Relations, Functions, and the CSP

Ferdinand Börner

Let A be a fixed finite set (*basic set, domain*)

Relations on A

An m-ary relation on A ($m \geq 1$) is a subset

$$\varrho \subseteq A^m$$

$$\varrho(a_1, \ldots, a_m) \iff (a_1, \ldots, a_m) \in \varrho$$

$\mathbf{R}_A^{(m)} :=$ set of all m–ary relations on A

$\mathbf{R}_A = \bigcup_{m \geq 1} \mathbf{R}_A^{(m)}$ set of all relations on A

Functions on A

An n-ary functions on A ($n \geq 1$) is a map

$$f \ : \ A^n \to A$$

$\mathbf{O}_A^{(n)} :=$ set of all n-ary relations on A

$\mathbf{O}_A := \bigcup_{n \geq 1} \mathbf{O}_A^{(n)}$ set of all functions on A

We can extend $f : A^n \to A$ to a function

$$f : (A^m)^n \to A^m$$

Let $\vec{r}_i = (a_{1,i}, a_{2,i}, \ldots, a_{m,i}) \in A^m$ ($i = 1 \ldots n$).

Then

$f(\vec{r}_1, \ldots, \vec{r}_n) := (f(a_{1,1}, \ldots, a_{1,n}), \ldots, f(a_{m,1}, \ldots, a_{m,n}))$

If we write the $\vec{r}_i$ as columns:

$$f \begin{pmatrix} a_{1,1} & a_{1,2} & & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & & \vdots \\ a_{m,1} & a_{m,2} & & a_{m,n} \end{pmatrix} = \begin{pmatrix} f(a_{1,1}, \ldots, a_{1,n}) \\ f(a_{2,1}, \ldots, a_{2,n}) \\ \vdots \\ f(a_{m,1}, \ldots, a_{m,n}) \end{pmatrix}$$

The Galois connection Inv - Pol

We say that a function $f : A^n \to A$ *preserves* a relation $\varrho \subseteq A^m$, and that ϱ is *invariant* for f,

$$f \operatorname{pres} \varrho,$$

if for all $\vec{r}_1, \vec{r}_2, \ldots, \vec{r}_n \in A^m$ holds

$$\vec{r}_1, \vec{r}_2, \ldots, \vec{r}_n \in \varrho \Longrightarrow f(\vec{r}_1, \vec{r}_2, \ldots, \vec{r}_n) \in \varrho$$

(Componentwise application of f to the m-tuples of ϱ never leads to a tuple outside of ϱ.)

Let $\Gamma \subseteq \mathbf{R}_A$, $F \subseteq \mathbf{O}_A$.

$$\begin{aligned} \mathsf{Pol}\,\Gamma &:= \{f \in \mathbf{O}_A \mid (\forall \varrho \in \Gamma)\; f \operatorname{pres} \varrho\} \\ \mathsf{Inv}\,F &:= \{\varrho \in \mathbf{R}_A \mid (\forall f \in F)\; f \operatorname{pres} \varrho\} \end{aligned}$$

The pair $\mathsf{Inv} : \mathcal{P}\,\mathbf{O}_A \to \mathcal{P}\,\mathbf{R}_A$ and $\mathsf{Pol} : \mathcal{P}\,\mathbf{R}_A \to \mathcal{P}\,\mathbf{O}_A$ forms a *Galois connection between sets of functions and sets of relations*.

Galois connections in general

Let X, Y be two sets. A pair $\alpha : \mathcal{P}X \to \mathcal{P}Y$ and $\beta : \mathcal{P}Y \to \mathcal{P}X$ is called a *Galois connection*, if the following hold for all subsets $X_0, X_1 \subseteq X$ and $Y_0, Y_1 \subseteq Y$.

1. $X_0 \subseteq X_1 \Longrightarrow \alpha X_1 \subseteq \alpha X_0$
2. $Y_0 \subseteq Y_1 \Longrightarrow \beta Y_1 \subseteq \beta Y_0$
3. $X_0 \subseteq \beta\alpha X_0$ and $Y_0 \subseteq \alpha\beta Y_0$

In this case, the operators $\alpha\beta : \mathcal{P}Y \to \mathcal{P}Y$ and $\beta\alpha : \mathcal{P}X \to \mathcal{P}X$ are closure operators. The sets X_0 and Y_0 with $X_0 = \beta\alpha X_0$ and $Y_0 = \alpha\beta Y_0$ are called *Galois closed*.

If $Q \subseteq X \times Y$ is a relation between X and Y, then we can define a Galois connection by

$$\begin{aligned} \alpha X_0 &:= \{y \in Y \mid (\forall x \in X_0) Q(x,y)\} \\ \beta Y_0 &:= \{x \in X \mid (\forall y \in Y_0) Q(x,y)\} \end{aligned}$$

Vice versa, every Galois connection can be constructed in such a way.

Inv – Pol is such a Galois connection, basing on the relationship pres between relations and functions.

Aim: Characterizing the Galois closed sets of relations and functions for Inv - Pol.

Clones of functions

elementary functions (projections):

$$e_i^n : A^n \to A, \ (a_1, a_2, \dots, a_n) \mapsto a_i$$

superposition

Let $f \in \mathbf{O}_A^{(n)}$ and $g_1, \dots, g_n \in \mathbf{O}_A^{(k)}$. The *superposition* of these functions is the function

$$f[g_1, \dots, g_n] : A^k \to A, \ \vec{a} \mapsto f(g_1(\vec{a}), \dots, g_n(\vec{a}))$$

A set $C \subseteq \mathbf{O}_A$ of functions is called a *clone (of functions)*, if

1. C contains the elementary functions e_i^n for all n, i with $1 \leq i \leq n$.
2. C is closed under superposition, i.e. if $f \in C^{(n)}$, $g_1, \dots, g_n \in C^{(k)}$, then $f[g_1, \dots, g_n]$ is also in C.

Let $F \subseteq \mathbf{O}_A$. Then

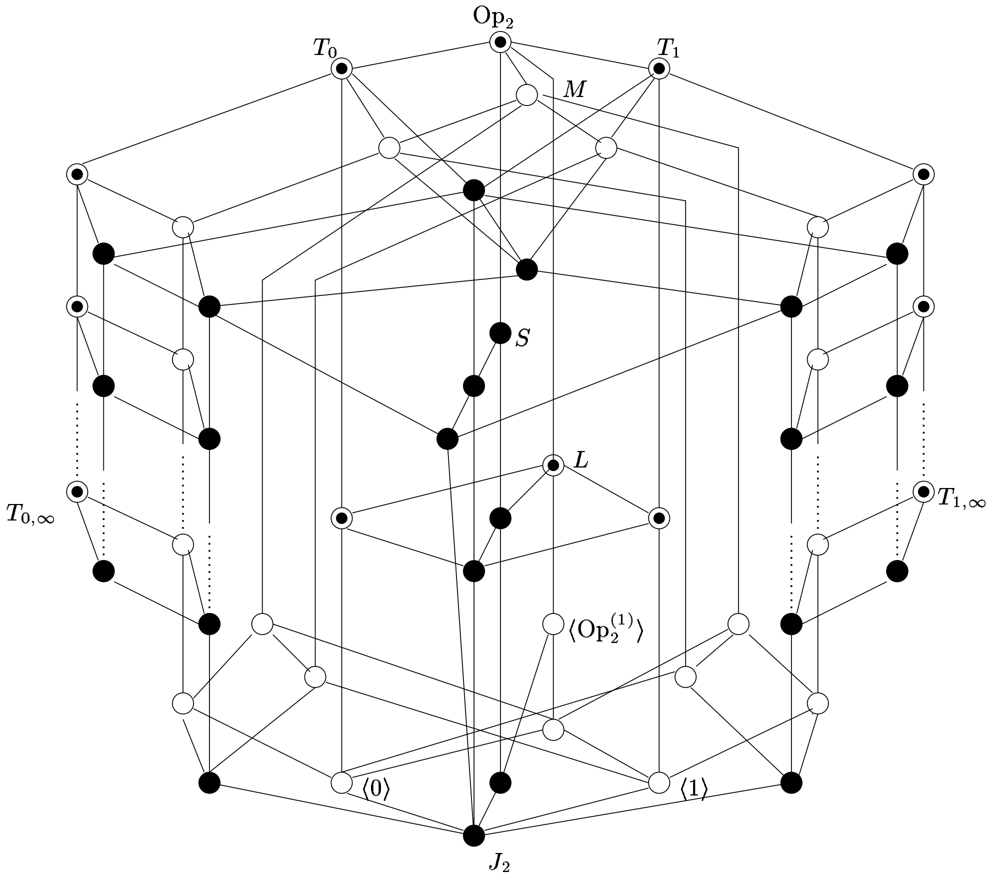
$$\mathsf{clone}(F) := \bigcap \{C \subseteq \mathbf{O}_A \mid F \subseteq C \text{ and } C \text{ is a clone}\}$$

denotes the *clone, generated by* F.

The set of all clones on A forms a lattice. For $|A| = 2$, this lattice is countable and well known (Posts lattice). If $|A| \geq 3$, there are uncountable many clones, and the lattice is widely unknown.

Lemma. *Let* $\Gamma \subseteq \mathbf{R}_A$ *be a set of relations. Then* $\mathsf{Pol}\,\Gamma$ *is a clone.*

Proof: easy



Op_2
T_0
T_1
M
S
L
$T_{0,\infty}$
$T_{1,\infty}$
$\langle \mathrm{Op}_2^{(1)} \rangle$
$\langle 0 \rangle$
$\langle 1 \rangle$
J_2

Logical operations on relations

Let $\varphi = \varphi(\varrho_1, \ldots, \varrho_l; x_1, \ldots, x_m)$ be a first order formula.

ϱ_i : m_i–ary predicate symbols (with arities m_i)

$\{x_1, \ldots, x_m\}$: free variables in φ

Then φ defines the following *logical operation*:

$$\begin{aligned} L_{\varphi,A} \ : \ \mathbf{R}_A^{(m_1)} \times \ldots \times \mathbf{R}_A^{(m_l)} &\to \mathbf{R}_A^{(m)} \\ (\varrho_1, \ldots, \varrho_l) &\mapsto \{(a_1, \ldots, a_m) \in A^m \mid \\ &\qquad \varphi(\varrho_1, \ldots, \varrho_l; a_1, \ldots, a_m)\} \end{aligned}$$

Examples:

- intersection of two m–ary relations

  $\varrho_1 \cap \varrho_2 =$
  $\{(a_1, \ldots, a_m) \mid \varrho_1(a_1, \ldots, a_m) \wedge \varrho_2(a_1, \ldots, a_m)\}$,

- projection onto the first m arguments

  $\mathrm{Pr}\, \varrho = \{(a_1, \ldots, a_m) \mid (\exists a_{m+1}) \varrho(a_1, \ldots, a_m, a_{m+1})\}$

Clones of relations

Let $S_1, S_2, \ldots$ be a list of logical symbols. With

$$\Phi(S_1, S_2, \ldots)$$

we denote the set of all first order formulas which contain besides technical symbols, predicate and variable symbols only symbols from the list $S_1, S_2, \ldots$.

A set $\Gamma \subseteq \mathbf{R}_A$ is called a *relational clone on A*, if Γ is closed under all logical operations $L_{\varphi,A}$ with $\varphi \in \Phi(\exists, \wedge, =, \mathsf{false})$.

Let $\Gamma \subseteq \mathbf{R}_A$ be a set of relations. Then

$$\langle\Gamma\rangle := \bigcap\{\Gamma_0 \mid \Gamma \subseteq \Gamma_0 \text{ and } \Gamma_0 \text{ is a relational clone}\}$$

denotes the *relational clone, generated by* Γ.

Therefore $\langle\Gamma\rangle$ is the least set of relations that

- contains all relations in Γ, the equality relation $d_A = \{(a, a) \mid a \in A\}$, and the empty relations and
- contains all relations that are definable from the relations above using existential quantification $(\exists)$ and conjunction $(\wedge)$.

Note: Let $s : \{1, \ldots, n\} \to \{1, \ldots, m\}$. Then a relational clone is also closed under the operation $W_s : \mathbf{R}_A^{(n)} \to \mathbf{R}_A^{(m)}$ with
$\varrho \mapsto \{(a_1, \ldots, a_m) \mid \varrho(a_{s(1)}, \ldots, a_{s(n)})\}$

Lemma. If $F \subseteq \mathbf{O}_A$ is a set of functions, then $\mathsf{Inv}\, F$ is a relational clone.

Proof: easy

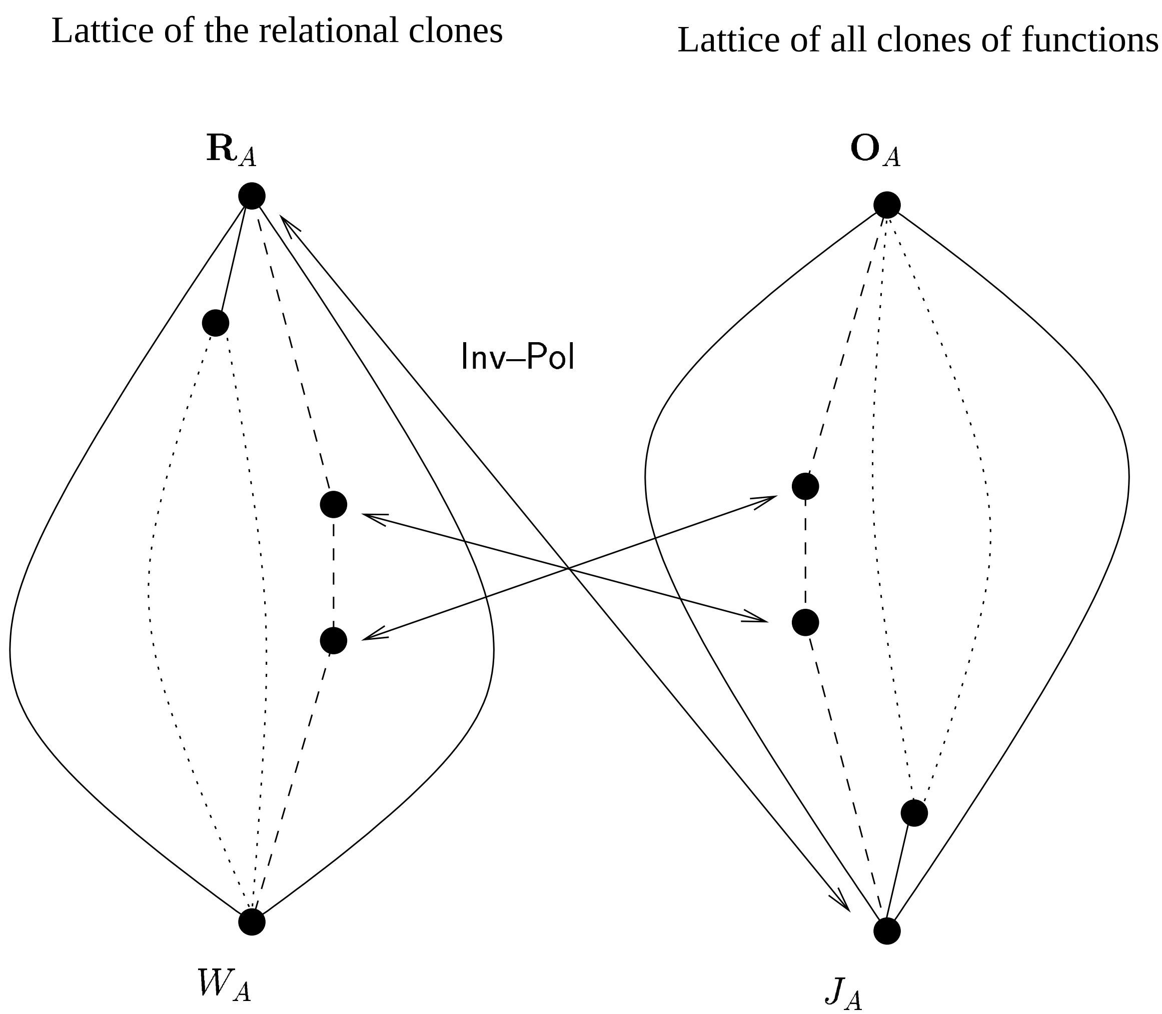
Characterization of Inv - Pol

Theorem. *Let* $C \subseteq \mathbf{O}_A$*. Then* C *is a clone of functions iff* $C = \mathsf{Pol}\,\Gamma$ *for some set* $\Gamma \subseteq \mathbf{R}_A$*.*

If $F \subseteq \mathbf{O}_A$*, then* $\mathsf{clone}\,F = \mathsf{Pol}\,\mathsf{Inv}\,F$.

Let $\Gamma_0 \subseteq \mathbf{R}_A$*. Then* Γ_0 *is a relational clone iff* $\Gamma_0 = \mathsf{Inv}\,F$ *for some set* $F \subseteq \mathbf{O}_A$*.*

If $\Gamma \subseteq \mathbf{R}_A$*, then* $\langle\Gamma\rangle = \mathsf{Inv}\,\mathsf{Pol}\,\Gamma$.


Lattice of the relational clones
Lattice of all clones of functions
$\mathbf{R}_A$
$\mathbf{O}_A$
Inv–Pol
W_A
J_A

Connection to the CSP

Let $\Gamma \subseteq \mathbf{R}_A$ be a (finite) set of relations. Then $\mathrm{CSP}(\Gamma)$ denotes the following decision problem:

Input: A sentence of the form

$$(\exists x_1)(\exists x_2)\ldots(\exists x_n)\,(\varrho_1(x_{i_{1,1}},\ldots)\wedge\ldots\wedge\varrho_m(x_{i_{m,1}},\ldots)\,)$$

with $\varrho_j \in \Gamma$, $i_{s,t} \in \{1,\ldots,n\}$.

Problem: Is this sentence true?

Assume $\Gamma_2 \subseteq \langle \Gamma_1 \rangle$.

Then for every relation $\sigma \in \Gamma_2$ there is a formula $\varphi \in \Phi(\exists, \wedge, =, \mathsf{false})$ with

$$\sigma(x_1, \ldots, x_m) \iff \varphi(\varrho_1, \ldots, \varrho_l; x_1, \ldots .x_m),$$

where $\varrho_1, \ldots, \varrho_l \in \Gamma_1$. If we have an input of $\mathrm{CSP}(\Gamma_2)$, then the $\sigma \in \Gamma_2$ can be replaced by the formulas on the right side. Then the new sentence can be transformed into a normal form that corresponds to an instance of $\mathrm{CSP}(\Gamma_1)$.

It can be shown that this is possible in polynomial time.

Theorem. (Jeavons) *Let* $\Gamma_1, \Gamma_2 \subseteq \mathbf{R}_A$ *be finite sets of relations. If* $\mathsf{Pol}\,\Gamma_1 \subseteq \mathsf{Pol}\,\Gamma_2$*, then* $\mathrm{CSP}(\Gamma_2)$ *is polynomial-time reducible to* Γ_1.

If $\mathsf{Pol}\,\Gamma_1 = \mathsf{Pol}\,\Gamma_2$*, then* $\mathrm{CSP}(\Gamma_1)$ *and* $\mathrm{CSP}(\Gamma_2)$ *are polynomial-time equivalent.*