QCSP Monsters and the future of the Chen Conjecture

Barnaby Martin with Dmitriy Zhuk and friends

Algorithms and Complexity Group, Durham University, UK

CSP Seminar, 21st October 2020 (on zoom)

Quantified Constraint Satisfaction

The *quantified constraint satisfaction problem* QCSP($\mathcal{B}$) has

- Input: a sentence ϕ of $\{\forall, \exists, \wedge, =\}$-FO.
- Question: does $\mathcal{B} \models \phi$?

It is the CSP with $\forall$ returned.

''CSPs are ubiquitous in CS . . . , while QCSPs can not nearly claim to be so important in applications."

useful QCSPs	classified?
relativised $(\forall x \in X, \exists y \in Y)$	$\surd$
Boolean (QBF or QSAT)	$\surd$

". . . what is left of the true non-Boolean QCSP is a problem I believe to be mostly of interest to theorists."

Nonetheless, finite-domain QCSPs have been heavily studied in the literature and are known to reach complexities P, NP-complete and Pspace-complete.

Complexity of Model Checking

Fragment	Dual	Classification?
$\{\exists, \vee\}$ $\{\exists, \vee, =\}$ $\{\exists, \vee, \neq\}$	$\{\forall, \wedge\}$ $\{\forall, \wedge, \neq\}$ $\{\forall, \wedge, =\}$	Logspace
$\{\exists, \wedge, \vee\}$ $\{\exists, \wedge, \vee, =\}$ $\{\exists, \wedge, \vee, \neq\}$	$\{\forall, \wedge, \vee\}$ $\{\forall, \wedge, \vee, \neq\}$ $\{\forall, \wedge, \vee, =\}$	Logspace if there is some element a s.t. all relations are a-valid, and NP-complete otherwise
$\{\exists, \wedge\}$ $\{\exists, \wedge, =\}$	$\{\forall, \vee\}$ $\{\forall, \vee, \neq\}$	CSP dichotomy conjecture: P or NP-complete
$\{\exists, \wedge, \neq\}$	$\{\forall, \vee, =\}$	NP-complete for $\lvert\mathcal{D}\rvert \geq 3$, reduces to Schaefer classes otherwise.
$\{\exists, \forall, \wedge\}$ $\{\exists, \forall, \wedge, =\}$	$\{\exists, \forall, \vee\}$ $\{\exists, \forall, \vee, \neq\}$	QCSP polychotomy: P, NP-complete, or Pspace-complete ?
$\{\exists, \forall, \wedge, \neq\}$	$\{\exists, \forall, \vee, =\}$	Pspace-complete for $\lvert\mathcal{D}\rvert \geq 3$, reduces to Schaefer classes for Quantified Sat otherwise.
$\{\forall, \exists, \wedge, \vee\}$		Tetrachotomy: P, NP-complete, co-NP-complete or Pspace-complete
$\{\forall, \exists, \wedge, \vee, =\}$ $\{\forall, \exists, \wedge, \vee, \neq\}$ $\{\neg, \exists, \forall, \wedge, \vee, =\}$		Logspace when $\lvert\mathcal{D}\rvert \leq 1$, Pspace-complete otherwise
$\{\neg, \exists, \forall, \wedge, \vee\}$		Logspace when $\mathcal{D}$ contains only empty or full relations, Pspace-complete otherwise

First-order structures

Relational structures:

$$\mathcal{B} := (B; R_1, R_2, \ldots)$$

Functional structures:

$$\mathbb{B} := (D; f_1, f_2, \ldots)$$

$$\text{functional structures} \;=\; \text{algebras.}$$

What is the interplay between relational and functional structures?

$$\text{Model Theory} \;=\; \text{Logic} \;+\; \text{Universal Algebra}$$

All our structures are finite-domain.

Interplay

Let R be an m-ary relation on $\mathcal{B}$. We say that a k-ary operation $f : B^k \to B$ *preserves* R (or R is *invariant*) under f if:

$$\frac{\begin{array}{cccc} f, & f, & \ldots, & f \\ (x_{11}, & x_{12}, & \ldots, & x_{1m}) \in R \\ (x_{21}, & x_{22}, & \ldots, & x_{2m}) \in R \\ \vdots & \vdots & & \vdots \\ (x_{k1}, & x_{k2}, & \ldots, & x_{km}) \in R \end{array}}{(y_1, \quad y_2, \quad \ldots, \quad y_m) \in R}$$

where each $y_i = f(x_{1i}, x_{2i}, \ldots, x_{ki})$.

- operations that preserve each of the relations of $\mathcal{B}$ are $\mathrm{Pol}(\mathcal{B})$.
- relations invariant under each operation of $\mathbb{B}$ are $\mathrm{Inv}(\mathbb{B})$.

one-side of a Galois Correspondence

Let $\mathcal{B}$ and $\mathbb{B}$ be over the same finite domain B.

$$\mathrm{Inv}(\mathrm{Pol}(\mathcal{B})) = \langle \mathcal{B} \rangle_{\{\exists,\wedge,=\}}$$
$$\mathrm{Inv}(\mathrm{surPol}(\mathcal{B})) = \langle \mathcal{B} \rangle_{\{\forall,\exists,\wedge,=\}}$$

Idempotent operations are surjective! The algebraic definition for QCSP($\mathbb{B}$) has

- Input: a sentence ϕ of $\{\forall, \exists, \wedge\}$-FO with some relations $\mathcal{B} \in \mathrm{Inv}(\mathbb{B})$.
- Question: does $\mathcal{B} \models \phi$?

What if $\mathrm{Inv}(\mathbb{B})$ is infinite?

one-side of a Galois Correspondence

Let $\mathcal{B}$ and $\mathbb{B}$ be over the same finite domain B.

$$\mathrm{Inv}(\mathrm{Pol}(\mathcal{B})) = \langle \mathcal{B} \rangle_{\{\exists,\wedge,=\}}$$
$$\mathrm{Inv}(\mathrm{surPol}(\mathcal{B})) = \langle \mathcal{B} \rangle_{\{\forall,\exists,\wedge,=\}}$$

Idempotent operations are surjective! The algebraic definition for QCSP($\mathbb{B}$) has

- Input: a sentence ϕ of $\{\forall, \exists, \wedge\}$-FO with some relations $\mathcal{B} \in \mathrm{Inv}(\mathbb{B})$.
- Question: does $\mathcal{B} \models \phi$?

What if $\mathrm{Inv}(\mathbb{B})$ is infinite? There isn't a simple way to solve this... traditionally it is forbidden – one studies arbitrary finite subsets of $\mathrm{Inv}(\mathbb{B})$ instead.

Let us turn to the the growth rate of generating sets for direct powers of an algebra $\mathbb{A}$.

For $\mathbb{A}$ we have a function $f_{\mathbb{A}} : \mathbb{N} \to \mathbb{N}$, giving the cardinality of the minimal generating sets of the sequence

- $\mathbb{A}, \mathbb{A}^2, \mathbb{A}^3, \ldots$ as
- $f(1), f(2), f(3), \ldots$.

We say $\mathbb{A}$ has the XGP with:

(PGP) polynomial, when $f_{\mathbb{A}}(i) = O(i^c)$, for some c; and

(EGP) exponential, when exists b so that $f_{\mathbb{A}}(i) = \Omega(b^i)$.

History

Theorem (Wiegold 1987)

Let $\mathbb{B}$ be a finite semigroup. If $\mathbb{B}$ is a monoid then $\mathbb{B}$ has the (linear) PGP. Otherwise, $\mathbb{B}$ has the EGP.

Proof of PGP.

If $\mathbb{B}$ is a monoid with identity 1 and $|B| = n$, then

$$\begin{array}{c}(B, 1, \ldots, 1, 1)\\(1, B, \ldots, 1, 1)\\\vdots\\(1, 1, \ldots, B, 1)\\(1, 1, \ldots, 1, B)\end{array}$$

is a generating set for $\mathbb{B}^m$ of size mn.

Theorem (Wiegold 1987)

Let $\mathbb{B}$ be a finite semigroup. If $\mathbb{B}$ is a monoid then $\mathbb{B}$ has the (linear) PGP. Otherwise, $\mathbb{B}$ has the EGP.

Proof of EGP.

Otherwise, without an identity, $\mathbb{B}$ and $\mathbb{B}^m$ have the properties that

$$|x \cdot B| \leq n-1, \text{ for each } x \in B.$$
$$|z \cdot B^m| \leq (n-1)^m, \text{ for each } z \in B^m.$$

Thus, a subset of B^m of size r can generate no more $r + r(n-1)^m$ elements in $\mathbb{B}^m$. Thus, a generating set must be of size $\geq \left(\frac{2n}{2n-1}\right)^m$.

Switchability and the PGP

Call an algebra $\mathbb{B}$ k-PGP-switchable if $\mathbb{B}^m$ is generated from the set of m-tuples of the form

- $(x_1, \ldots, x_1, x_2, \ldots x_2, \ldots, \ldots, x_{k'}, \ldots, x_{k'})$ for some $k' \leq k$.

switchability were originally introduced in connection with the QCSP by Hubie Chen!

Theorem (Chen 2008)

If $\mathbb{A}$ is switchable then QCSP($\mathbb{A}$) is in NP.

Theorem (Carvalho et al. 2015)

$\mathbb{A}$ is PGP-switchable iff it is switchable.

The Chen Conjecture

Conjecture (Chen Conjecture 2012)

Let $\mathcal{B}$ be a finite relational structure expanded with all constants. If Pol($\mathcal{B}$) has PGP, then QCSP($\mathcal{B}$) is in NP; otherwise QCSP($\mathcal{B}$) is Pspace-complete.

Part way there...

Theorem (Zhuk 2015)

Let $\mathbb{B}$ be a finite algebra, then either $\mathbb{B}$ is PGP-switchable or it has EGP.

Theorem (Feder-Vardi Conjecture; Bulatov/ Zhuk 2017)

Let $\mathcal{B}$ be a finite relational structure expanded with all constants. Pol($\mathcal{B}$) has a WNU, then CSP($\mathcal{B}$) in P; otherwise CSP($\mathcal{B}$) is NP-complete.

The Chen Conjecture

Conjecture (Chen Conjecture New Form)

Let $\mathcal{B}$ be a finite relational structure expanded with all constants. If Pol($\mathcal{B}$) has PGP and a WNU, then QCSP($\mathcal{B}$) is in P; if Pol($\mathcal{B}$) has PGP and no WNU, then QCSP($\mathcal{B}$) is NP-complete; otherwise QCSP($\mathcal{B}$) is Pspace-complete.

Part way there...

Theorem (Zhuk 2015)

Let $\mathbb{B}$ be a finite algebra, then either $\mathbb{B}$ is PGP-switchable or it has EGP.

Theorem (Feder-Vardi Conjecture; Bulatov/ Zhuk 2017)

Let $\mathcal{B}$ be a finite relational structure expanded with all constants. Pol($\mathcal{B}$) has a WNU, then CSP($\mathcal{B}$) in P; otherwise CSP($\mathcal{B}$) is NP-complete.

The life of the Chen Conjecture

Let $\mathbb{A}$ be an idempotent algebra on a finite domain A. Consider two encodings of relations in $\mathrm{Inv}(\mathbb{A})$, tuples vs. DNF:

$$\{ \quad (1,0,0), \quad (0,1,0), \quad (0,0,1), \quad (1,1,0), \quad (1,0,1), \quad (1,1,0), \quad \} \qquad (x \neq y \vee y \neq z)$$

Theorem (Revised Chen Conjecture: Carvalho et al. 2017)

Choose the DNF encoding. If $\mathbb{A}$ satisfies PGP, then $QCSP(\mathrm{Inv}(\mathbb{A}))$ is in NP. Otherwise, if $\mathbb{A}$ satisfies EGP, then $QCSP(\mathrm{Inv}(\mathbb{A}))$ is co-NP-hard.

Conjecture (Alternative Chen Conjecture: Carvalho et al. 2017)

If $\mathbb{A}$ satisfies PGP, then for every finite reduct $\mathcal{B} \subseteq \mathrm{Inv}(\mathbb{A})$, $QCSP(\mathcal{B})$ is in NP. Otherwise, there exists a finite reduct $\mathcal{B} \subseteq \mathrm{Inv}(\mathbb{A})$ so that $QCSP(\mathcal{B})$ is co-NP-hard.

The life of the Chen Conjecture

Let $\mathbb{A}$ be an idempotent algebra on a finite domain A. Consider two encodings of relations in $\mathrm{Inv}(\mathbb{A})$, tuples vs. DNF:

$$\{ \quad (1,0,0), \quad (0,1,0), \quad (0,0,1), \quad (1,1,0), \quad (1,0,1), \quad (1,1,0), \quad \} \qquad (x \neq y \vee y \neq z)$$

Theorem (Revised Chen Conjecture: Carvalho et al. 2017)

Choose the DNF encoding. If $\mathbb{A}$ satisfies PGP, then $QCSP(\mathrm{Inv}(\mathbb{A}))$ is in NP. Otherwise, if $\mathbb{A}$ satisfies EGP, then $QCSP(\mathrm{Inv}(\mathbb{A}))$ is co-NP-hard.

Conjecture (Alternative Chen Conjecture: Carvalho et al. 2017)

If $\mathbb{A}$ satisfies PGP, then for every finite reduct $\mathbb{B} \subseteq \mathrm{Inv}(\mathbb{A})$, $QCSP(\mathbb{B})$ is in NP. Otherwise, there exists a finite reduct $\mathbb{B} \subseteq \mathrm{Inv}(\mathbb{A})$ so that $QCSP(\mathbb{B})$ is co-NP-hard.

This conjecture is equivalent to the Revised Chen Conjecture using the tuple encoding. It is false.

Henceforth, α, β be strict subsets of A so that $\alpha \cup \beta = A$.

Theorem (Zhuk 2015)

Algebra $\mathbb{A}$ (idempotent) has EGP iff exists such α, β with

$$\sigma_k(x_1, y_1, \ldots, x_k, y_k) := \rho(x_1, y_1) \vee \ldots \vee \rho(x_k, y_k),$$

where $\rho(x, y) = (\alpha \times \alpha) \cup (\beta \times \beta)$, is in $\mathrm{Inv}(\mathbb{A})$, for each $k \in \mathbb{N}$.

We prefer the relation $\tau_k(x_1, y_1, z_1 \ldots, x_k, y_k, z_k)$ defined by

$$\tau_k(x_1, y_1, z_1 \ldots, x_k, y_k, z_k) := \rho'(x_1, y_1, z_1) \vee \ldots \vee \rho'(x_k, y_k, z_k),$$

where $\rho'(x, y, z) = (\alpha \times \alpha \times \alpha) \cup (\beta \times \beta \times \beta)$.

Corollary

Algebra $\mathbb{A}$ (idempotent) has EGP iff exists such α, β with $\tau_k(x_1, y_1, z_1 \ldots, x_k, y_k, z_k)$ in $\mathrm{Inv}(\mathbb{A})$, for each $k \in \mathbb{N}$.

co-NP-hardness

Theorem (Carvalho et al. 2017)

If $\mathrm{Inv}(\mathbb{A})$ *satisfies EGP, then QCSP*$(\mathrm{Inv}(\mathbb{A}))$ *is co-NP-hard.*

Proof.

Reduce from the complement of (monotone) 3-*not-all-equal-sat*.

$$\exists x_1^1, x_1^2, x_1^3, \ldots, \ldots, x_m^1, x_m^2, x_m^3 \, \mathrm{NAE}(x_1^1, x_1^2, x_1^3) \wedge \ldots \wedge \mathrm{NAE}(x_m^1, x_m^2, x_m^3)$$

becomes

$$\forall x_1^1, x_1^2, x_1^3, \ldots, \ldots, x_m^1, x_m^2, x_m^3 \; \rho'(x_1^1, x_1^2, x_1^3) \vee \ldots \vee \rho'(x_m^1, x_m^2, x_m^3)$$

where we note that $\tau_m(x_1, y_1, z_1 \ldots, x_m, y_m, z_m) :=$

$$\rho'(x_1, y_1, z_1) \vee \ldots \vee \rho'(x_m, y_m, z_m)$$

has a DNF representation that is polynomially-sized in m.

□

Recall, α, β be strict subsets of A so that $\alpha \cup \beta = A$. Now ask further that $\alpha \cap \beta \neq \emptyset$.

Corollary (Carvalho et al. 2017)

$QCSP(A; \{\tau_n : n \in \mathbb{N}\}, \{a : a \in A\})$ is co-NP-hard.

In fact,

Proposition (Carvalho et al. 2017)

$QCSP(A; \{\tau_n : n \in \mathbb{N}\}, \{a : a \in A\})$ is in co-NP.

Proof.

Roughly speaking, evaluate all existential variables to something in $\alpha \cap \beta$. But $(A; \{\tau_n : n \in \mathbb{N}\}, \{a : a \in A\})$ is not finitely related. □

Proposition (Carvalho et al. 2017)

For every finite reduct $\mathcal{B}$ of $(A; \{\tau_n : n \in \mathbb{N}\}, \{a : a \in A\})$, $QCSP(\mathcal{B})$ is in NL.

Back to * finite structures * and the Chen Conjecture

The conventional definition for QCSP($\mathcal{B}$), where $\mathcal{B}$ is a finite constraint language, is

- Input: a sentence ϕ of $\{\forall, \exists, \wedge\}$-FO.
- Question: does $\mathcal{B} \models \phi$?

Conjecture (Chen Conjecture New Form)

Let $\mathcal{B}$ be a finite relational structure expanded with all constants. If Pol($\mathcal{B}$) has PGP and a WNU, then QCSP($\mathcal{B}$) is in P; if Pol($\mathcal{B}$) has PGP and no WNU, then QCSP($\mathcal{B}$) is NP-complete; otherwise QCSP($\mathcal{B}$) is Pspace-complete.

If Pol($\mathcal{B}$) has EGP, for co-NP-hardness in place of Pspace-completeness, all we need to do is polynomially compute $\{\exists, \wedge, =\}$-definitions of τ_n from $\mathcal{B}$!

Death of the Chen Conjecture I

Example $R_{\delta,3}$.

$$\{(1,\_,\_), \quad (2,\_,\_), \qquad\qquad (x \neq 0 \vee y = z)$$
$$(0,0,0), \quad (0,1,1), \quad (0,2,2),$$

Example $R_{\mathrm{and},2}$.

$$\{ \quad (0,0,0), \quad (0,1,0), \quad (1,0,0),$$
$$(1,1,1), \quad (2,\_,\_), \quad (\_,2,\_), \quad \}$$

- QCSP$(\{0,1,2\}; 0, 1, 2, R_{\mathrm{and},2}, R_{\delta})$ is co-NP-complete.

Death of the Chen Conjecture II

Example $R_{\delta,2}$.

$$\{ \quad (0,0), \quad (1,0), \quad (2,0), \\ \quad (1,2), \quad (2,2) \qquad\qquad \}$$

Example $R_{\mathrm{and},2}$.

$$\{ \quad (0,0), \quad (1,0), \quad (2,0), \\ \quad (1,2), \quad (2,2) \qquad\qquad \}$$

- $\mathrm{Pol}(\{0,1,2\}; 0, 1, 2, R_{\mathrm{and},2}, R_{\delta,3})$ has EGP.
- $\mathrm{QCSP}(\{0,1,2\}; 0, 1, 2, R_{\mathrm{and},2}, R_{\delta,3})$ is in P.

QCSP Monsters

There are finite $\mathcal{B}$ so that QCSP($\mathcal{B}$) ranges over

- in P.
- NP-complete.
- Pspace-complete.
- co-NP-complete.
- DP-complete.
- Θ_2^P-complete.
- ...

Theorem

Let $\mathcal{B}$ be a finite 3-element relational structure expanded with all constants. Either QCSP($\mathcal{B}$) is in P, is NP-complete, is co-NP-complete or is Pspace-complete.

co-NP membership through the Olšák-Zhuk method

Consider the domain $A = \{0, 1, 2\}$. An operation f is 0-*stable* if $f(x, 0) = x$ and $f(x, 2) = 2$. s is the idempotent semilattice with $s(a, b) = 2$ whenever $a \neq b$.

Lemma

Suppose Γ *is preserved by* s *and a 0-stable operation* h_0*. Then an instance*

$$\forall x_1 \exists y_1 \forall x_2 \exists y_2 \ldots \forall x_n \exists y_n \Phi$$

of $\mathrm{QCSP}(\Gamma)$ *is equivalent to*

$$\forall x_1 \forall x_2 \ldots \forall x_n \exists \exists ((\exists' \exists' \Phi_1) \wedge (\exists' \exists' \Phi_2) \wedge \cdots \wedge (\exists' \exists' \Phi_n)),$$

where

$$\Phi_i = \Phi^{x_{i+1},\ldots,x_n,y_{i+1},\ldots,y_n}_{x'_{i+1},\ldots,x'_n,y'_{i+1},\ldots,y'_n} \wedge x'_{i+1} = 0 \wedge \cdots \wedge x'_n = 0,$$

Proof of Lemma

(Forwards/ downwards.) If we have a solution $(f_1, \ldots, f_n)$ of the original instance then it is also a solution of the new instance with the additional assignments $x'_j = 0$ and $y'_j = f_j(x_1, \ldots, x_i, 0, \ldots, 0)$ in the definition of Φ_i for every j.

Proof of Lemma

(Backwards/ upwards.) Consider solutions of the new instance such that $y_i = f_i(x_1, \ldots, x_n)$ for every i. Let N be the minimal s.t. f_N depends on x_j for some $j > N$. Assume for contradiction that such an N does exist and choose it minimal among all the solutions. Since $(f_1, \ldots, f_n)$ is also a solution of Φ_N, the following tuple is a solution of Φ

$$(x_1, \ldots, x_N, 0, \ldots, 0, f_1(x_1, \ldots, x_n), \ldots, f_N(x_1, \ldots, x_n), h_{N+1}(x_1, \ldots, x_n), \ldots, h_n(x_1, \ldots, x_n))$$

for every $x_1, \ldots, x_n$ and some functions $h_{N+1}, \ldots, h_n$.

Proof of Lemma

Note that we could see this tuple as
$(x_1, \ldots, x_N, 0, \ldots, 0, f_1(x_1), \ldots, f_{N-1}(x_1, \ldots, x_{N-1}), f_N(x_1, \ldots, x_n), h_{N+1}(x_1, \ldots, x_n), \ldots)$
as we assume f_i depends only on $x_1, \ldots, x_i$ for $i \leq N$. Consider all the evaluations of the variables $x_{N+1}, \ldots, x_n$ to obtain 3^{n-N} solutions of Φ, then apply s to them to obtain one solution $\alpha(x_1, \ldots, x_N)$ of the form
$(x_1, \ldots, x_N, 0, \ldots, 0, f_1(x_1, \ldots, x_n), \ldots, f_{N-1}(x_1, \ldots, x_n), e_N(x_1, \ldots, x_N), \ldots, e_n(x_1, \ldots, x_N))$.
Note that $e_N(x_1, \ldots, x_N)$ is equal to c if $f_N(x_1, \ldots, x_N, a_{N+1}, \ldots, a_n) = c$ for every $a_{N+1}, \ldots, a_n$, and $e_N(x_1, \ldots, x_N) = 2$ otherwise.
It remains to apply h_0 to $(x_1, \ldots, x_n, f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$ and $\alpha(x_1, \ldots, x_N)$ to obtain a solution of the instance such that f_N doesn't depend on $x_{N+1}, \ldots, x_n$, which gives us a contradiction to the minimality of N over all solutions.

Future of the Chen Conjecture

The conservative case is a natural large class on which the Chen Conjecture holds.

Theorem

Let $\mathcal{B}$ be a finite relational structure expanded with all unary relation. Either QCSP($\mathcal{B}$) is in P, is NP-complete, or is Pspace-complete.

Can PGP and EGP be sensibly modified to make the Chen Conjecture "true"?

Is there a clear condition for co-NP-membership?

H*bert's Problems 1900-2019

Hubert's Problems 2019

1. Complexity of $\mathrm{QCSP}(\mathbb{N}; x = y \to y = z)$.
2. Complexity of 3-No-Rainbow.
3. Some nonsense.

Hubert's Problems 2019

1. Complexity of $\mathrm{QCSP}(\mathbb{N}; x = y \to y = z)$.
2. Complexity of 3-No-Rainbow.
3. Some nonsense.

Hubert 2 is solved by Zhuk!

Hubert 1 is in co-NP (I claim)!

Quest for Hubert 1