On the complexity of Quantified Constraint Satisfaction Problem via polymorphisms

Petar Marković

University of Novi Sad, Serbia

AAA92, Prague, May 2016

QCSP definition

Definition

Let $\mathbb{A}$ be a finite relational structure. The decision problem $QCSP(\mathbb{A})$ is:
INPUT: sentence $\varphi = (Q_1 x_1) \ldots (Q_n x_n)$(conjunction of atomic formulae).
Each $Q_i \in \{\exists, \forall\}$. Accept iff $\mathbb{A} \models \varphi$.

QCSP definition

Definition

Let $\mathbb{A}$ be a finite relational structure. The decision problem $QCSP(\mathbb{A})$ is:
INPUT: sentence $\varphi = (Q_1 x_1) \dots (Q_n x_n)$(conjunction of atomic formulae).
Each $Q_i \in \{\exists, \forall\}$. Accept iff $\mathbb{A} \models \varphi$.

Definition

The problem $CSP(\mathbb{A})$ additionally stipulates that all Q_i are $\exists$.

QCSP definition

Definition

Let $\mathbb{A}$ be a finite relational structure. The decision problem $QCSP(\mathbb{A})$ is:
INPUT: sentence $\varphi = (Q_1 x_1) \ldots (Q_n x_n)$(conjunction of atomic formulae).
Each $Q_i \in \{\exists, \forall\}$. Accept iff $\mathbb{A} \models \varphi$.

Definition

The problem $CSP(\mathbb{A})$ additionally stipulates that all Q_i are $\exists$.

$CSP(\mathbb{A})$ is at worst NP-complete, while $QCSP(\mathbb{A})$ is at worst Pspace-complete (for polynomial time many-one reductions).

Connectedness

Theorem

If $\mathbb{A}$ is disconnected, then $QCSP(\mathbb{A})$ reduces to $CSP(\mathbb{A}^c)$ (thus $QCSP(\mathbb{A}) \in NP$).

Connectedness

Theorem

If $\mathbb{A}$ is disconnected, then $QCSP(\mathbb{A})$ reduces to $CSP(\mathbb{A}^c)$ (thus $QCSP(\mathbb{A}) \in NP$).

Theorem

$QCSP(\mathbb{A})$ and $QCSP(\mathbb{A}^k)$ have the same complexity.

Connectedness

Theorem

If $\mathbb{A}$ is disconnected, then $QCSP(\mathbb{A})$ reduces to $CSP(\mathbb{A}^c)$ (thus $QCSP(\mathbb{A}) \in NP$).

Theorem

$QCSP(\mathbb{A})$ and $QCSP(\mathbb{A}^k)$ have the same complexity.

Theorem

$\mathbb{A}^k$ is connected for some $k \geq 2$ iff $\mathbb{A}^2$ is connected.

Connectedness

Theorem

If $\mathbb{A}$ is disconnected, then $QCSP(\mathbb{A})$ reduces to $CSP(\mathbb{A}^c)$ (thus $QCSP(\mathbb{A}) \in NP$).

Theorem

$QCSP(\mathbb{A})$ and $QCSP(\mathbb{A}^k)$ have the same complexity.

Theorem

$\mathbb{A}^k$ is connected for some $k \geq 2$ iff $\mathbb{A}^2$ is connected.

3 cases: $\mathbb{A}$ disconnected;

Connectedness

Theorem

If $\mathbb{A}$ is disconnected, then QCSP($\mathbb{A}$) reduces to CSP($\mathbb{A}^c$) (thus QCSP($\mathbb{A}$) $\in$ NP).

Theorem

QCSP($\mathbb{A}$) and QCSP($\mathbb{A}^k$) have the same complexity.

Theorem

$\mathbb{A}^k$ is connected for some $k \geq 2$ iff $\mathbb{A}^2$ is connected.

3 cases: $\mathbb{A}$ disconnected; $\mathbb{A}$ connected, but $\mathbb{A}^2$ disconnected

Connectedness

Theorem

If $\mathbb{A}$ is disconnected, then QCSP$(\mathbb{A})$ reduces to CSP$(\mathbb{A}^c)$ (thus QCSP$(\mathbb{A}) \in NP$).

Theorem

QCSP$(\mathbb{A})$ and QCSP$(\mathbb{A}^k)$ have the same complexity.

Theorem

$\mathbb{A}^k$ is connected for some $k \geq 2$ iff $\mathbb{A}^2$ is connected.

3 cases: $\mathbb{A}$ disconnected; $\mathbb{A}$ connected, but $\mathbb{A}^2$ disconnected and $\mathbb{A}^2$ connected.

Examples of CSP vs QCSP

$\mathbb{A}$ core and $\mathbb{A}^2$ disconnected $\Rightarrow QCSP(\mathbb{A})$ reduces to $CSP(\mathbb{A})$.

Examples of CSP vs QCSP

$\mathbb{A}$ core and $\mathbb{A}^2$ disconnected $\Rightarrow$ $QCSP(\mathbb{A})$ reduces to $CSP(\mathbb{A})$.

Example (Chen & Mayr; Božin - announced)

$\mathbb{A}$ such that $CSP(\mathbb{A}) \in P$, but $QCSP(\mathbb{A})$ is NP-complete.

Examples of CSP vs QCSP

$\mathbb{A}$ core and $\mathbb{A}^2$ disconnected $\Rightarrow$ $QCSP(\mathbb{A})$ reduces to $CSP(\mathbb{A})$.

Example (Chen & Mayr; Božin - announced)

$\mathbb{A}$ such that $CSP(\mathbb{A}) \in P$, but $QCSP(\mathbb{A})$ is NP-complete.

Example (Božin - announced)

$\mathbb{A}$ such that $CSP(\mathbb{A}) \in P$, but $QCSP(\mathbb{A})$ is *Pspace*-complete.

Examples of CSP vs QCSP

$\mathbb{A}$ core and $\mathbb{A}^2$ disconnected $\Rightarrow$ $QCSP(\mathbb{A})$ reduces to $CSP(\mathbb{A})$.

Example (Chen & Mayr; Božin - announced)

$\mathbb{A}$ such that $CSP(\mathbb{A}) \in P$, but $QCSP(\mathbb{A})$ is NP-complete.

Example (Božin - announced)

$\mathbb{A}$ such that $CSP(\mathbb{A}) \in P$, but $QCSP(\mathbb{A})$ is *Pspace*-complete.

Example (Easy)

$\mathbb{A}$ such that $CSP(\mathbb{A}) \in NP$, but $QCSP(\mathbb{A})$ is *Pspace*-complete.

Examples of CSP vs QCSP

$\mathbb{A}$ core and $\mathbb{A}^2$ disconnected $\Rightarrow$ $QCSP(\mathbb{A})$ reduces to $CSP(\mathbb{A})$.

Example (Chen & Mayr; Božin - announced)

$\mathbb{A}$ such that $CSP(\mathbb{A}) \in P$, but $QCSP(\mathbb{A})$ is *NP*-complete.

Example (Božin - announced)

$\mathbb{A}$ such that $CSP(\mathbb{A}) \in P$, but $QCSP(\mathbb{A})$ is *Pspace*-complete.

Example (Easy)

$\mathbb{A}$ such that $CSP(\mathbb{A}) \in NP$, but $QCSP(\mathbb{A})$ is *Pspace*-complete.

Conjecture (The Greater Barny Conjecture)

If $\mathbb{A}$ is a smooth digraph with no loops but with algebraic length 1 (= with $\mathbb{A}^2$ connected), then $QCSP(\mathbb{A})$ is *Pspace*-complete.

A Galois connection

$Pol(\mathbb{A}) = \{$All compatible operations of $\mathbb{A}\}$ (polymorphisms). The set of all surjective polymorphisms is denoted by $s - Pol(\mathbb{A})$.

A Galois connection

$Pol(\mathbb{A}) = \{$All compatible operations of $\mathbb{A}\}$ (polymorphisms). The set of all surjective polymorphisms is denoted by $s - Pol(\mathbb{A})$.

A relation compatible with all operations of $\mathbf{A}$ is an invariant relation (subpower) of $\mathbf{A}$. The relational clone of all subpowers of $\mathbf{A}$ is $Inv(\mathbf{A})$.

A Galois connection

$Pol(\mathbb{A}) = \{$All compatible operations of $\mathbb{A}\}$ (polymorphisms). The set of all surjective polymorphisms is denoted by $s - Pol(\mathbb{A})$.

A relation compatible with all operations of $\mathbf{A}$ is an invariant relation (subpower) of $\mathbf{A}$. The relational clone of all subpowers of $\mathbf{A}$ is $Inv(\mathbf{A})$.

Theorem (Jeavons, 1998)

If $Pol(A; \Gamma_1) \subseteq Pol(A; \Gamma_2)$ and Γ_2 is finite, then $CSP(A; \Gamma_2)$ logspace-reduces to $CSP(A; \Gamma_1)$.

A Galois connection

$Pol(\mathbb{A}) = \{$All compatible operations of $\mathbb{A}\}$ (polymorphisms). The set of all surjective polymorphisms is denoted by $s - Pol(\mathbb{A})$.

A relation compatible with all operations of **A** is an invariant relation (subpower) of **A**. The relational clone of all subpowers of **A** is $Inv(\mathbf{A})$.

Theorem (Jeavons, 1998)

If $Pol(A;\Gamma_1) \subseteq Pol(A;\Gamma_2)$ and Γ_2 is finite, then $CSP(A;\Gamma_2)$ logspace-reduces to $CSP(A;\Gamma_1)$.

Theorem (BBCJK, 2009)

If $s - Pol(A;\Gamma_1) \subseteq s - Pol(A;\Gamma_2)$ and Γ_2 is finite, then $QCSP(A;\Gamma_2)$ logspace-reduces to $QCSP(A;\Gamma_1)$

Basic Pspace-complete cases

Theorem (Shaeffer, 1978; Dalmau, 1997)

$Q - NAE - SAT$ and $Q - 1 - in - 3 - SAT$ are Pspace-complete.

Basic Pspace-complete cases

Theorem (Shaeffer, 1978; Dalmau, 1997)

$Q - NAE - SAT$ *and* $Q - 1 - in - 3 - SAT$ *are Pspace-complete.*

Theorem (Creignou, Khanna & Sudan, 2001)

$QCSP(\rho_{NAE})$ *and* $QCSP(\rho_{1/3})$ *are Pspace-complete.*

Basic Pspace-complete cases

Theorem (Shaeffer, 1978; Dalmau, 1997)

$Q - NAE - SAT$ *and* $Q - 1 - in - 3 - SAT$ *are Pspace-complete.*

Theorem (Creignou, Khanna & Sudan, 2001)

$QCSP(\rho_{NAE})$ *and* $QCSP(\rho_{1/3})$ *are Pspace-complete.*

Theorem (BBCJK, 2009)

For any $n \geq 3$, $QCSP(\rho_{NAE})$ *reduces to* $QCSP(\mathbb{K}_n)$, *so* $QCSP(\mathbb{K}_n)$ *is Pspace-complete.*

Basic Pspace-complete cases

Theorem (Shaeffer, 1978; Dalmau, 1997)

$Q - NAE - SAT$ *and* $Q - 1 - in - 3 - SAT$ *are Pspace-complete.*

Theorem (Creignou, Khanna & Sudan, 2001)

$QCSP(\rho_{NAE})$ *and* $QCSP(\rho_{1/3})$ *are Pspace-complete.*

Theorem (BBCJK, 2009)

For any $n \geq 3$, $QCSP(\rho_{NAE})$ *reduces to* $QCSP(\mathbb{K}_n)$, *so* $QCSP(\mathbb{K}_n)$ *is Pspace-complete.*

Some applications

Fact

All polymorphisms of $\mathbb{K}_n$*,* $n \geq 3$ *are of the form* $f(x_1, \ldots, x_k) = \pi(x_i)$*, where* $\pi \in Sym(n)$ *and* $1 \leq i \leq k$ *are arbitrary.*

Some applications

Fact

All polymorphisms of $\mathbb{K}_n$, $n \geq 3$ *are of the form* $f(x_1, \ldots, x_k) = \pi(x_i)$, *where* $\pi \in Sym(n)$ *and* $1 \leq i \leq k$ *are arbitrary.*

Corollary

QCSP$(\mathbb{A})$ *is Pspace-complete when all* $f \in s - Pol(\mathbb{A})$ *are essentially unary (*$=$ $\mathbb{A}$ *is idempotent-trivial when* $\mathbb{A}$ *is core).*

Some applications

Fact

All polymorphisms of $\mathbb{K}_n$, $n \geq 3$ are of the form $f(x_1, \ldots, x_k) = \pi(x_i)$, where $\pi \in Sym(n)$ and $1 \leq i \leq k$ are arbitrary.

Corollary

$QCSP(\mathbb{A})$ is Pspace-complete when all $f \in s - Pol(\mathbb{A})$ are essentially unary ($= \mathbb{A}$ is idempotent-trivial when $\mathbb{A}$ is core).

Theorem (Larose, 2006)

Any tournament $\mathbb{T}$ with loops and all constants added is either idempotent trivial or transitive. In the second case it easily follows that $QCSP(\mathbb{T}) \in P$.

Some applications

Fact

All polymorphisms of $\mathbb{K}_n$, $n \geq 3$ are of the form $f(x_1, \ldots, x_k) = \pi(x_i)$, where $\pi \in Sym(n)$ and $1 \leq i \leq k$ are arbitrary.

Corollary

$QCSP(\mathbb{A})$ is Pspace-complete when all $f \in s - Pol(\mathbb{A})$ are essentially unary ($=$ $\mathbb{A}$ is idempotent-trivial when $\mathbb{A}$ is core).

Theorem (Larose, 2006)

Any tournament $\mathbb{T}$ with loops and all constants added is either idempotent trivial or transitive. In the second case it easily follows that $QCSP(\mathbb{T}) \in P$.

Theorem (Đapić, - & Martin - see Petar's talk)

All smooth semicomplete digraphs are idempotent-trivial, except $\mathbb{K}_2$ and $\mathbb{C}_3$.

Cycle with an extra edge

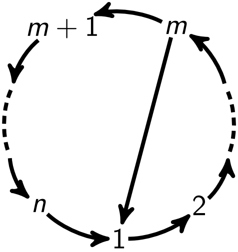

Figure : $\mathbb{C}_{m,n}$

Cycle with an extra edge

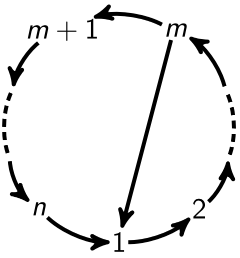

Figure : $\mathbb{C}_{m,n}$

Example (Bašić, - & Martin)

Let $\mathbb{C}_{m,n}$ $(1 < m < n)$ be the digraph drawn on the above picture.

Cycle with an extra edge

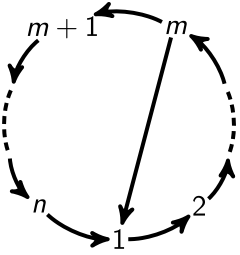

Figure : $\mathbb{C}_{m,n}$

Example (Bašić, - & Martin)

Let $\mathbb{C}_{m,n}$ $(1 < m < n)$ be the digraph drawn on the above picture.
If $m|n$ then $QCSP(\mathbb{C}_{m,n}) \in P$,

Cycle with an extra edge

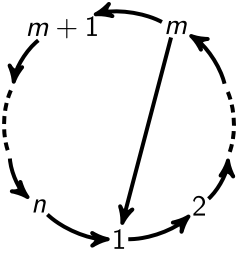

Figure : $\mathbb{C}_{m,n}$

Example (Bašić, - & Martin)

Let $\mathbb{C}_{m,n}$ $(1 < m < n)$ be the digraph drawn on the above picture.
If $m|n$ then $QCSP(\mathbb{C}_{m,n}) \in P$,
If $(m,n) > 1$ and $m \nmid n$, then $QCSP(\mathbb{C}_{m,n})$ is NP-complete,

Cycle with an extra edge

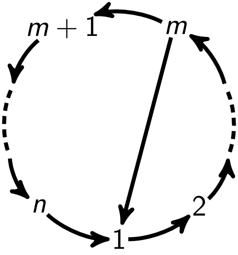

Figure : $\mathbb{C}_{m,n}$

Example (Bašić, - & Martin)

Let $\mathbb{C}_{m,n}$ $(1 < m < n)$ be the digraph drawn on the above picture.
If $m|n$ then $QCSP(\mathbb{C}_{m,n}) \in P$,
If $(m,n) > 1$ and $m \nmid n$, then $QCSP(\mathbb{C}_{m,n})$ is NP-complete,
If $(m,n) = 1$ then $\mathbb{C}_{m,n}$ is idempotent-trivial and so $QCSP(\mathbb{C}_{m,n})$ is *Pspace*-complete.

Chen's collapsibility and switchability

The collapsibility given below is not the original definition, but an equivalent over idempotent finite algebras:

Chen's collapsibility and switchability

The collapsibility given below is not the original definition, but an equivalent over idempotent finite algebras:

Definition (Collapsibility)

An algebra $\mathbf{A}$ is k-collapsible if for all $n > k$, $\mathbf{A}^n$ is generated by all n-tuples in which there are at least $n - k$ coordinates which are equal.

Chen's collapsibility and switchability

The collapsibility given below is not the original definition, but an equivalent over idempotent finite algebras:

Definition (Collapsibility)

An algebra $\mathbf{A}$ is k-collapsible if for all $n > k$, $\mathbf{A}^n$ is generated by all n-tuples in which there are at least $n - k$ coordinates which are equal.

Definition (Switch)

A tuple $(a_1, \ldots, a_n) \in A^n$ has a *switch* at i if $a_{i-1} \neq a_i$.

Chen's collapsibility and switchability

The collapsibility given below is not the original definition, but an equivalent over idempotent finite algebras:

Definition (Collapsibility)

An algebra $\mathbf{A}$ is k-collapsible if for all $n > k$, $\mathbf{A}^n$ is generated by all n-tuples in which there are at least $n - k$ coordinates which are equal.

Definition (Switch)

A tuple $(a_1, \ldots, a_n) \in A^n$ has a *switch* at i if $a_{i-1} \neq a_i$.

Definition (Switchability)

An algebra $\mathbf{A}$ is k-switchable if for all $n > k$, $\mathbf{A}^n$ is generated by all n-tuples with at most k switches. $\mathbf{A}$ is switchable if it is k-switchable for some k.

PGP and EGP

The central notions to Chen's approach to QCSP are PGP and EGP.

PGP and EGP

The central notions to Chen's approach to QCSP are PGP and EGP.

Definition (PGP and EGP)

A finite algebra $\mathbf{A}$ has *polynomially generated powers* (PGP) if there exists a polynomial $p(x)$ such that for all n, $\mathbf{A}^n$ is generated by some set of tuples with at most $p(n)$ elements. $\mathbf{A}$ has *exponentially generated powers* (EGP) if there exists a constant $c > 0$ such that for almost all n, any generating set of $\mathbf{A}^n$ has more than 2^{cn} elements.

PGP and EGP

The central notions to Chen's approach to QCSP are PGP and EGP.

Definition (PGP and EGP)

A finite algebra $\mathbf{A}$ has *polynomially generated powers* (PGP) if there exists a polynomial $p(x)$ such that for all n, $\mathbf{A}^n$ is generated by some set of tuples with at most $p(n)$ elements. $\mathbf{A}$ has *exponentially generated powers* (EGP) if there exists a constant $c > 0$ such that for almost all n, any generating set of $\mathbf{A}^n$ has more than 2^{cn} elements.

Theorem (Zhuk 2015)

Let $\mathbf{A}$ be a finite algebra. Then either $\mathbf{A}$ is switchable, or $\mathbf{A}$ has EGP.

PGP and EGP

The central notions to Chen's approach to QCSP are PGP and EGP.

Definition (PGP and EGP)

A finite algebra $\mathbf{A}$ has *polynomially generated powers* (PGP) if there exists a polynomial $p(x)$ such that for all n, $\mathbf{A}^n$ is generated by some set of tuples with at most $p(n)$ elements. $\mathbf{A}$ has *exponentially generated powers* (EGP) if there exists a constant $c > 0$ such that for almost all n, any generating set of $\mathbf{A}^n$ has more than 2^{cn} elements.

Theorem (Zhuk 2015)

Let $\mathbf{A}$ *be a finite algebra. Then either* $\mathbf{A}$ *is switchable, or* $\mathbf{A}$ *has EGP.*

It is easy to show that collapsibility implies switchability, which implies PGP. So the above theorem gives a dichotomy between PGP and EGP for finite algebras.

Applications to QCSP

Theorem (Chen)

Let $\mathbf{A}$ *be a finite idempotent algebra. Switchability of* $\mathbf{A}$ *implies that* $QCSP(\mathbb{A})$ *reduces to* $CSP(\mathbb{A})$ *for any relational structure* $\mathbb{A}$ *which consists of relations in* $Inv(\mathbf{A})$.

Applications to QCSP

Theorem (Chen)

Let $\mathbf{A}$ *be a finite idempotent algebra. Switchability of* $\mathbf{A}$ *implies that* $QCSP(\mathbb{A})$ *reduces to* $CSP(\mathbb{A})$ *for any relational structure* $\mathbb{A}$ *which consists of relations in* $Inv(\mathbf{A})$.

HOWEVER:

Applications to QCSP

Theorem (Chen)

Let $\mathbf{A}$ *be a finite idempotent algebra. Switchability of* $\mathbf{A}$ *implies that* $QCSP(\mathbb{A})$ *reduces to* $CSP(\mathbb{A})$ *for any relational structure* $\mathbb{A}$ *which consists of relations in* $Inv(\mathbf{A})$.

HOWEVER:

Example [Zhuk]

There exists a finite relational structure $\mathbb{A}$ such that $QCSP(\mathbb{A})$ is in P, while the algebra $Pol(\mathbb{A})$ has EGP.

Applications to QCSP

Theorem (Chen)

Let $\mathbf{A}$ *be a finite idempotent algebra. Switchability of* $\mathbf{A}$ *implies that* $QCSP(\mathbb{A})$ *reduces to* $CSP(\mathbb{A})$ *for any relational structure* $\mathbb{A}$ *which consists of relations in* $Inv(\mathbf{A})$.

HOWEVER:

Example [Zhuk]

There exists a finite relational structure $\mathbb{A}$ such that $QCSP(\mathbb{A})$ is in P, while the algebra $Pol(\mathbb{A})$ has EGP.

Also, Martin and Zhuk (2015) proved that on three-element idempotent algebras which have no type $\mathbf{1}$ covers, finite relatedness and switchability imply collapsibility. They conjecture that the same holds for all idempotent algebras which omit type $\mathbf{1}$.

DĚKUJI ZA POZORNOST!