On the Complexity of Set CSPs

François Bossière - joint work with Manuel Bodirsky

LIX - Ecole Polytechnique

December 18, 2013

Constraint Satisfaction Problems

Informal definition of CSPs

- A CSP is a computational problem.
- The input consists of a finite set of variables and a finite set of constraints imposed on those variables.
- The task is to decide whether there is an assignment of values to the variables such that all the constraints are simultaneously satisfied.

Examples

- Is a propositional formula in CNF with at most three literals per clause satisfiable on $\{0, 1\}$?
- Is there a solution to a finite set of linear equations over $\mathbb{F}_2$?

Formalisation of *CSPs*

Preliminaries

- Given a signature τ, an atomic formula is of the form $R(\overline{x})$ with R a relation in τ.
- A primitive positive formula on a signature τ is of the form $\exists x_1 \ldots x_n(\phi_1(\overline{x}) \wedge \cdots \wedge \phi_k(\overline{x}))$ where all ϕ_i are atomic formulas.
- An homomorphism from a τ-structure Γ to a τ-structure Δ is a map which preserves all atomic formulas.

Formal definition of *CSPs*

- Given a structure Γ on a finite relational signature τ, we define the computational problem CSP(Γ):
  - **Input**: a primitive positive sentence ϕ.
  - **Question**: $\Gamma \models \phi$?
- Equivalently:
  - **Input**: a finite τ-structure Δ.
  - **Question**: Is there an homomorphism from Δ to Γ?

Formal definition of *CSPs*

- Given a structure Γ on a finite relational signature τ, we define the computational problem CSP(Γ):
  - **Input**: a primitive positive sentence ϕ.
  - **Question**: $\Gamma \models \phi$?
- Equivalently:
  - **Input**: a finite τ-structure Δ.
  - **Question**: Is there an homomorphism from Δ to Γ?

- The domain of the structure Γ can be either finite, or infinite.
- Many computational problems can be modelled as CSPs.
- **Natural question**: what is the complexity of CSP(Γ) for a given Γ?

Formal definition of *CSPs*

- Given a structure Γ on a finite relational signature τ, we define the computational problem CSP(Γ):
  - **Input**: a primitive positive sentence ϕ.
  - **Question**: $\Gamma \models \phi$?
- Equivalently:
  - **Input**: a finite τ-structure Δ.
  - **Question**: Is there an homomorphism from Δ to Γ?

- The domain of the structure Γ can be either finite, or infinite.
- Many computational problems can be modelled as CSPs.
- **Natural question**: what is the complexity of CSP(Γ) for a given Γ?

Important property

For any relation R pp-definable on a structure Γ, CSP(Γ) and CSP(Γ, R) are polynomial-time equivalent.

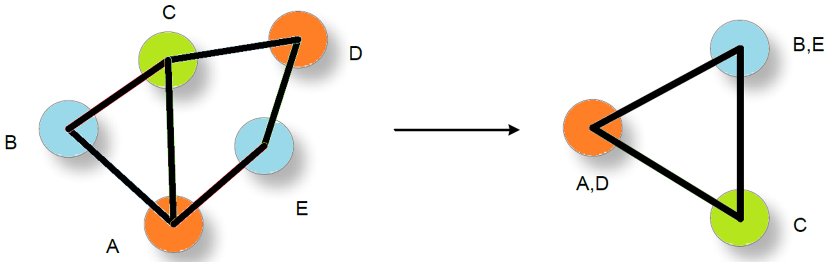
Example: 3-colorability

The famous problem...

- 3-colorability
  - ◇ **Input**: a finite graph G.
  - ◇ **Question**: can the vertices be colored with three colors such that no two vertices adjacent in G get the same color?

... can be formulated as a CSP with a finite structure:

- CSP(K_3):
  - ◇ **Input**: a finite graph G.
  - ◇ **Question**: is there a homomorphism from G to K_3?



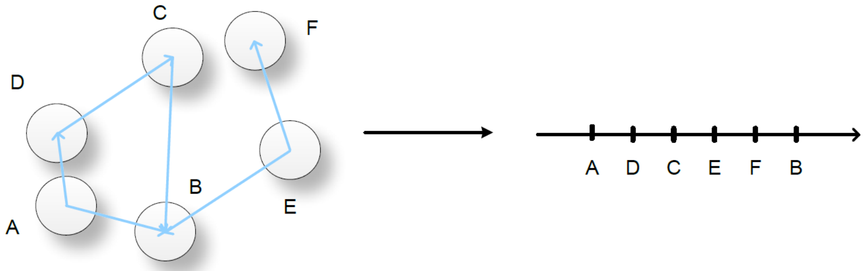
Example: Directed Graph Acyclicity

The famous problem...

- Directed Graph Acyclicity
  - **Input**: a finite directed graph G.
  - **Question**: is G acyclic?

... can be formulated as a CSP with an infinite structure:

- CSP$(\mathbb{Q}, <)$:
  - **Input**: a finite directed graph G.
  - **Question**: is there a homomorphism from G to $(\mathbb{Q}, <)$?



Dichotomy for finite Structures

- Schaefer'77: for any 2-element structure Γ, CSP(Γ) is either polynomially solvable or NP-complete.

Conjecture

Feder-Vardi'93 (**conjecture**): this dichotomy holds for every finite structure Γ.

- Bulatov'03: confirmed Feder-Vardi's conjecture for domains of size 3.
- Markovic'12: confirmed for domains of size 4 (announced but not published yet).
- The conjecture is already open for domains of size ≥ 5.

Dichotomy for finite Structures

- Schaefer'77: for any 2-element structure Γ, CSP(Γ) is either polynomially solvable or NP-complete.

Conjecture

Feder-Vardi'93 (**conjecture**): this dichotomy holds for every finite structure Γ.

- Bulatov'03: confirmed Feder-Vardi's conjecture for domains of size 3.
- Markovic'12: confirmed for domains of size 4 (announced but not published yet).
- The conjecture is already open for domains of size ≥ 5.
- What about infinite structures?

Infinite Structures

Non-Dichotomy

- Bodirsky-Grohe'08: Every computational decision problem is polynomial-time equivalent to a CSP with an infinite template.
- Ladner'75: if $P \neq NP$, there are NP-intermediate computational decision problems, i.e., problems in NP that are neither polynomial-time tractable nor NP-complete.
- Consequently: no dichotomy for CSPs on infinite structures.

Infinite Structures

Non-Dichotomy

- Bodirsky-Grohe'08: Every computational decision problem is polynomial-time equivalent to a CSP with an infinite template.
- Ladner'75: if P $\neq$ NP, there are NP-intermediate computational decision problems, i.e., problems in NP that are neither polynomial-time tractable nor NP-complete.
- Consequently: no dichotomy for CSPs on infinite structures.

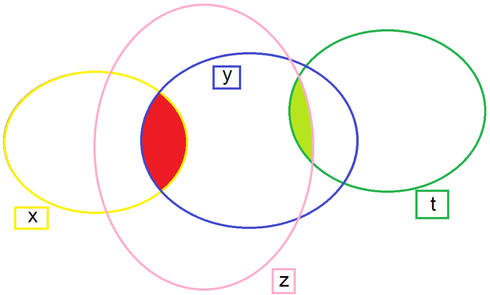
Question

Can we identify large natural classes of CSPs on infinite structures whose complexity can be classified?

More examples of CSPs: We denote by $\mathcal{P}(\mathbb{N})$ **the power set of** $\mathbb{N}$.

$\rightsquigarrow$ CSP$(\mathcal{P}(\mathbb{N}), x \cap y \subseteq z, x \not\subseteq y, x \parallel y)$ where $\parallel$ states for disjointness.

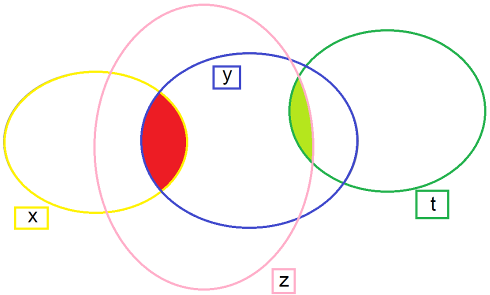
- **Ex. of input**: $(x \cap y \subseteq z) \wedge (t \not\subseteq z) \wedge (t \parallel x) \wedge (t \cap z \subseteq y)$
- **Answer**: yes, there is a solution.



More examples of CSPs: We denote by $\mathcal{P}(\mathbb{N})$ **the power set of** $\mathbb{N}$.

$\leadsto$ CSP$(\mathcal{P}(\mathbb{N}), x \cap y \subseteq z, x \not\subseteq y, x \parallel y)$ where $\parallel$ states for disjointness.

- **Ex. of input**: $(x \cap y \subseteq z) \wedge (t \not\subseteq z) \wedge (t \parallel x) \wedge (t \cap z \subseteq y)$
- **Answer**: yes, there is a solution.



$\leadsto$ CSP$(\mathcal{P}(\mathbb{N}), x \cap y = z, x \cup y = z, x \neq y)$

- **Ex. of input**:
  $(x \cap y = z) \wedge (x \cup y = t) \wedge (t \cap u = z) \wedge (u \cap x = x) \wedge (u \neq x)$
- **Answer**: No solution.

Generalities on set CSPs

- These problems belong to a large class of CSPs called set CSPs.

Informal definition

A set CSP is a CSP where the variables take as values subsets of the natural numbers. It is parametrized by the set of "boolean constraints" allowed in the input.

Generalities on set CSPs

- These problems belong to a large class of CSPs called set CSPs.

Informal definition

A set CSP is a CSP where the variables take as values subsets of the natural numbers. It is parametrized by the set of "boolean constraints" allowed in the input.

- Set CSPs appear naturally in various areas like program analysis (Kuncak-Nguyen-Rinard'06), knowledge representation (Küsters-Molitor'02), and spatial reasoning (Drakengren-Jonsson'97).
- Mariott-Odersky'96: all set CSPs are in NP.

Definition of a set CSP

Reducts

A reduct Γ of a structure Δ is a structure with a finite relational signature and whose relations are definable over Δ by a quantifier free formula.

Examples

Let $\mathfrak{B} = (\mathcal{P}(\mathbb{N}), \cap, \cup, \complement, \emptyset, \mathbb{N})$ be the Boolean algebra of the subsets of $\mathbb{N}$.

- $(\mathcal{P}(\mathbb{N}), \{(x, y) \mid x \cap y \neq x\}, \{(x, y) \mid x \cap y = \emptyset\})$ is a reduct of $\mathfrak{B}$.
- $(\mathcal{P}(\mathbb{N}), \{(x, y, z) \mid (x \cup y) \cap (\complement x \cup \complement y) = z\}$ as well.

Definition of a set CSP

Reducts

A reduct Γ of a structure Δ is a structure with a finite relational signature and whose relations are definable over Δ by a quantifier free formula.

Examples

Let $\mathfrak{B} = (\mathcal{P}(\mathbb{N}), \cap, \cup, \complement, \emptyset, \mathbb{N})$ be the Boolean algebra of the subsets of $\mathbb{N}$.

- $(\mathcal{P}(\mathbb{N}), \{(x,y) \mid x \cap y \neq x\}, \{(x,y) \mid x \cap y = \emptyset\})$ is a reduct of $\mathfrak{B}$.
- $(\mathcal{P}(\mathbb{N}), \{(x,y,z) \mid (x \cup y) \cap (\complement x \cup \complement y) = z\}$ as well.

Set Constraint Satisfaction Problems

A set CSP is a CSP for a reduct of $(\mathcal{P}(\mathbb{N}), \cap, \cup, \complement, \emptyset, \mathbb{N})$.

Examples

- $\mathrm{CSP}(\mathcal{P}(\mathbb{N}), \not\subseteq, \parallel, \neq)$ and $\mathrm{CSP}(\mathcal{P}(\mathbb{N}), \ominus, \neq)$ are set CSPs.

Conjecture

Every set CSP is either in P, or NP-complete.

Conjecture

Every set CSP is either in P, or NP-complete.

Universal algebraic approach

- For finite structures, the complexity of CSPs can be analysed using a *universal algebraic approach*.
- This approach was used by Bulatov'03 to confirm the Feder-Vardi conjecture for domains of size 3.
- The universal algebraic approach does not work in general for infinite structures, but it does if the structure has a strong model-theoretic property: *ω-categoricity*.

ω-categoricity

- A first-order theory is ω-categorical if all its countably infinite models are isomorphic.
- A structure is ω-categorical whenever its first-order theory is.

- **Fact**: A reduct of an ω-categorical structure is ω-categorical.

ω-categoricity

- A first-order theory is ω-categorical if all its countably infinite models are isomorphic.
- A structure is ω-categorical whenever its first-order theory is.

- **Fact**: A reduct of an ω-categorical structure is ω-categorical.

Examples

- Any finite structure is ω-categorical.
- The theory of every dense linear order is ω-categorical. Hence, $(\mathbb{Q}, <)$ and $(\mathbb{R}, <)$ are ω-categorical.
- $(\mathbb{Q}, \{(x, y, z) \in \mathbb{Q}^3 \mid (x < y < z) \vee (z < y < x)\})$ is ω-categorical since it is a reduct of $(\mathbb{Q}, <)$.
- The theory of any infinite vector space over a finite field is ω-categorical.

Important definitions

- A m-ary operation f preserves a n-ary relation R if for all n-tuples $\overline{x_1}, \cdots, \overline{x_m}$ in R, the n-tuple $(f(x_{1,i}, \cdots, x_{m,i}))_{1 \leq i \leq n}$ is again in R.
- f is called a polymorphism of a relational structure Γ if it preserves every relation of Γ.

$$\begin{array}{cccccccc}
 & & \overbrace{\phantom{x_{1,1}}}^{f} & \overbrace{\phantom{x_{1,2}}}^{f} & \overbrace{\phantom{x_{1,3}}}^{f} & & \overbrace{\phantom{x_{1,n}}}^{f} & \\
\overline{x_1} & = & x_{1,1} & x_{1,2} & x_{1,3} & \cdots & x_{1,n} & \in R \\
\overline{x_2} & = & x_{2,1} & x_{2,2} & x_{2,3} & \cdots & x_{2,n} & \in R \\
\vdots & & \vdots & \vdots & \vdots & & \vdots & \\
\overline{x_m} & = & x_{m,1} & x_{m,2} & x_{m,3} & \cdots & x_{m,n} & \in R \\
 & & \underbrace{\phantom{x_{m,1}}} & \underbrace{\phantom{x_{m,2}}} & \underbrace{\phantom{x_{m,3}}} & & \underbrace{\phantom{x_{m,n}}} & \\
 & & \| & \| & \| & & \| & \\
 & & z_1 & z_2 & z_3 & \cdots & z_n &
\end{array}$$

We denote by:

- $\mathrm{Pol}(\Gamma)$ the set of all polymorphisms of Γ.
- $\mathrm{Inv}(F)$ the set of all relations preserved by a set F of operations.
- $\langle\Gamma\rangle_{\mathrm{pp}}$ the set of all relations which are pp-definable over Γ.

Theorem - Geiger '68 & Bodirsky-Nesetril '03

For every countably infinite ω-categorical or finite structure Γ:

$$\mathrm{Inv}(\mathrm{Pol}(\Gamma)) = \langle\Gamma\rangle_{\mathrm{pp}}$$

Looking for better settings

- **Fact**: In general, a reduct of the Boolean algebra $\mathfrak{B}$ is not ω-categorical.
- **Question**: Can we formulate every set CSP as a CSP for an ω-categorical structure?
- **Answer**: Yes!

Looking for better settings

- **Fact**: In general, a reduct of the Boolean algebra $\mathfrak{B}$ is not ω-categorical.
- **Question**: Can we formulate every set CSP as a CSP for an ω-categorical structure?
- **Answer**: Yes!

Definition: An element x of a Boolean algebra is called an atom when there is no strictly smaller element than x other than 0.
Example: the singletons $\{n\}$ are the atoms of $(\mathcal{P}(\mathbb{N}), \cap, \cup, \complement, \emptyset, \mathbb{N})$.

Definition - The atomless Boolean algebra

There is a unique countable atomless Boolean algebra up to isomorphism. We denote it by $\mathfrak{A} = (A, \sqcap, \sqcup, c, 0, 1)$.

Key property

- For every reduct Γ of $\mathfrak{B}$, there exists a reduct Δ of $\mathfrak{A}$ which has the same CSP as Γ.
- Conversely, for every reduct Δ of $\mathfrak{A}$, there exists a reduct Γ of $\mathfrak{B}$ which has the same CSP as Δ.

Key property

- For every reduct Γ of $\mathfrak{B}$, there exists a reduct Δ of $\mathfrak{A}$ which has the same CSP as Γ.
- Conversely, for every reduct Δ of $\mathfrak{A}$, there exists a reduct Γ of $\mathfrak{B}$ which has the same CSP as Δ.

Consequences

- To solve the conjecture, we have to understand the complexity of $\mathrm{CSP}(\Gamma)$ for every reduct Γ of $\mathfrak{A}$.
- Since the complexity of a CSP does not change when adding pp-definable relations, and since $\mathrm{Inv}(\mathrm{Pol}(\Gamma)) = \langle \Gamma \rangle_{\mathrm{pp}}$, the complexity of $\mathrm{CSP}(\Gamma)$ is determined by $\mathrm{Pol}(\Gamma)$.
- Classify the complexity of set CSPs $\Leftrightarrow$ understand the polymorphisms of reducts of $\mathfrak{A}$.

Automorphisms

Starting by classifying the automorphisms

- Automorphisms are special polymorphisms.
- The classification of automorphism groups of reducts is an important topic in the theory of ω-categorical structures.
- Such a classification has been done for $(\mathbb{Q}, <)$ (Cameron'89), the random Graph (Thomas'91), the random Poset (P^4-Sz'13), etc...

Automorphisms

Starting by classifying the automorphisms

- Automorphisms are special polymorphisms.
- The classification of automorphism groups of reducts is an important topic in the theory of ω-categorical structures.
- Such a classification has been done for $(\mathbb{Q}, <)$ (Cameron'89), the random Graph (Thomas'91), the random Poset (P^4-Sz'13), etc...
- For the atomless Boolean algebra $\mathfrak{A}$, the classification of the automorphism groups of reducts is still to be done.
- We give such a classification for an important reduct of $\mathfrak{A}$: the countably infinite vector space over $\mathbb{F}_2$.

The countably infinite vector space over $\mathbb{F}_2$

Definition

- There is a unique countably infinite vector space over $\mathbb{F}_2$, up to isomorphism.
- It is isomorphic to the reduct $(A, +)$ of $\mathfrak{A}$, where $+$ corresponds to the symmetric difference of sets.
- **Formally**: $+(x, y, z)$ if and only if $(x \sqcup y) \sqcap (c(x) \sqcup c(y)) = z$.

Partial classification

Theorem - Bodirsky-B.'13

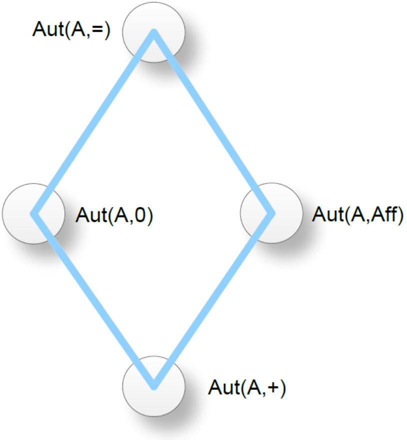
Let Γ be a reduct of $(A, +)$, then:

- either $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(A, +)$
- either $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(A, \mathrm{Aff})$
- either $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(A, 0)$
- or $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(A, =)$

where $\mathrm{Aff} = \left\{(x, y, z, t) \in A^4 \mid x + y = z + t\right\}$.

Example: consider the relation Eq_4 consisting of all tuples (x, y, z, t) such that $x + y = z + t$ and $(x, y, z), (x, z, t), (y, z, t)$ are a free families of $(A, +)$. The automorphism group of (A, Eq_4) is $\mathrm{Aut}(A, +)$.

Automorphism groups of the reducts of $(A, +)$



We believe that the proof techniques for our result are useful also to study polymorphisms of reducts of $(A, +)$.

Sketch of proof

- Graham-Leeb-Rothschild'72: the countably infinite vector space over $\mathbb{F}_2$ has a strong combinatorial property called *Ramsey property*.
- **Main idea**: we use Ramsey theory to prove that automorphisms are *canonical* on large subsets of the domain.

Sketch of proof

- Graham-Leeb-Rothschild'72: the countably infinite vector space over $\mathbb{F}_2$ has a strong combinatorial property called *Ramsey property*.
- **Main idea**: we use Ramsey theory to prove that automorphisms are *canonical* on large subsets of the domain.
- A function $f : A \to A$ is called canonical if for all $a_1, \ldots, a_n \in A$, the model-theoretic type of $(f(a_1), \ldots, f(a_n))$ only depends on the model-theoretic type of $(a_1, \ldots, a_n)$.
- **Example**: let $(a_i)_{i\in\mathbb{N}}$ be an enumeration of A and $(b_i)_{i\in\mathbb{N}}$ be a basis of $(A, +)$. The map $\mathrm{gen} : A \to A$ such that $\mathrm{gen}(a_i) = b_i$ is canonical.

Sketch of proof

- Graham-Leeb-Rothschild'72: the countably infinite vector space over $\mathbb{F}_2$ has a strong combinatorial property called *Ramsey property*.
- **Main idea**: we use Ramsey theory to prove that automorphisms are *canonical* on large subsets of the domain.
- A function $f: A \to A$ is called canonical if for all $a_1, \ldots, a_n \in A$, the model-theoretic type of $(f(a_1), \ldots, f(a_n))$ only depends on the model-theoretic type of $(a_1, \ldots, a_n)$.
- **Example**: let $(a_i)_{i\in\mathbb{N}}$ be an enumeration of A and $(b_i)_{i\in\mathbb{N}}$ be a basis of $(A, +)$. The map $\mathrm{gen}: A \to A$ such that $\mathrm{gen}(a_i) = b_i$ is canonical.
- We write $f \sim g$ if for all $a_1, \ldots, a_n \in A$, the type of $(f(a_1), \ldots, f(a_n))$ and the type of $(g(a_1), \ldots, g(a_n))$ are the same. Note that $\sim$ is an equivalence relation.
- We prove that $(A, +)$ has nine canonical functions modulo $\sim$.
- We climb the automorphism groups lattice step by step, producing canonical functions and performing at each step a case distinction.

Perspectives

Open problems:

- Classify the polymorphisms of reducts of the countably infinite vector space over $\mathbb{F}_2$.
- Classify the automorphism groups of reducts of the atomless Boolean algebra.
- Finally: classify the polymorphisms of reducts of the atomless Boolean algebra and obtain a complexity classification of all set CSPs.

Thank you!