) \land \ldots$

QCSP is PSPACE-complete.
Fixed template QCSP

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

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

Problem: \(\mathbb{B} \models \Phi\)?
Fixed template QCSP

**QCSP**(\(\mathcal{B}\)), restricted version for fixed finite algebra \(\mathcal{B}\):

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

**Problem:** \(\mathcal{B} \models \Phi?\)

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

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

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

1 Examples of QCSP(\(\mathbb{B}\)) are in P, NP-complete, PSPACE-complete.
2 Complexity classification of 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 \( \text{CSP}(S) \) is in \( P \).
2. Else \( \text{CSP}(S) \) is \( \text{NP-complete} \).

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

\[
\begin{align*}
  ef &= e, \quad fe = f \Rightarrow e = f \\
  ef &= f, \quad fe = e \Rightarrow e = f
\end{align*}
\]
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 \( \text{QCSP}(S) \) is in \( P \).
- Else \( \text{QCSP}(S) \) is \( \text{NP-complete} \).

\[ a \in S \text{ is regular if } \exists b \in S : aba = a. \]
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 $\text{QCSP}(S)$ is in $P$.
- Else $\text{QCSP}(S)$ is $\text{NP}$-complete.

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

Theorem (Chen, M)

Let $S$ be a finite semigroup without 1 such that

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

Then $\text{QCSP}(S)$ is PSPACE-complete.
From tractable CSP to NP-complete QCSP

Example

\( S \ldots a \) zero semigroup with 1 adjoined

\[
\begin{array}{c|ccc}
\cdot & 0 & a & 1 \\
\hline 
0 & 0 & 0 & 0 \\
a & 0 & 0 & a \\
1 & 0 & a & 1 \\
\end{array}
\]

1. CSP\((S)\) is in P.
2. QCSP\((S)\) is NP-complete.
Proof: NP-hardness

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

Lemma (Chen, M, 2016)

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

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

Lemma (Chen, M, 2016)

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

Proof.

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

$a \in S \ldots$ maximal with respect to $\leq_J$, not generated by regulars

$0 \ldots$ elements $\not\in_J a$
Proof: NP-hardness

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

Lemma (Chen, M, 2016)
If a semigroup $S$ is not generated by its regular elements, then $\text{QCSP}(S)$ is NP-hard.

Proof.
$S$ has homomorphic image $\tilde{S} := S / 0$:

- $a \in S$ ... maximal with respect to $\leq \mathcal{J}$,
- not generated by regulars
- $0$ ... elements $\not\leq \mathcal{J} a$

Encode 1-in-3 SAT (NP-hard) into $\text{QCSP}(\tilde{S})$. 
Homomorphic images

Easy fact

For $\theta \in \text{Con}(B)$, QCSP($B/\theta$) has polytime reduction to QCSP($B$).
Lemma (Chen, 2008)

For any monoid $S$, $\text{QCSP}(S)$ is in NP.
Lemma (Chen, 2008)
For any monoid $S$, $\text{QCSP}(S)$ is in NP.

Proof.
Instances for monoids are collapsible:

$$\forall y_1 \exists x_1 \ldots \forall y_n \exists x_n : \phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$$

iff for every $i \leq n$:

$$\exists x_1 \ldots \exists x_{i-1} \forall y_i \exists x_i \ldots \exists x_n : \phi(x_1, \ldots, x_n, 1, \ldots, 1, y_i, 1 \ldots, 1).$$
Lemma (Chen, 2008)

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

Proof.

Instances for monoids are **collapsible**:

$$\forall y_1 \exists x_1 \ldots \forall y_n \exists x_n : \phi(x_1, \ldots, x_n, y_1, \ldots, y_n)$$

iff for every $i \leq n$:

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

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 $\text{QCSP}(S)$ is in $P$.

Proof.

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

$$\exists x_1 \ldots x_m \forall y \exists z_1 \ldots z_n : \phi(x_1 \ldots x_m, y, z_1 \ldots z_n)$$
Proof: tractability

Lemma (Chen, M, 2016)
Let $S$ be a block group with 1 that is generated by its regular elements. Then $QCSP(S)$ is in P.

Proof.

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

   $$\exists x_1 \ldots x_m \forall y \exists z_1 \ldots z_n : \phi(x_1 \ldots x_m, y, z_1 \ldots z_n)$$

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

   $$\phi(e_1 \ldots e_m, 1, f_1 \ldots f_n)$$
Proof: tractability

Lemma (Chen, M, 2016)
Let $S$ be a block group with 1 that is generated by its regular elements. Then $QCSP(S)$ is in P.

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

   $$\exists x_1 \ldots x_m \forall y \exists z_1 \ldots z_n : \phi(x_1 \ldots x_m, y, z_1 \ldots z_n)$$

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

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

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

   $$\forall y \exists z_1 \ldots z_n : \phi(e_1 \ldots e_m, y, z_1 \ldots z_n)$$
Given a QCSP\((S)\)-instance

\[ \forall y \exists z_1 \ldots \exists z_n \psi(y, z_1, \ldots, z_n), \quad (1) \]

for any regular \(a \in S\), deciding

\[ \exists z_1 \ldots \exists z_n \psi(a, z_1, \ldots, z_n) \quad (2) \]

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 \(a\).
Given a QCSP($S$)-instance

$$\forall y \exists z_1 \ldots \exists z_n \psi(y, z_1, \ldots, z_n),$$  \hspace{1cm} (1)

for any regular $a \in S$, deciding

$$\exists z_1 \ldots \exists z_n \psi(a, z_1, \ldots, z_n)$$  \hspace{1cm} (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 $a$.

Since $S$ is generated by regular elements and $\psi$ 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**).
Outlook

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