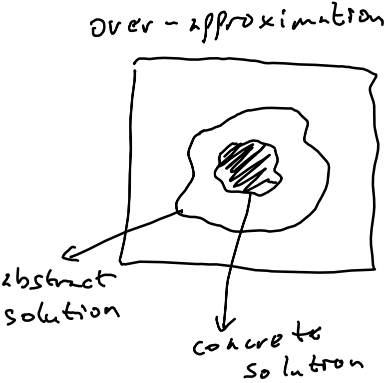
Abstract Interpretation

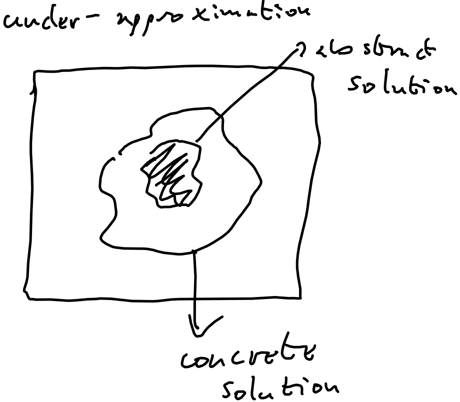
Juri Kolčák

Wednesday 8^{th} January, 2025

Intuition

Sound approximation based on **monotonic functions** over **ordered sets**.





P. Cousot & R. Cousot late 1970s

Abstraction

$I \subseteq S$

Transition system $\tau = (S, I, T)$. $T \subseteq S \times S$

A partial trace of length $n \in \mathbb{N}$ is a sequence of states $\sigma = (s_1, s_2, \ldots, s_n)$ between which exist transitions, $\forall i \in \{1, \ldots, n-1\}, (s_i, s_{i+1}) \in T$. $s_1 \in I$

Let Σ denote the set of all partial traces.

abstraction $\left\{ \begin{array}{l} \alpha \colon \mathcal{P}(\Sigma) \to \mathcal{P}(S^2) \\ \alpha \colon X \mapsto \{\alpha'(x) \mid x \in X\} \end{array} \right.$

$$\alpha' \colon \Sigma \to S^2$$

$$\alpha' \colon (s_1, s_2, \ldots, s_n) \mapsto (s_1, s_n)$$

Concretisation

$$\gamma \colon \mathcal{P}(S^2) \to \mathcal{P}(\Sigma)$$
$$\gamma \colon Y \mapsto \{\sigma | \alpha'(\sigma) \in Y\}$$

$X \subseteq \gamma \circ \alpha(X)$

Galois Connection

Let $(C, \leq_C)$ and $(A, \leq_A)$ be partially ordered sets. Then a pair of total monotonic functions $\alpha\colon C \to A$ and $\gamma\colon A \to C$ is a Galois connection if and only if for all $c \in C$ and $a \in A$, $\alpha(c) \leq_A a \iff c \leq_C \gamma(a)$.

$\forall c, c' \in C, \quad c \leq c' \Rightarrow \alpha(c) \leq \alpha(c') \Leftarrow$ Monotonic

An abstraction defined by the means of a Galois connection is always sound.

$$\alpha(c) \leq \alpha(c) \iff \underbrace{c \leq \gamma \circ \alpha(c)}$$

$$\alpha \circ \gamma(a) \leq a$$

Galois Connections for Complete Lattices

C, A are complete lattice

$\forall D \subseteq C, \exists \underline{d}, \bar{d} \in C$ such that $\wedge D = \underline{d}$ and $\vee D = \bar{d}$

α uniquely determines γ and vice versa.

$$\alpha(x) = \bigwedge \{y \in A \mid x \leq \gamma(y)\}$$

$$\gamma(y) = \bigvee \{x \in C \mid \alpha(x) \leq y\}$$

α preserves joins and γ preserves meets.

$$\alpha(\vee X) = \bigvee \{\alpha(x) \mid x \in X\}$$

$$\gamma(\wedge Y) = \bigwedge \{\gamma(y) \mid y \in Y\}$$

Galois connections are closed under composition and product.

$$C \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} D \underset{\alpha'}{\overset{\gamma'}{\leftrightarrows}} E \qquad C \underset{\alpha' \circ \alpha}{\overset{\gamma \circ \gamma'}{\leftrightarrows}} E$$

$$C \underset{\alpha_C}{\overset{\gamma_C}{\leftrightarrows}} C' \qquad D \underset{\alpha_D}{\overset{\gamma_D}{\leftrightarrows}} D' \qquad C \times D \underset{\alpha_C \times \alpha_D}{\overset{\gamma_C \times \gamma_D}{\leftrightarrows}} C' \times D'$$

α and γ define the best abstraction of monotonic functions.

$f: C \to C$ be an monotonic function

then $f^{\#}: A \to A$ defined as $f^{\#} = \alpha \circ f \circ \gamma$ is the best ("tightest") abstraction of f

$f^\# = \alpha \circ f \circ \gamma$ is the best abstraction of $f: C \to C$

$g: A \to A$ be a sound approximation of f

$$f(x) \le \gamma \circ g \circ \alpha(x)$$

$\underline{\alpha(x) \le y}$ $\qquad$ $x \le \gamma \circ \alpha(x) \le \gamma(y)$

$$\alpha \circ f(x) \le \alpha \circ f \circ \gamma(y) \le g(y)$$

$$\alpha \circ f(x) \le g(y)$$

Let's assume g is the most precise ("best")

$$g(y) = \bigvee \{\alpha \circ f(x) \mid \alpha(x) \le y\}$$

$$g(y) = \alpha\left(\bigvee \{f(x) \mid \alpha(x) \le y\}\right)$$

$$\bigvee \{f(x) \mid \alpha(x) \le y\} \le f\left(\bigvee \{x \mid \alpha(x) \le y\}\right)$$

$$\alpha \circ \gamma(y) \le y \Rightarrow \gamma(y) \in \{x \mid \alpha(x) \le y\}$$

$$f \circ \gamma(y) \le \bigvee \{f(x) \mid \alpha(x) \le y\} \le f\left(\bigvee \{x \mid \alpha(x) \le y\}\right)$$

Assume $\exists x \in C$ such that $\alpha(x) \ge \alpha \circ \gamma(y)$

$\alpha(x) \le y$ $\qquad$ $x \ge \gamma(y)$

$$\gamma \circ \alpha(x) \le \gamma(y) \le x$$

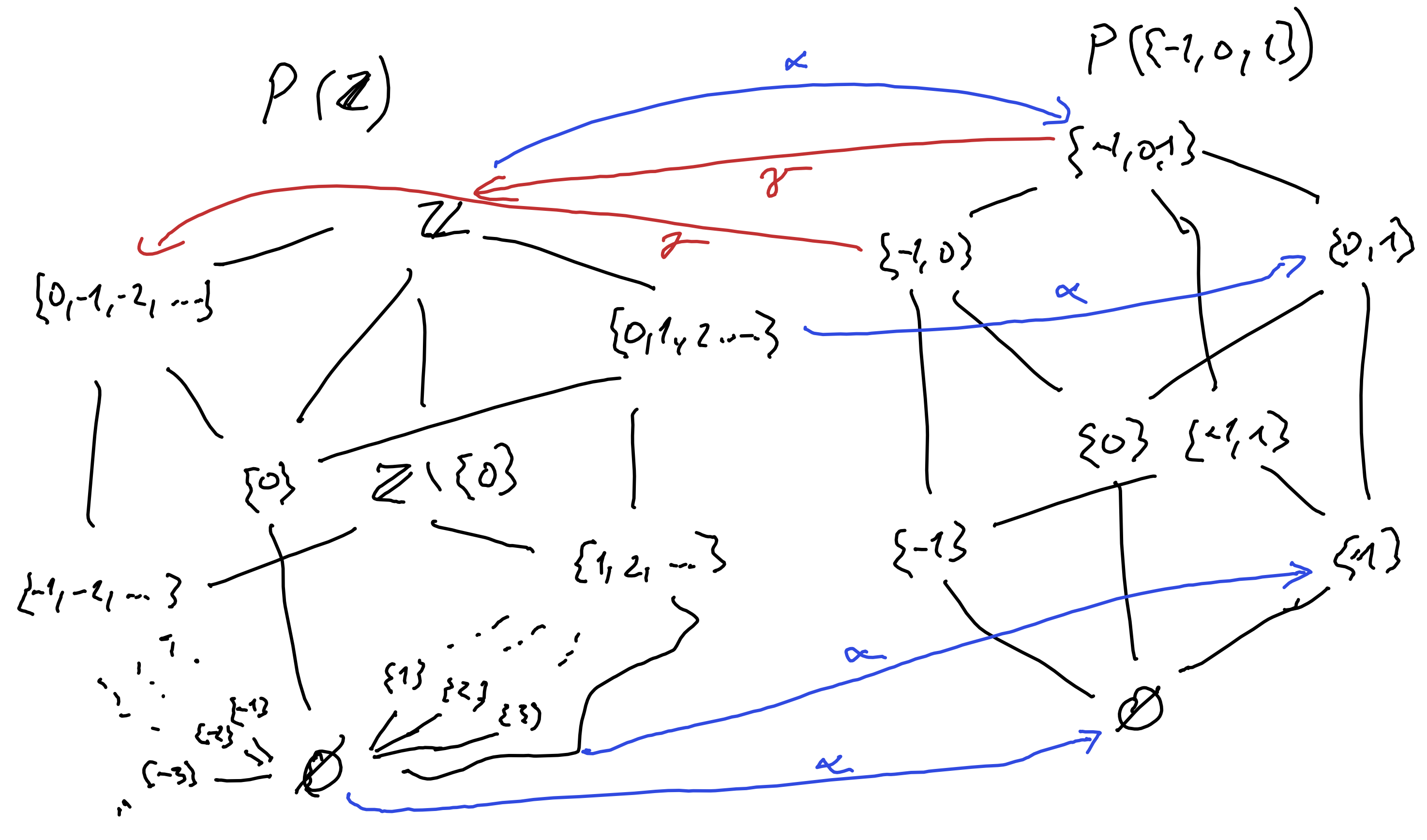
$$x \le \gamma \circ \alpha(x)$$

$\Leftarrow$

$$\gamma(y) = \bigvee \{x \mid \alpha(x) \le y\}$$

$$f \circ \gamma(y) = \bigvee \{f(x) \mid \alpha(x) \le y\} = f\left(\bigvee \{x \mid \alpha(x) \le y\}\right)$$

$$g(y) = \alpha \circ f \circ \gamma(y) = f^\#(y)$$



Closures

A function $\rho\colon C \to C$ is a **closure map** if and only if it is

1. monotonic, $\forall c, c' \in C, c \leq c' \implies \rho(c) \leq \rho(c')$;
2. extensive, $\forall c \in C, c \leq \rho(c)$;
3. idempotent, $\rho \circ \rho = \rho$;

Very often α is surjective

Then $\gamma \circ \alpha : C \to C$ is a closure map

Given a closure map $\rho : C \to C$

then $C \underset{\rho}{\overset{id}{\leftrightarrows}} \rho(C)$ is a Galois connection

Moore Families

$M \subseteq C$ is a Moore family $\iff$ for all $S \subseteq M$, $\bigwedge S \in M$

$c \in C$ $\rho(c) = \bigwedge \{c' \in M \mid c \leq c'\}$ then such ρ is

a closure map

Power Sets and Properties as Relations

$(d, a) \in R \Rightarrow$ "d has a property a"

Let $C = \mathcal{P}(D)$ for some set D and $R \subseteq D \times A$ a relation. Then R defines a Galois connection between C and A if it satisfies the following properties

1. For all $a, a' \in A$ and $d \in D$, $(d, a) \in R \wedge a \leq a' \Longrightarrow (d, a') \in R$;
2. For all $d \in D$, $(d, \bigwedge\{a \mid (d, a) \in R\}) \in R$;

$\gamma(a) = \{d \in D \mid (d, a) \in R\}$

$\gamma(A)$ is Moore family