Algorithms and Complexity of Constraint Satisfaction Problems (course number 4)

Nicolas (Miki) Hermann

LIX, École Polytechnique

hermann@lix.polytechnique.fr
Another characterization of bijunctive constraints

**Definition**

A function $f : D^k \to D$ of arity $k$ over domain $D$ is called a **near unanimity** if $k \geq 3$ and it satisfies the following identities:

$$f(y, x, \ldots, x) = f(x, y, x, \ldots, x) = \cdots = f(x, \ldots, x, y) = x.$$ 

**Majority** is near unanimity for $k = 3$.

**Theorem (Baker, Pixley (1975))**

Let $(A; F)$ be a finite algebra with a polynomial $m(x_1, \ldots, x_{d+1}) \in [F]$ that satisfies the near unanimity identities. Then for any positive integer $n$, a function $f : A^n \to A$ is a (polynomial) function from $[F]$ if and only if every subalgebra of $A^d$ is closed under $f$. 
Another characterization of bijunctive constraints

**Corollary (Jeavons (1997))**

Given an \( n \)-ary bijunctive constraint \( R(x_1, \ldots, x_n) \) then it is equivalent to

\[
\bigwedge_{1 \leq i \leq j \leq n} R_{ij}(x_i, x_j)
\]

where \( R_{ij} \) is the projection of the relation \( R \) to the coordinates \( i \) and \( j \).

**Proof.**

Apply Baker-Pixley with \( d = 2 \).
The notion of closure of relations under functions was established in general for any (finite) domain $D$.

**Definition**

Let $f : D^p \rightarrow D$ be a function of arity $p$. A relation $R \subseteq D^k$ of arity $k$ is closed under the function $f$ (we also say that $f$ is a polymorphism of $R$) if for each choice of $p$ not necessarily distinct vectors $m_1, \ldots, m_p \in R$ we have

$$(f(m_1[1], \ldots, m_p[1]), \ldots, f(m_1[k], \ldots, m_p[k])) \in R.$$ 

In other words, the new vector constructed coordinatewise from the chosen vectors $m_1, \ldots, m_p$ by the function $f$ belongs to the relation $R$. 
Attention

The arities of the function $f$ and of the relation $R$ are different and perpendicular! Visualize the vectors $m_1, \ldots, m_p$ in the form of a matrix of size $p \times k$ and apply the function $f$ on columns.

\[
\begin{array}{ccc}
  f & \cdots & f \\
  \downarrow & & \downarrow \\
  m_1 &=& (m_1[1], \ldots, m_1[k]) \in R \\
  \vdots & & \vdots \ \\
  m_p &=& (m_p[1], \ldots, m_p[k]) \in R \\
  \parallel & & \parallel \\
  f(m_\perp) &=& (m[1], \ldots, m[k]) \in R \\
\end{array}
\]
Let $R \subseteq D^k$ be a relation. We will investigate the set of all functions $f$ under which the relation $R$ is closed. This will be the characterization of the relation $R$.

**Definition**

Let $R$ be a relation and $S$ a set of relations not necessarily of same arity.

- $\text{Pol } R$ is the set of all functions which are the polymorphisms of $R$.
- $\text{Pol } S$ is the set of all functions which are the polymorphisms for each relation $R \in S$. 

... and if we reverse the characterization?

Let $F$ be a set of functions, not necessarily of same arity. We will investigate the set of all relations closed under the functions $F$.

**Definition**

Let $F$ be a set of functions, not necessarily of same arity. The set of invariants $\text{Inv } F$ contains all relations closed under each function $f \in F$.

**Attention**

The set $F$ is not necessarily finite.
We identified two characterization problems of boolean relations on previous slides.

**Question 1**
Given a set of boolean relations $S$, identify the set of its polymorphisms $\text{Pol } S$.

**Question 2**
Given a set of boolean functions $F$, identify the set of its invariants $\text{Inv } F$.

**Answers**
To be able to give an adequate answer, we need to study sets of boolean functions.
If we have two boolean functions

\[ bor_0(x, y) = (x \lor y) \quad \text{and} \quad not(x) = \neg x \]

we can construct a new function

\[ bor_1(x, y) = (x \lor \neg y) \]

by composition \( bor_0(x, not(y)) \).

This way, we can construct the majority function from conjunction 
\( and(x, y) = (x \land y) \) and disjunction \( or_0(x, y, z) = (x \lor y \lor z) \):

\[
\text{maj}(x, y, z) = or_0(and(x, y), and(y, z), and(z, x)) \\
= (x \land y) \lor (y \land z) \lor (z \land x)
\]
Exercise 9

Construct the function

$$\text{aff}(x, y, z) = x + y + z \pmod{2}$$

from the functions $\text{and}(x, y) = (x \land y)$ and $\text{not}(x) = \neg x$.

Construct the function $\text{and}(x, y)$ from the functions $\text{bor}_0(x, y) = (x \lor y)$ and $\text{not}(x)$.

Construct the function $\text{bor}_0(x, y)$ from the functions $\text{aff}(x, y, z)$ and $\text{and}(x, y)$. 

Rules for constructing functions

Definition

Let $B$ be a set of functions not necessarily of same arity. The set $[B]$ contains all functions constructed from $B$. The set $[B]$ is constructed by saturation:

Introduction: If $f(\bar{x}) \in B$ then $f(\bar{x}) \in [B]$.

Permutation: If $f(x_1, \ldots, x_k) \in [B]$ and $\pi$ is a permutation of $\{1, \ldots, k\}$, then we have $f(x_{\pi(1)}, \ldots, x_{\pi(k)}) \in [B]$.

Diagonalisation: If $f(x_1, \ldots, x_{k-1}, x_k) \in [B]$ and $f'(x_1, \ldots, x_{k-1}) = f(x_1, \ldots, x_{k-1}, x_{k-1})$, then $f'(x_1, \ldots, x_{k-1}) \in [B]$.

Composition: If $f(\bar{x}, y) \in [B]$ and $g(\bar{z}) \in [B]$, then $f(\bar{x}, g(\bar{z})) \in [B]$.

Cylindrification: If $f(\bar{x}) \in [B]$ then $f'(\bar{x}, y) \in [B]$. 
The last rule can be replaced with another, a simpler one, what will give us the following list:

<table>
<thead>
<tr>
<th>Alternative definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introduction:</strong> If $f(\vec{x}) \in B$ then $f(\vec{x}) \in [B]$.</td>
</tr>
<tr>
<td><strong>Permutation:</strong> If $f(x_1, \ldots, x_k) \in [B]$ and $\pi$ is a permutation of ${1, \ldots, k}$, then we have $f(x_{\pi(1)}, \ldots, x_{\pi(k)}) \in [B]$.</td>
</tr>
<tr>
<td><strong>Diagonalisation:</strong> If $f(x_1, \ldots, x_{k-1}, x_k) \in [B]$ and $f'(x_1, \ldots, x_{k-1}) = f(x_1, \ldots, x_{k-1}, x_{k-1})$, then $f'(x_1, \ldots, x_{k-1}) \in [B]$.</td>
</tr>
<tr>
<td><strong>Composition:</strong> If $f(\vec{x}, y) \in [B]$ and $g(\vec{z}) \in [B]$, then $f(\vec{x}, g(\vec{z})) \in [B]$.</td>
</tr>
<tr>
<td><strong>Projection:</strong> The function $pr^m_k(x_1, \ldots, x_m, \ldots, x_k) = x_m$ belongs to $[B]$ for each $k$ and $m = 1, \ldots, k$.</td>
</tr>
</tbody>
</table>
Definition
If \( f \in [B] \), we say that the set of functions \( B \) constructs the function \( f \).

Definition
Let \( B \) be a set of functions. The saturated set of functions \([B]\) is called a clone.

Attention
Do not mix up \( \langle B \rangle \) and \([B]\).
Properties of clones

The set of functions $B$ and their clones $[B]$ satisfy the following three properties:

1. $B \subseteq [B]$
2. $B \subseteq B'$ implies $[B] \subseteq [B']$
3. $[[B]] = [B]$

Remark

The same identities are satisfied by the sets of relations $S$ and their co-clones $\langle S \rangle$, i.e.,

1. $S \subseteq \langle S \rangle$
2. $S \subseteq S'$ implies $\langle S \rangle \subseteq \langle S' \rangle$
3. $\langle \langle S \rangle \rangle = \langle S \rangle$
How to classify clones?

Remark
For each set of functions $B$ there exists a clone $[B]$, but two different sets of functions $B$ and $B'$ can generate the same clone $[B] = [B']$. To classify clones, we need first some supplementary algebraic structures.

Definition
A binary relation $\leq \subseteq A \times A$ on a set $A$ is called a partial order if it satisfies the following conditions for each triplet of elements $a, b, c \in A$:

- Reflexivity: $a \leq a$
- Antisymmetry: $a \leq b$ and $b \leq a$ implies $a = b$
- Transitivity: $a \leq b$ and $b \leq c$ implies $a \leq c$
A partial order \( \leq \) on a set \( A \) is called a lattice order if it satisfies the additional two conditions:

- For each \( a, b \in A \) there exists a \( c \in A \), such that \( c \leq a \) and \( c \leq b \), and for each \( d \in A \) the relations \( d \leq a \) and \( d \leq b \) imply \( d \leq c \). The unique element \( c \) is called the infimum of \( a \) and \( b \), denoted by \( a \sqcap b \).
- For each \( a, b \in A \) there exists a \( c \in A \), such that \( a \leq c \) and \( b \leq c \), and for each \( d \in A \) the relations \( a \leq d \) and \( b \leq d \) imply \( c \leq d \). The unique element \( c \) is called the supremum of \( a \) and \( b \), denoted by \( a \sqcup b \).

The structure \( (A, \sqcup, \sqcap) \) is called a lattice.
Let $\mathcal{B}$ be a set of clones. The structure $\mathcal{B}$ is partially ordered by inclusion $\subseteq$ of clones (set inclusion). The operations of infimum and supremum are respectively the intersection $\cap$ and the union $\cup$ on sets. Hence the structure $(\mathcal{B}, \cup, \cap)$ is a lattice. In the boolean case it is called Post’s lattice.

**Question**
What is the structure of Post’s lattice?

**Answer**
It was established by Emil Post (1857 – 1954) between 1920 and 1940. The proof of 120 pages was published in 1941.
Bases of clones

It is not desirable to work with all functions of the clone $[B]$. Does there exist for each clone a finite subset of functions, from which we can generate the clone by saturation of composition? We prefer to have the smallest subset.

**Definition**

Let $B$ be a set of functions. Each set $B_0 \subseteq B$, such that $[B_0] = B$, is called a generator of $B$. If $B_0$ is a generator of $B$ and for each set $B_1 \subsetneq B_0$ we have $[B_1] \neq B$, then $B_0$ is called a basis of $B$. In other words, a basis is an inclusion minimal generator.

**Theorem (Post)**

*Each boolean clone has a finite basis.*

**Remark**

The proof spans on 8 pages. A clone can have more than one basis.
The following boolean functions are important for the bases of clones.

**Constant:** 0 and 1.

**Unary:** \( id(x) = x \) and \( not(x) = \neg x \).

**Binary:** \( and(x, y) = (x \land y) \) and \( or(x, y) = (x \lor y) \).

**Ternary:** \( maj(x, y, z) = (x \lor y) \land (y \lor z) \land (z \lor x) \) and \( aff(x, y, z) = x + y + z \pmod{2} \).
Classification of interesting clones

1 trivial clone: $I_2$.

7 minimal non-trivial clones: $I_0, I_1, N_2, E_2, V_2, L_2, D_2$. 
### Bases of interesting clones

<table>
<thead>
<tr>
<th>Clone</th>
<th>Name</th>
<th>Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td>( I_2 )</td>
<td>identity</td>
<td>{id}</td>
</tr>
<tr>
<td>( I_0 )</td>
<td>constant 0</td>
<td>{id, 0}</td>
</tr>
<tr>
<td>( I_1 )</td>
<td>constant 1</td>
<td>{id, 1}</td>
</tr>
<tr>
<td>( N_2 )</td>
<td>negation</td>
<td>{not}</td>
</tr>
<tr>
<td>( E_2 )</td>
<td>conjunction</td>
<td>{and}</td>
</tr>
<tr>
<td>( V_2 )</td>
<td>disjunction</td>
<td>{or}</td>
</tr>
<tr>
<td>( L_2 )</td>
<td>affinity</td>
<td>{aff}</td>
</tr>
<tr>
<td>( D_2 )</td>
<td>majority</td>
<td>{maj}</td>
</tr>
</tbody>
</table>
Reformulation of known results

\[ \text{Pol}(R) \supseteq I_2 \iff R \text{ is a boolean relation} \]
\[ \text{Pol}(R) \supseteq I_0 \iff R \text{ is 0-valid} \]
\[ \text{Pol}(R) \supseteq I_1 \iff R \text{ is 1-valid} \]
\[ \text{Pol}(R) \supseteq N_2 \iff R \text{ is complementive} \]
\[ \text{Pol}(R) \supseteq E_2 \iff R \text{ is Horn} \]
\[ \text{Pol}(R) \supseteq V_2 \iff R \text{ is dual Horn} \]
\[ \text{Pol}(R) \supseteq L_2 \iff R \text{ is affine} \]
\[ \text{Pol}(R) \supseteq D_2 \iff R \text{ is bijunctive} \]
Correspondence between the inclusions

An observation of Post lattice indicates the existence of the following two properties:

- If $S_1 \subseteq S_2$ then $\text{Pol}(S_1) \supseteq \text{Pol}(S_2)$ for all sets of boolean relations $S_1, S_2$.
- If $F_1 \subseteq F_2$ then $\text{Inv}(F_1) \supseteq \text{Inv}(F_2)$ for all sets of boolean functions $F_1, F_2$.

Galois correspondence

Such correspondence was studied for the first time by Évariste Galois (1811 – 1832).
## Galois correspondence

### Definition

Let \( \mathcal{A} = (A, \leq^A) \) and \( \mathcal{B} = (B, \leq^B) \) be two structures with their corresponding partial orders. Two functions \( \alpha: A \rightarrow B \) and \( \beta: B \rightarrow A \) form a **Galois correspondence** (sometimes called **Galois connection**) between \( \mathcal{A} \) and \( \mathcal{B} \) if the following four properties are satisfied:

1. \( a \leq^A b \) implies \( \alpha(b) \leq^B \alpha(a) \) for all \( a, b \in A \).
2. \( c \leq^B d \) implies \( \beta(d) \leq^A \beta(c) \) for all \( c, d \in B \).
3. \( a \leq^A \beta(\alpha(a)) \) for each \( a \in A \).
4. \( b \leq^B \alpha(\beta(b)) \) for each \( b \in B \).

### Question

Does there exists a Galois correspondence between the **clones** \( \mathcal{B} \) and the **co-clones** \( \mathcal{A} \)?
Galois correspondence

Question
Let us take for $\alpha$ the morphism $\text{Pol}$ and for $\beta$ the morphism $\text{Inv}$. The first two conditions of the Galois Correspondence Definition are already established. What about the others?

Answer
YES, since the inclusions $S \subseteq \text{Inv} (\text{Pol}(S))$ and $B \subseteq \text{Pol} (\text{Inv}(B))$ are always satisfied.

Theorem
Let $\mathcal{A}$ be a set of all co-clones and $\mathcal{B}$ the set of all clones over a finite domain. The morphisms $\text{Pol} : \mathcal{A} \rightarrow \mathcal{B}$ and $\text{Inv} : \mathcal{B} \rightarrow \mathcal{A}$ form a Galois correspondence.

Exercice 10
Formally prove the previous Theorem.
There exists a stronger and more interesting result.

**Theorem**

Let $S$ be a set of relations and $F$ a set of functions over a finite domain. Then the following identities are satisfied:

- $\text{Inv}(\text{Pol}(S)) = \langle S \rangle$
- $\text{Pol}(\text{Inv}(F)) = [F]$
Theorem

Let \((A, \sqcup^A, \sqcap^A), (B, \sqcup^B, \sqcap^B)\) be two lattices and \(\alpha: A \rightarrow B, \beta: B \rightarrow A\) two morphisms forming a Galois correspondence on these lattices. Then the following identities are valid for all \(a_1, a_2 \in A\) and \(b_1, b_2 \in B\):

1. \(\alpha(a_1 \sqcup^A a_2) = \alpha(a_1) \sqcap^B \alpha(a_2)\)
2. \(\alpha(a_1 \sqcap^A a_2) = \alpha(a_1) \sqcup^B \alpha(a_2)\)
3. \(\beta(b_1 \sqcup^B b_2) = \beta(b_1) \sqcap^A \beta(b_2)\)
4. \(\beta(b_1 \sqcap^B b_2) = \beta(b_1) \sqcup^A \beta(b_2)\)

Proof.

Exercise!
**Question**

How to determine the clone or the co-clone if we have the set of relations or the set of functions represented in several parts?

**Corollary**

Let $S_1, S_2$ be two sets of relations and $F_1, F_2$ two sets of functions. Then the following identities hold:

1. $\text{Pol}(S_1 \cup S_2) = \text{Pol}(S_1) \cap \text{Pol}(S_2)$
2. $\text{Inv}(F_1 \cup F_2) = \text{Inv}(F_1) \cap \text{Inv}(F_2)$

**Proof.**

The clones $(\mathcal{B}, \cup, \cap)$ as well as the co-clones $(\mathcal{A}, \cup, \cap)$ form lattices. The morphisms $\text{Pol}$ and $\text{Inv}$ determine a Galois correspondence between the clones and the co-clones.
Remark

It is not necessary to consider the whole co-clone $\langle S \rangle$, it is sufficient to work always with the original set of relations $S$.

Theorem

Let $S$ be a set of relations. The constraint satisfaction problems $\text{CSP}(S)$ and $\text{CSP}(\langle S \rangle)$ are polynomially equivalent.

Proof.

Given the inclusion $S \subseteq \langle S \rangle$, the polynomial reduction of $\text{CSP}(S)$ to $\text{CSP}(\langle S \rangle)$ is trivial. The set of relations $S$ implements the co-clone $\langle S \rangle$. Therefore we can write each formula $\varphi$ of $\text{CSP}(\langle S \rangle)$ as an equivalent formula $\varphi'$ of $\text{CSP}(S)$. The implementation $\varphi'$ is polynomial with respect to the original formula $\varphi$. This determines the polynomial reduction of $\text{CSP}(\langle S \rangle)$ to $\text{CSP}(S)$.
Question
If we have two sets of relations $S_1$ and $S_2$, how to determine the relation between $\text{CSP}(S_1)$ and $\text{CSP}(S_2)$, especially if $S_1$ and $S_2$ are incomparable?

Theorem
Let $S_1$ and $S_2$ be two sets of relations. If $\text{Pol}(S_1) \supseteq \text{Pol}(S_2)$ then there exists a polynomial reduction from $\text{CSP}(S_1)$ to $\text{CSP}(S_2)$.

Proof.
If $\text{Pol}(S_1) \supseteq \text{Pol}(S_2)$ then $\text{Inv}(\text{Pol}(S_1)) \subseteq \text{Inv}(\text{Pol}(S_2))$. Therefore $\langle S_1 \rangle \subseteq \langle S_2 \rangle$ holds, which gives us the polynomial reduction from $\text{CSP}(\langle S_1 \rangle)$ to $\text{CSP}(\langle S_2 \rangle)$. The previous Theorem then implies that there exists a polynomial reduction from $\text{CSP}(S_1)$ to $\text{CSP}(S_2)$. \qed
It’s all for today.
Do you have questions?