Algorithms and Complexity of Constraint Satisfaction Problems (course number 8)

Nicolas (Miki) Hermann

LIX, École Polytechnique

hermann@lix.polytechnique.fr
**CSP on finite domains**

<table>
<thead>
<tr>
<th>Question 1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What about CSP on finite domains</strong> $D = {0, \ldots, n - 1}$ where $</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is a large and not much explored area, but also a difficult subject.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What remains valid and what changes with respect to Boolean CSP?</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Galois correspondence and the identities $\text{Inv Pol } S = \langle S \rangle$ and $\text{Pol Inv } F = [F]$ remain valid, but not much else is transmitted from Boolean CSP to CSP over finite domains.</td>
</tr>
</tbody>
</table>
Post lattice is infinite, but countable. On the other hand, the equivalent of Post lattice for finite domains of cardinality $n > 2$ are not countable. The proof for $n = 3$ follows. Its generalization to superior cardinalities is obvious.
Lemma

Let $D = \{0, 1, 2\}$. For each $k \geq 1$, let $f_k$ be the function of arity $k$ over $D$ such that

$$f_k(a_1, \ldots, a_k) = \begin{cases} 1 & \text{if } \exists i (a_i = 1) \land \forall j (j \neq i \rightarrow a_j = 0), \\ 2 & \text{otherwise.} \end{cases}$$

For each $p \geq 1$, let $R_p$ be the relation of arity $p$ over $D$ such that

$$R_p = \{(a_1, \ldots, a_p) \in D^p \mid \exists i (a_i = 1) \land \forall j (j \neq i \rightarrow a_j = 0)\} \cup \{(a_1, \ldots, a_p) \in D^p \mid \exists i (a_i = 2)\}$$

Then $f_k \in \text{Pol } R_p$ if and only if $k \neq p$. 
Proof.

If $k = p$, consider the relation $M$ of arity and cardinality $k$ which corresponds to the rows of the identity matrix $I_k$. It is clear that $M \subseteq R_k$, but $f_k(M) \notin R_k$.

If $k \neq p$, let $M$ be an arbitrary relation over $D$ of arity $p$ and of cardinality $k$. If one of the vectors $m_1, \ldots, m_k \in M$ contains the value 2, then the vector $f_k(m_1, \ldots, m_k)$ also contains the value 2 and therefore $f_k(m_1, \ldots, m_k) \in R_p$. Suppose that each of the vectors $m_1, \ldots, m_k \in M$ contains only the values 0 and 1. If $\{m_1, \ldots, m_k\} \subseteq R_p$ then the vector $(m_1[j], \ldots, m_k[j])$ contains exactly one value 1 and the others are the values 0, for each $j = 1, \ldots, p$. Given that $k \neq p$, there exists a vector $m_i \in M$ which contains either more values 1, or it does not contains any (vector $0 \cdots 0$). This implies that one of the values of $f_k(m_1, \ldots, m_k)$ is equal to 2. Therefore $f_k(M) \in R_p$. 

$\square$
The lattice of clones over the domain $D = \{0, 1, 2\}$ is not countable.

Proof.

Let $f_k$ be the function and $R_p$ the relation defined in the previous Lemma. For each $I \subseteq \mathbb{N}$, let $C_I = [F_I]$ be the clone generated by the set of functions $F_I = \{ f_k \mid k \in I \}$. Hence we have $f_k \in C_I$ if and only if $k \in I$. One of the implications is trivial. For the other, suppose that $k \notin I$. Hence for each $f \in [F_I]$ we have $f(R_k) \subseteq R_k$. Therefore $f_k \notin C_I$ holds. For each couple of subsets $I, J \subseteq \mathbb{N}$ such that $I \neq J$, we have $C_I \neq C_J$. Given that there exists an uncountable number of subsets of $\mathbb{N}$, there exists an uncountable number of clones over the domain $D = \{0, 1, 2\}$.

Remark

Despite of this result, we can always hope to have a characterization by finite bases, but the situation is even worse.
**Theorem**

Let $D$ be a domain of cardinality $|D| > 2$. There exist clones of functions over $D$ which do not contain a finite basis.

**Proof.**

Let $f_i$ be the function defined in the previous Lemma and

$$F = \{ f_i \mid i \in \mathbb{N}^{++} \}$$

where $\mathbb{N}^{++} = \mathbb{N} \setminus \{0, 1\}$. Hence $F$ contains neither a unary function nor a constant. We will show that the infinite set $F$ is the basis of the clone $[F]$.

Let $h(x_1, \ldots, x_r) = f_k(\varphi_1, \ldots, \varphi_k)$ a new function $h \in [F]$ constructed from the functions $F$. 

.../...
Proof (cont).

Recall that \( h(x_1, \ldots, x_r) = f_k(\varphi_1, \ldots, \varphi_k), \ k \geq 2 \) and

\[
f_k(a_1, \ldots, a_k) = \begin{cases} 
1 & \text{if } \exists i(a_i = 1) \land \forall j(j \neq i \rightarrow a_j = 0), \\
2 & \text{otherwise.}
\end{cases}
\]

If at least two formulas \( \varphi_i \) are not variables, then \( h \equiv 2 \), because there exist two indices \( i \neq j \) such that \( \varphi_i, \varphi_j \in \{1, 2\} \). Hence \( h \notin F \).

If only one of the formulas \( \varphi_i \) is not a variable and \( k \geq 2 \), there exists \( j \neq i \) with \( \varphi_j = y_j \) where \( y_j \in \{x_1, \ldots, x_r\} \). Substituting \( y_j = 1 \) and \( x = 0 \) for each variable \( x \in \{x_1, \ldots, x_r\} \setminus \{y_j\} \) in \( h(x_1, \ldots, x_r) \), this function will have the value 2. Therefore \( h \notin F \).

If all formulas \( \varphi_i \) are variables and \( k > r \), there exist two indices \( i \neq j \) such that \( \varphi_i = \varphi_j = y \) for \( y \in \{x_1, \ldots, x_r\} \). Substituting \( y = 1 \) and \( x = 0 \) for each variable \( x \in \{x_1, \ldots, x_r\} \setminus \{y\} \), the function \( h(x_1, \ldots, x_r) \) will have the value 2. Therefore \( h \notin F \).
Bases of clones in uncountable lattices

Proof.
We have proved that we can never construct other functions $f_i$ by composition and variable identification from the subset of functions $F$. Therefore the infinite set of functions $F$ is the basis of the clone $[F]$.

Consequence
If $S \subseteq D^k$ is a relation over a non-boolean domain and $\text{Pol} S$ is a clone with an infinite basis, we have no finite characterization for $S$.

Remark
We can hope now to have a possibility to finitely describe infinite bases, but there is worse.
Theorem

Let $D$ be a domain of cardinality $|D| > 2$. There exist clones of functions over $D$ which have no basis.

Proof.

Let $D = \{0, 1, 2\}$. Let $f_0 = 2$ and for each $k \geq 1$, let $f_k$ be the function of arity $k$ over $D$ such that

$$f_k(a_1, \ldots, a_k) = \begin{cases} 1 & \text{if } a_1 = \cdots = a_k = 0, \\ 2 & \text{otherwise.} \end{cases}$$

Let $F = \{f_i \mid i \in \mathbb{N}\}$. We can never produce another function $f_i$ by composition from a subset of functions $F$, because each composition of functions $F$ produces the constant function equal to 2. On the other hand, from the function $f_i$ we can construct all functions $f_j$ for $j < i$ by variable identification.

.../...
Proof.

Suppose that the clone \([F]\) has a basis. Hence this basis contains a function \(g\) produced from the function \(f_{k_0} \in F\) with minimal index \(k_0\) among all functions in the basis.

There are two possibilities:

1. The basis contains another function \(g'\). This function was constructed from the function \(f_{k_1} \in F\) where \(k_1 > k_0\). Alas \(f_{k_0}\) can be constructed from \(f_{k_1}\) by variable identification. Therefore the function \(g\) can be composed from function \(g'\), which is a contradiction with the definition of a basis.

2. The basis is composed from a single function \(g\). In this case, no function \(f_k\) for \(k > k_0\) can be constructed from the function \(g\), since each composition of the function \(f_{k_0}\) with itself constructs the constant function equal to 2, which is once more a contradiction.
Hypothesis

Do the clones used for the characterization of the frontier between the polynomial-time decidable and NP-complete cases have a finite basis?
Minimal non-trivial clones

Maybe we do not need to know all clones, but only the trivial clone $I_2$ and the minimal non-trivial clones.

Theorem (Rosenberg, 1983)

Let $D$ be a finite domain of cardinality $k$. The number of minimal non-trivial clones is finite for each $k \geq 3$.

Number of minimal non-trivial clones

However, the number of minimal non-trivial clones grows fast.

- For $k = 2$ there are 7 minimal non-trivial clones $I_0, I_1, N_2, E_2, V_2, L_2$ and $D_2$.
- For $k = 3$ Csákány enumerated all minimal non-trivial clones: they are 84, 24 principals and the rest are duals!
- For $k \geq 4$ only an approximative characterization is known.
For $k \geq 3$, the minimal non-trivial clones are insufficient for complexity classification.

**Example**

Let $D = \{r, g, b\}$ and $\text{Perm}$ be the set of all permutations over $D$. It is clear that $\text{Perm}$ is a clone, since the projections are permutations and composition of permutations is a permutation. The clone $\text{Perm}$ is not a minimal non-trivial clone (Csákány).

The relation $3\text{col} = \{rg, rb, gr, gb, br, bg\}$ belongs to $\text{Inv(Perm)}$, since the inclusion $\pi(3\text{col}) \subseteq 3\text{col}$ is valid for each permutation $\pi \in \text{Perm}$. Therefore $\text{Perm}$ is a characterization of NP-complete CSP.
Minimal non-trivial clones

**Advantage**

The clone \( \text{Perm} \) has a finite basis by the functions \( x + 1 \mod 3 \) and \( \{0 \mapsto 1, 1 \mapsto 0, 2 \mapsto 2\} \). The structure of the lattice between \( \text{Perm} \) and the clone \( \Omega_3 \) of all functions over \( D \) with \( |D| = 3 \) is known. Moreover, this sublattice is finite.

**Drawback**

This is only a small portion of the lattice.
At the end of 1990s, Feder and Vardi published a challenge to prove or refute the following hypothesis:

**Hypothesis**

Let $D$ be a finite domain. For each set of relations $S$ over $D$, the problem $\text{CSP}(S)$ is either NP-complete or polynomial-time decidable.

**Status of this hypothesis**

- $|D| = 2$: Solved by Schaefer’s Dichotomy Theorem. Positive answer.
- $|D| = 3$: Bulatov presented a complicated proof in 2002 with 10 polynomial cases, the rest is NP-complete.
- $|D| > 3$: Some work of Jeavons et co. on the closure properties are known, but we have very few information in general.
Closure properties of constraints

Definition

Let $f : D^k \rightarrow D$ be a function of arity $k$ over the domain $D$. The function $f$ is a

- **semi-lattice** operation if $f$ is binary ($k = 2$) and it satisfies the following three identities:
  - idempotence: $f(x, x) = x$
  - commutativity: $f(x, y) = f(y, x)$
  - associativity: $f(f(x, y), z) = f(x, f(y, z))$

- **near unanimity** operation if $k \geq 3$ and it satisfies the following identities:
  \[
  f(y, x, \ldots, x) = f(x, y, x, \ldots, x) = \cdots = f(x, \ldots, x, y) = x
  \]

- **Mal'tsev** operation if it is ternary ($k = 3$) and satisfies the following identities:
  \[
  f(x, y, y) = f(y, y, x) = x
  \]

- **conservative** operation if $f(x_1, \ldots, x_k) \in \{x_1, \ldots, x_k\}$ for each $x_i$. 

Definition

Let $f : D^k \rightarrow D$ be a function of arity $k$ over a domain $D$. The function $f$ is a

- **essentially unary** operation if $f$ is not constant, there exists a unary function $g$ and a coordinate $i \in \{1, \ldots, k\}$ which satisfy the following identity:

$$f(x_1, \ldots, x_k) = g(x_i)$$

- **majority** operation if it is ternary ($k = 3$) and it satisfies the following identities:

$$f(x, x, y) = f(x, y, x) = f(y, x, x) = x$$

- **affinity** operation if it is ternary ($k = 3$) and it satisfies the identity

$$f(x, y, z) = x - y + z$$

where $+$ and $-$ are operations of a commutative group $(D, +, -)$. 
Relations between different types of functions

Theorem

Each affinity operation is a Mal’tsev operation.
Each majority operation is a near unanimity operation.
**Definition**

Let $f : D^k \to D$ be a function of arity $k$ over the domain $D$. The function $f$ is a semi-projection if $k \geq 3$ and there exists a coordinate $i \in \{1, \ldots, k\}$, such that the identity $f(x_1, \ldots, x_k) = x_i$ is satisfied if there exist indices $j$ and $\ell$ where $x_j = x_\ell$ is satisfied.

**Alternative definition**

In other words, $f$ is a semi-projection if there exists a coordinate $i$ such that for each $d_1, \ldots, d_k \in D$ with $|\{d_1, \ldots, d_k\}| < k$, we have $f(d_1, \ldots, d_k) = d_i$. 
Caracterization of clones

Theorem (Rosenberg, 1965)

Let $S$ be a set of relations over the domain $D$. The clone $\text{Pol } S$ contains
- either only essentially unary functions,
- or a function $f$ which is
  - constant, or
  - a majority function, or
  - an idempotent binary function which is not a projection, or
  - an affine function, or
  - a semi-projection.
Theorem

Let $S$ be a set of relations over the domain $D$. If the clone $\text{Pol} S$ contains only essentially unary functions then $\text{CSP}(S)$ is NP-complete.
Partial characterization of $\text{CSP}(S)$

Proof.

Let $|D| = n$ and

$$n\text{COL} = \{(d_1, \ldots, d_n) \in D^n \mid (d_i = d_j) \rightarrow (i = j)\}.$$ 

Each essentially unary function $f$ is either a permutation, or it is injective. If $f$ is a permutation then $f(n\text{COL}) = n\text{COL}$ and $\text{CSP}(n\text{COL})$ is NP-complete for $n \geq 3$. For $n = 2$, the negation $\neg$ and the identity $\text{id}$ are permutations.

If $f$ is not injective then $|f(D)| < |D|$. Now

- either $\text{CSP}(f(S))$ is NP-complete, which implies that $\text{CSP}(S)$ is NP-complete, too,

- or we can recursively go from $\text{CSP}(S)$ to $\text{CSP}(f(S))$. This step can be iterated only finitely many times.

Hence, at the end $\text{CSP}(f^k(S))$ is either NP-complete or $f^k(S)$ is closed under a non-unary function. The latter is a contradiction with the assumption.

}\hfill\square
Theorem

Let $S$ be a set of relations over the domain $D$. If a clone $\text{Pol} S$ contains one of the following functions:

- constant (generalization of 0 and 1)
- semi-lattice (gen. of $\land$ and $\lor$)
- near unanimity (gen. of majority $\text{maj}$)
- Mal’tsev (gen. of affinity $\text{aff}$)
- binary commutative conservative

then $\text{CSP}(S')$ is decidable in polynomial time.

Remark

Compare the two previous theorems with Schaefer’s Dichotomy Theorem.
Semi-projections

**Theorem**

For each finite domain $D$ with $|D| \geq 3$ there exists a relation $R$ over $D$, such that $R$ is closed under all semi-projections over $D$ and $\text{CSP}(R)$ is NP-complete.

**Proof.**

Let $d_0, d_1 \in D$. Let

$$R = \{(d_0, d_0, d_1), (d_0, d_1, d_0), (d_1, d_0, d_0)\}.$$

The homomorphism $h : D \rightarrow \{0, 1\}$ with $h(d_0) = 0$ and $h(d_1) = 1$ constructs the relation $h(R) = 1\text{-in-3}$. If $\text{CSP}(h(R))$ is NP-complete then $\text{CSP}(R)$ is NP-complete, too. □
Work during internship continued in PhD ...
Approximation problem of CSP

Problem \textsc{MAXCSP}(S)

\textit{Input}: Finite set of constraints \( C = \{R_1(\vec{x}_1), \ldots, R_p(\vec{x}_p)\} \) over \( D \) and \( V \), where \( R_j \in S \) for each \( j \).

\textit{Output}: Maximal number of satisfied constraints among \( C \).

Situation

Partial results by Krokhin, Johnson and co.
Approximation problem of CSP

**Problem APX(S)**

*Input:*

Finite set of constraints $C = \{R_1(\vec{x}_1), \ldots, R_p(\vec{x}_p)\}$ over $D$ and $V$, where $R_j \in S$ for each $j$ and where each solution $m$ of $C$ has a value $w(m) \in \mathbb{R}^+$.

*Question:* Is the optimal solution (max or min) approximable in polynomial time by a constant?

**Situation**

| $|D| = 2$: Complete solution by Creignou in 1995. |
| $|D| > 2$: No result. |
Approximation ratio of CSP

**Problem** \textsc{Ratio}(S)

*Input:* Finite set of constraints $C = \{R_1(\vec{x}_1), \ldots, R_p(\vec{x}_p)\}$ over $D$ and $V$, where $R_j \in S$ for each $j$ and where each solution $m$ of $C$ has a value $w(m) \in \mathbb{R}^+$.  

*Output:* Best polynomial approximation ratio of the optimal solution.

**Situation**

$|D| = 2$: Partial result of Zwick.

$|D| > 2$: No result.
Ordered domain and minimal models

**Definition**

Let the domain $D = \{0, \ldots, n - 1\}$ be ordered by $<$, where $0 < 1 < \cdots < n - 2 < n - 1$. Partial order $\prec$ over the tuples of $D^k$ is defined by

$$m \prec m'$$

if

- $m \neq m'$,
- $m[i] \leq m'[i]$ for each $i \in \{1, \ldots, k\}$.

The relation $m \preceq m'$ means $m \prec m'$ or $m = m'$.

**Definition**

A **minimal model** of $R(x_1, \ldots, x_k)$ is a tuple $m \in R$ such that each $m' \in R$ satisfies $m \preceq m'$ or $m$ and $m'$ are incomparable.
**Problem** \textsc{mininf}(S)

**Input:** Finite set of constraints \( C = \{R_1(\vec{x}_1), \ldots, R_p(\vec{x}_p)\} \) over \( D \) and \( V \), where \( R_j \in S \) for each \( j \), and a constraint \( R(\vec{x}) \).

**Question:** Is the constraint \( R(\vec{x}) \) satisfiable by every minimal model of \( C \)?

**Difficulty**

The notion of minimality is incompatible with existential quantification.

**Situation**

\( |D| = 2 \): Result of Durand, H. and Nordh (5 years of work) for unbounded arity of \( R \), using results of Kirousis and Kolaitis.

\( |D| > 2 \): No result.
### Problem \#\text{CIRC}(S)

**Input:** Finite set of constraints $C = \{R_1(\vec{x}_1), \ldots, R_p(\vec{x}_p)\}$ over $D$ and $V$, where $R_j \in S$ for each $j$.

**Output:** Number of minimal models of $C$.

### Situation

- $|D| = 2$: Partial result of Durand, H. and Kolaitis.
- $|D| > 2$: No result.
**Problem** \( \text{GENCSP}(S, O) \)

**Input:** Formula \( \varphi \) constructed from atomic constraints \( R(\vec{x}) \) over the relations \( R \in S \) using the operations \( O \).

**Question:** Is the formula \( \varphi \) satisfiable?

**Situation**

\( O = \{ \exists, \land \} \): CSP classic

\( O = \{ \exists, \land, \lor, = \} \): Solved recently by H. and Richoux (finite domains), as well as by Bodirsky, H. and Richoux (infinite case).

Other configurations of \( O \): No result.

**Particularly interesting configurations of \( O \)**

\( \{ \text{maj} \} \), \( \{ \text{maj}, = \} \) — satisfiability of the majority of constraints

\( \{ \oplus \} \) — satisfaction of odd number of constraints
Other variants of CSP

- fuzzy CSP
- CSP generated by equalities between finite functions
- randomized CSP
- CSP with different structure
- up to your imagination . . .
Partial exam will take place on 4 december 2012, 17:45 — 19:15.

Good luck!