Principles of Program Analysis:

Abstract Interpretation

Transparencies based on Chapter 4 of the book: Flemming Nielson, Hanne Riis Nielson and Chris Hankin: Principles of Program Analysis. Springer Verlag 2005.

Correctness Relations

$$R : V \times L \to \{\mathit{true}, \mathit{false}\}$$

Idea: $v \; R \; l$ means that the value v is described by the property l.

Correctness criterion: R is preserved under computation:

$$\begin{array}{ccccc}
p & \vdash & v_1 & \rightsquigarrow & v_2 \\
 & & \vdots & & \vdots \\
 & & R & \Rightarrow & R \\
 & & \vdots & & \vdots \\
p & \vdash & l_1 & \rhd & l_2
\end{array}$$

logical relation:

$$(p \vdash \cdot \rightsquigarrow \cdot) \; (R \twoheadrightarrow R) \; (p \vdash \cdot \rhd \cdot)$$

Admissible Correctness Relations

$$v \; R \; l_1 \;\wedge\; l_1 \sqsubseteq l_2 \;\Rightarrow\; v \; R \; l_2$$

$$(\forall l \in L' \subseteq L : v \; R \; l) \;\Rightarrow\; v \; R \; (\bigsqcap L')$$ ($\{l \mid v \; R \; l\}$ is a Moore family)

Two consequences:

$$v \; R \; \top$$

$$v \; R \; l_1 \;\wedge\; v \; R \; l_2 \;\Rightarrow\; v \; R \; (l_1 \sqcap l_2)$$

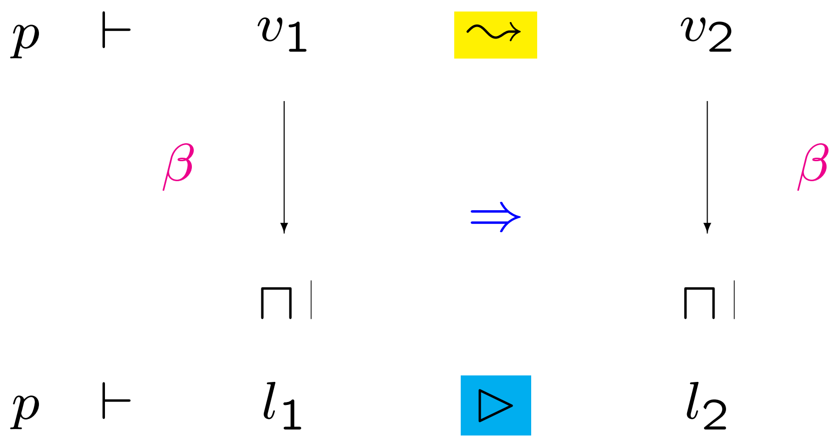
Assumption: $(L, \sqsubseteq)$ is a complete lattice.

Representation Functions

$$\beta : V \to L$$

Idea: β maps a value to the *best* property describing it.

Correctness criterion:



Equivalence of Correctness Criteria

Given a representation function β we define a correctness relation R_β by

$$v \; R_\beta \; l \quad \text{iff} \quad \beta(v) \sqsubseteq l$$

Given a correctness relation R we define a representation function β_R by

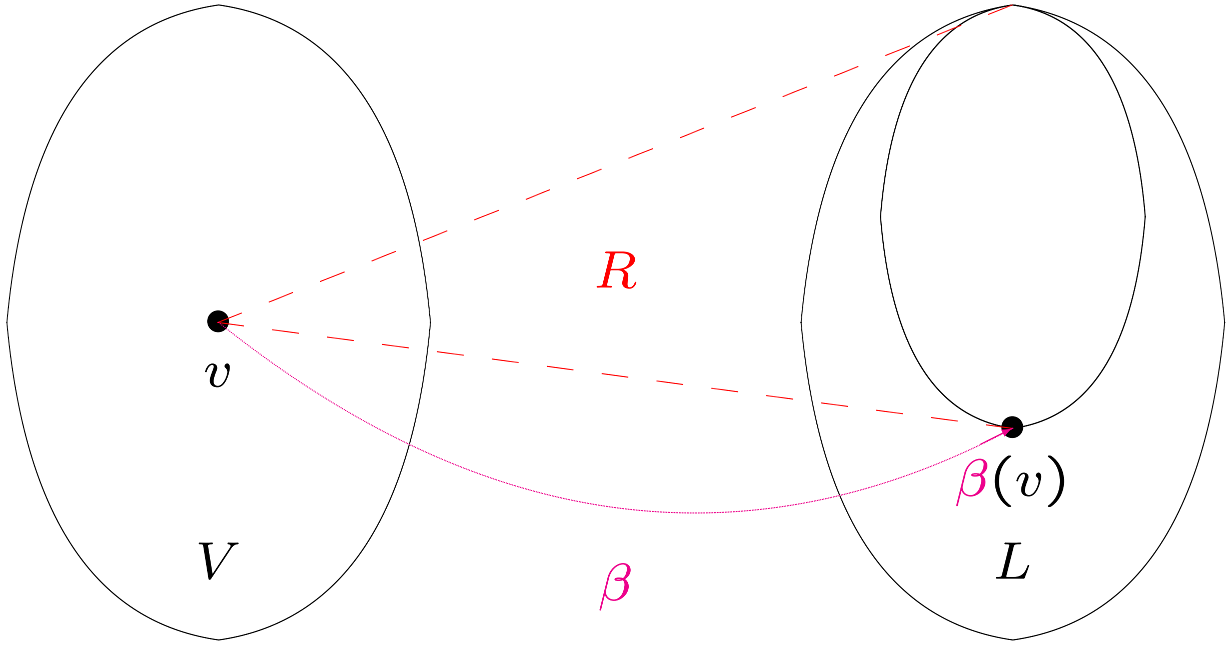
$$\beta_R(v) \;=\; \bigsqcap \{l \mid v \; R \; l\}$$

Lemma:

(i) Given $\beta : V \to L$, then the relation $R_\beta : V \times L \to \{\mathit{true}, \mathit{false}\}$ is an admissible correctness relation such that $\beta_{R_\beta} = \beta$.

(ii) Given an admissible correctness relation $R : V \times L \to \{\mathit{true}, \mathit{false}\}$, then β_R is well-defined and $R_{\beta_R} = R$.

Equivalence of Criteria: R is *generated* by β



A Modest Generalisation

Semantics:

$$p \vdash v_1 \leadsto v_2$$

where $v_1 \in V_1, v_2 \in V_2$

Program analysis:

$$p \vdash l_1 \rhd l_2$$

where $l_1 \in L_1, l_2 \in L_2$

$$\begin{array}{ccccc} p & \vdash & v_1 & \leadsto & v_2 \\ & & \vdots & & \vdots \\ & & R_1 & \Rightarrow & R_2 \\ & & \vdots & & \vdots \\ p & \vdash & l_1 & \rhd & l_2 \end{array}$$

logical relation:

$$(p \vdash \cdot \leadsto \cdot)\ (R_1 \twoheadrightarrow R_2)\ (p \vdash \cdot \rhd \cdot)$$

Galois Connections

- Galois connections and adjunctions

- Extraction functions

- Galois insertions

- Reduction operators

Galois connections

$$L \underset{\alpha}{\overset{\gamma}{\rightleftarrows}} M$$

α: *abstraction function*

γ: *concretisation function*

is a Galois connection if and only if

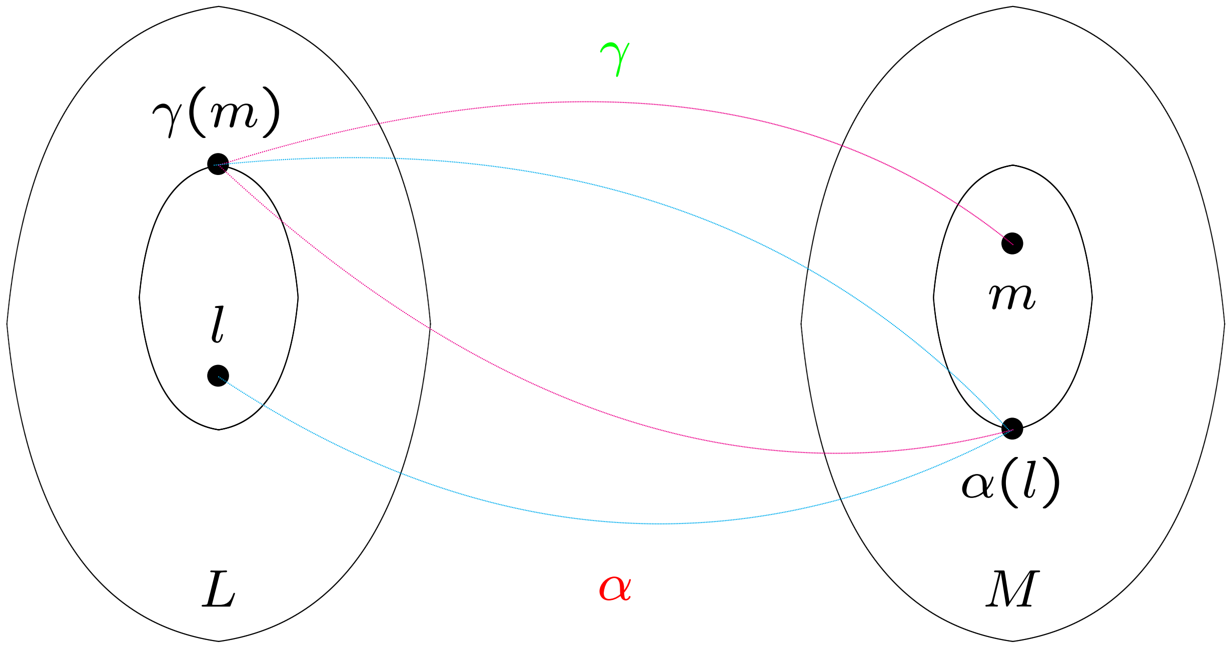
α and γ are monotone functions

that satisfy

$$\gamma \circ \alpha \sqsupseteq \lambda l.l$$

$$\alpha \circ \gamma \sqsubseteq \lambda m.m$$

Galois connections



$\gamma \circ \alpha \sqsupseteq \lambda l.l$ $\qquad$ $\alpha \circ \gamma \sqsubseteq \lambda m.m$

Example:

Galois connection

$$(\mathcal{P}(\mathbf{Z}), \alpha_{\mathrm{ZI}}, \gamma_{\mathrm{ZI}}, \textbf{Interval})$$

with concretisation function

$$\gamma_{\mathrm{ZI}}(\mathit{int}) = \{z \in \mathbf{Z} \mid \inf(\mathit{int}) \leq z \leq \sup(\mathit{int})\}$$

and abstraction function

$$\alpha_{\mathrm{ZI}}(Z) = \begin{cases} \bot & \text{if } Z = \emptyset \\ [\inf{}'(Z), \sup{}'(Z)] & \text{otherwise} \end{cases}$$

Examples:

$$\begin{aligned} \gamma_{\mathrm{ZI}}([0,3]) &= \{0,1,2,3\} \\ \gamma_{\mathrm{ZI}}([0,\infty]) &= \{z \in \mathbf{Z} \mid z \geq 0\} \\ \alpha_{\mathrm{ZI}}(\{0,1,3\}) &= [0,3] \\ \alpha_{\mathrm{ZI}}(\{2 * z \mid z > 0\}) &= [2,\infty] \end{aligned}$$

Adjunctions

$$L \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} M$$

is an *adjunction* if and only if

$$\alpha : L \to M \text{ and } \gamma : M \to L \text{ are total functions}$$

that satisfy

$$\alpha(l) \sqsubseteq m \quad \underline{\text{iff}} \quad l \sqsubseteq \gamma(m)$$

for all $l \in L$ and $m \in M$.

Proposition: (α, γ) is an adjunction iff it is a Galois connection.

Galois connections from representation functions

A representation function $\beta : V \to L$ gives rise to a Galois connection

$$(\mathcal{P}(V), \alpha, \gamma, L)$$

where

$$\begin{array}{rcl} \alpha(V') & = & \bigsqcup\{\beta(v) \mid v \in V'\} \\ \gamma(l) & = & \{v \in V \mid \beta(v) \sqsubseteq l\} \end{array}$$

for $V' \subseteq V$ and $l \in L$.

This indeed defines an adjunction:

$$\begin{array}{rcl} \alpha(V') \sqsubseteq l & \Leftrightarrow & \bigsqcup\{\beta(v) \mid v \in V'\} \sqsubseteq l \\ & \Leftrightarrow & \forall v \in V' : \beta(v) \sqsubseteq l \\ & \Leftrightarrow & V' \subseteq \gamma(l) \end{array}$$

Galois connections from extraction functions

An *extraction function*

$$\eta : V \to D$$

maps the values of V to their best descriptions in D.

It gives rise to a representation function $\beta_\eta : V \to \mathcal{P}(D)$ (corresponding to $L = (\mathcal{P}(D), \subseteq)$) defined by

$$\beta_\eta(v) = \{\eta(v)\}$$

The associated Galois connection is

$$(\mathcal{P}(V), \alpha_\eta, \gamma_\eta, \mathcal{P}(D))$$

where

$$\begin{array}{rcl@{\quad}c@{\quad}l} \alpha_\eta(V') &=& \bigcup\{\beta_\eta(v) \mid v \in V'\} &=& \{\eta(v) \mid v \in V'\} \\ \gamma_\eta(D') &=& \{v \in V \mid \beta_\eta(v) \subseteq D'\} &=& \{v \mid \eta(v) \in D'\} \end{array}$$

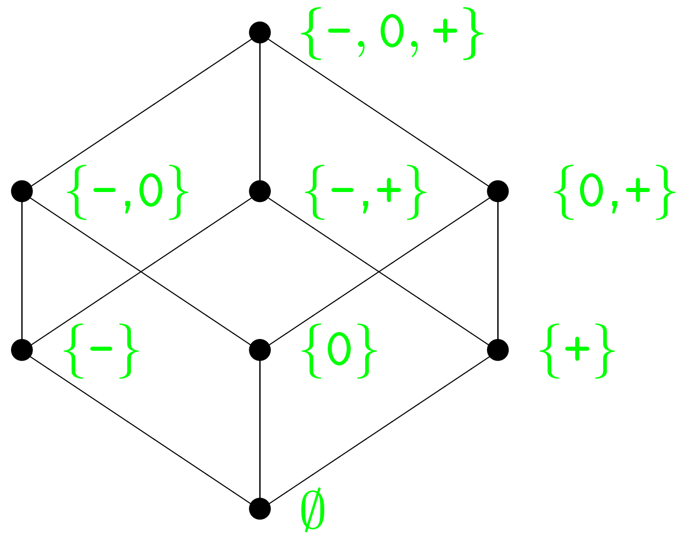
Example:

Extraction function

$$\text{sign} : \mathbf{Z} \rightarrow \mathbf{Sign}$$

specified by

$$\text{sign}(z) = \begin{cases} - & \text{if } z < 0 \\ 0 & \text{if } z = 0 \\ + & \text{if } z > 0 \end{cases}$$



Galois connection

$$(\mathcal{P}(\mathbf{Z}), \alpha_{\text{sign}}, \gamma_{\text{sign}}, \mathcal{P}(\mathbf{Sign}))$$

with

$$\alpha_{\text{sign}}(Z) = \{\text{sign}(z) \mid z \in Z\}$$
$$\gamma_{\text{sign}}(S) = \{z \in \mathbf{Z} \mid \text{sign}(z) \in S\}$$

Properties of Galois Connections

Lemma: If (L, α, γ, M) is a Galois connection then:

- α uniquely determines γ by $\gamma(m) = \bigsqcup\{l \mid \alpha(l) \sqsubseteq m\}$
- γ uniquely determines α by $\alpha(l) = \bigsqcap\{m \mid l \sqsubseteq \gamma(m)\}$
- α is completely additive and γ is completely multiplicative

In particular $\alpha(\bot) = \bot$ and $\gamma(\top) = \top$.

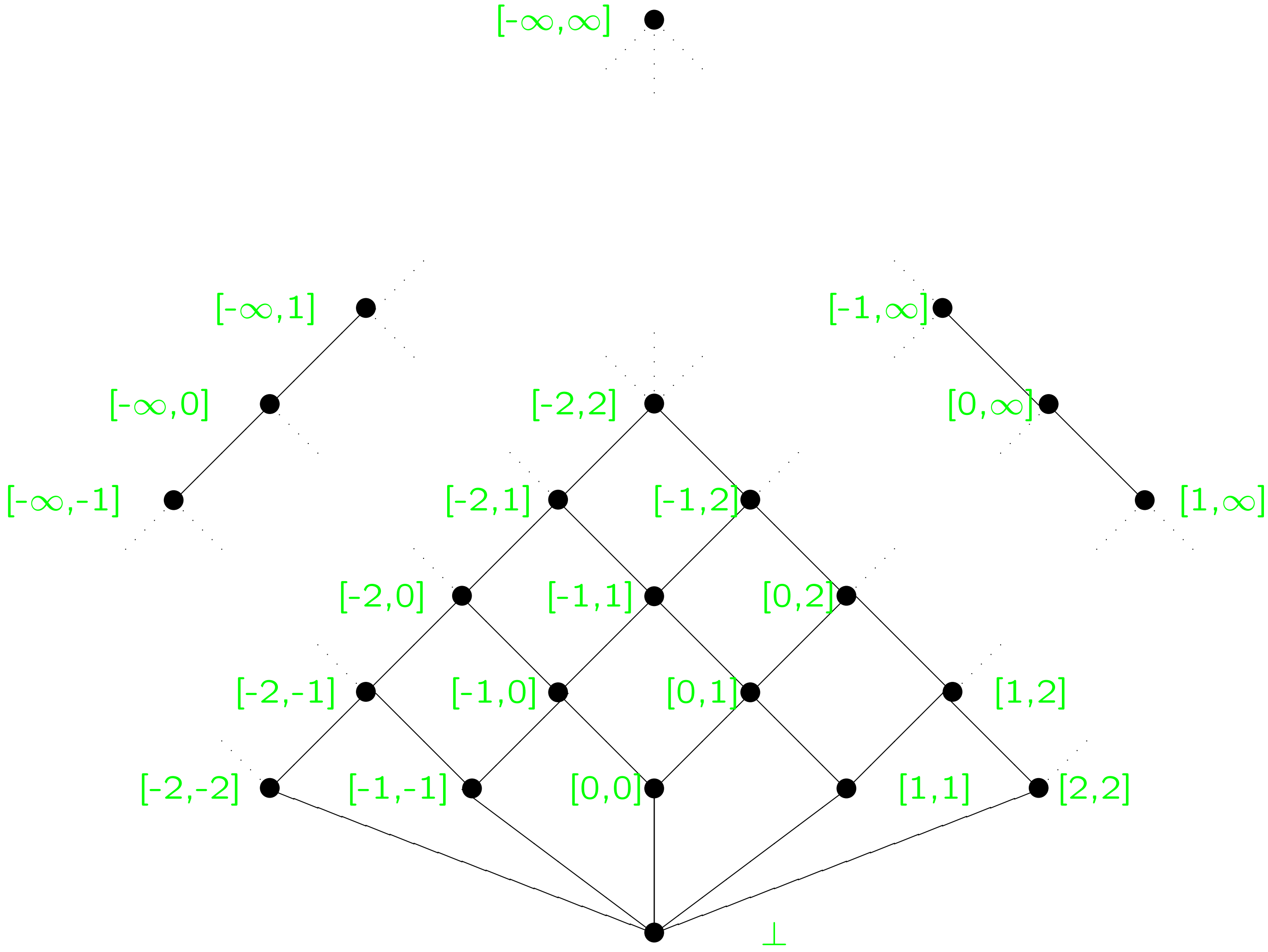
Lemma:

- If $\alpha : L \to M$ is completely additive then there exists (an upper adjoint) $\gamma : M \to L$ such that (L, α, γ, M) is a Galois connection.
- If $\gamma : M \to L$ is completely multiplicative then there exists (a lower adjoint) $\alpha : L \to M$ such that (L, α, γ, M) is a Galois connection.

Fact: If (L, α, γ, M) is a Galois connection then

- $\alpha \circ \gamma \circ \alpha = \alpha$ and $\gamma \circ \alpha \circ \gamma = \gamma$

The complete lattice **Interval** = (**Interval**, $\sqsubseteq$)



Example:

Define $\gamma_{\text{IS}} : \mathcal{P}(\mathbf{Sign}) \rightarrow \textbf{Interval}$ by:

$$\begin{array}{rcl} \gamma_{\text{IS}}(\{\texttt{-},\texttt{0},\texttt{+}\}) & = & [-\infty,\infty] \\ \gamma_{\text{IS}}(\{\texttt{-},\texttt{+}\}) & = & [-\infty,\infty] \\ \gamma_{\text{IS}}(\{\texttt{-}\}) & = & [-\infty,-1] \\ \gamma_{\text{IS}}(\{\texttt{+}\}) & = & [1,\infty] \end{array} \qquad \begin{array}{rcl} \gamma_{\text{IS}}(\{\texttt{-},\texttt{0}\}) & = & [-\infty,0] \\ \gamma_{\text{IS}}(\{\texttt{0},\texttt{+}\}) & = & [0,\infty] \\ \gamma_{\text{IS}}(\{\texttt{0}\}) & = & [0,0] \\ \gamma_{\text{IS}}(\emptyset) & = & \bot \end{array}$$

Does there exist an abstraction function

$$\alpha_{\text{IS}} : \textbf{Interval} \rightarrow \mathcal{P}(\mathbf{Sign})$$

such that $(\textbf{Interval}, \alpha_{\text{IS}}, \gamma_{\text{IS}}, \mathcal{P}(\mathbf{Sign}))$ is a Galois connection?

Example (cont.):

Is γ_{IS} completely multiplicative?

- if yes: then there exists a Galois connection
- if no: then there cannot exist a Galois connection

Lemma: If L and M are complete lattices and M is finite then $\gamma : M \to L$ is completely multiplicative if and only if the following hold:

- $\gamma : M \to L$ is monotone,
- $\gamma(\top) = \top$, and
- $\gamma(m_1 \sqcap m_2) = \gamma(m_1) \sqcap \gamma(m_2)$ whenever $m_1 \not\sqsubseteq m_2 \wedge m_2 \not\sqsubseteq m_1$

We calculate

$$
\begin{array}{rcccl}
\gamma_{\text{IS}}(\{\text{-}, 0\} \cap \{\text{-}, +\}) & = & \gamma_{\text{IS}}(\{\text{-}\}) & = & [-\infty, -1] \\
\gamma_{\text{IS}}(\{\text{-}, 0\}) \sqcap \gamma_{\text{IS}}(\{\text{-}, +\}) & = & [-\infty, 0] \sqcap [-\infty, \infty] & = & [-\infty, 0]
\end{array}
$$

showing that there is no Galois connection involving γ_{IS}.

Galois Connections are the Right Concept

We use the mundane approach to correctness to demonstrate this for:

- Admissible correctness relations

- Representation functions

The mundane approach: correctness relations

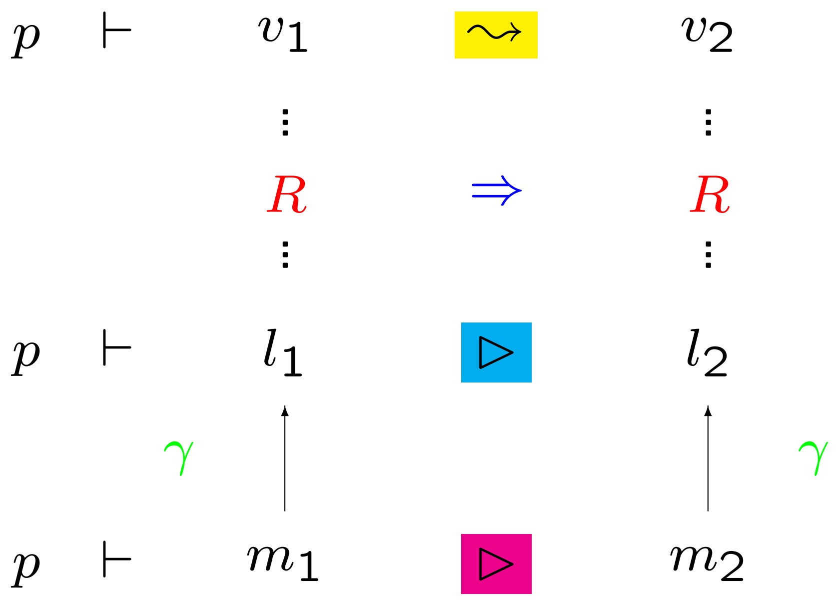
Assume

- $R : V \times L \to \{\mathit{true}, \mathit{false}\}$ is an admissible correctness relation
- (L, α, γ, M) is a Galois connection

Then $S : V \times M \to \{\mathit{true}, \mathit{false}\}$ defined by

$$v\ S\ m \quad \underline{\text{iff}} \quad v\ R\ (\gamma(m))$$

is an admissible correctness relation between V and M



The mundane approach: representation functions

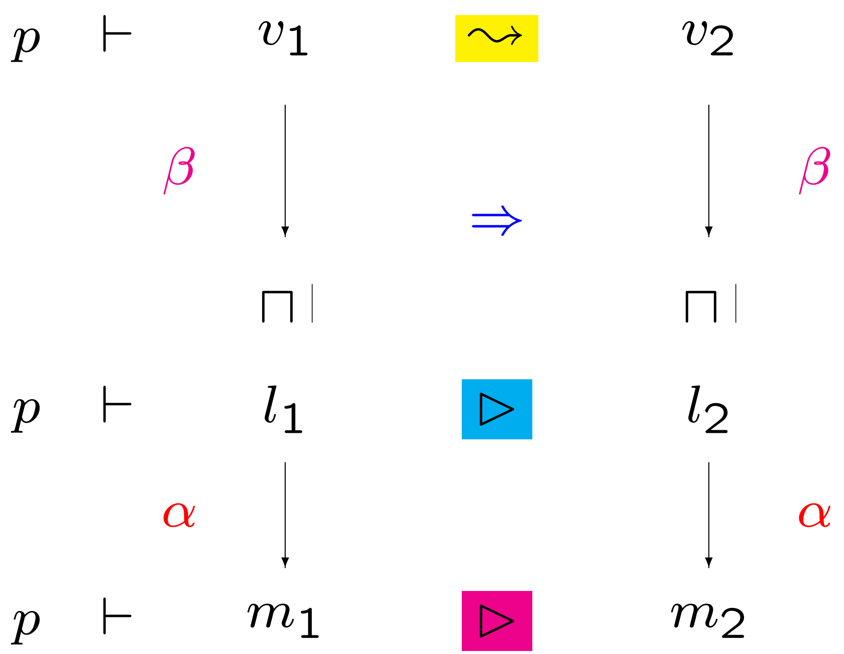
Assume

- $R : V \times L \to \{$*true*, *false*$\}$ is *generated by* $\beta : V \to L$
- (L, α, γ, M) is a Galois connection

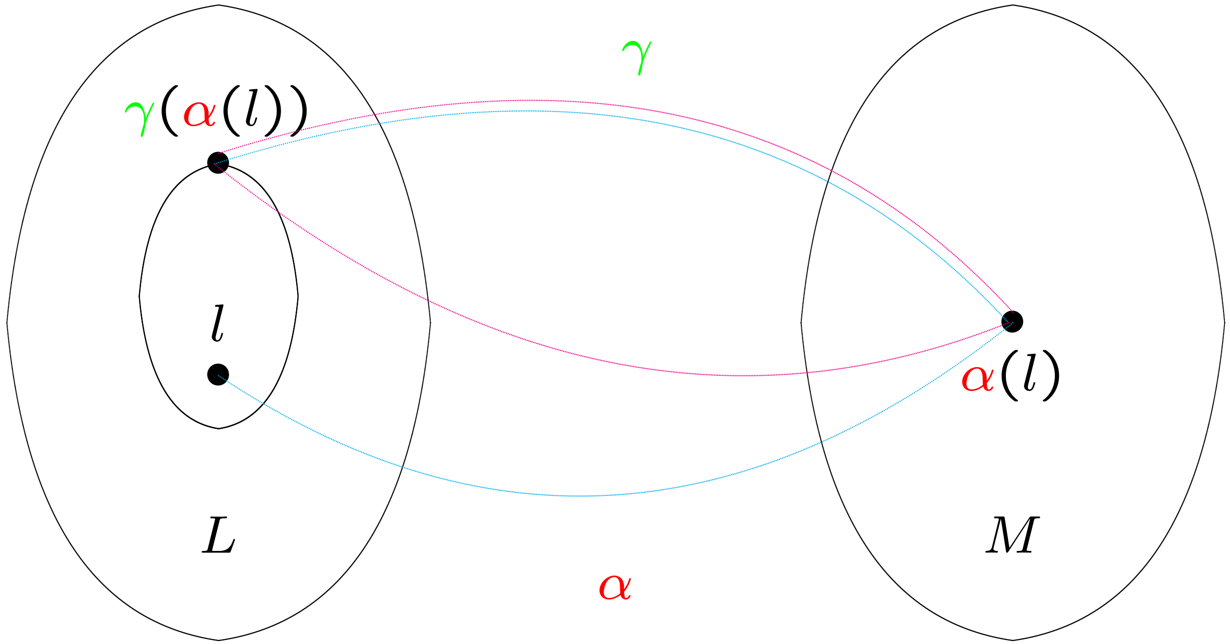
Then $S : V \times M \to \{$*true*, *false*$\}$ defined by

$$v \; S \; m \quad \underline{\text{iff}} \quad v \; R \; (\gamma(m))$$

is *generated by* $\alpha \circ \beta : V \to M$



Galois Insertions



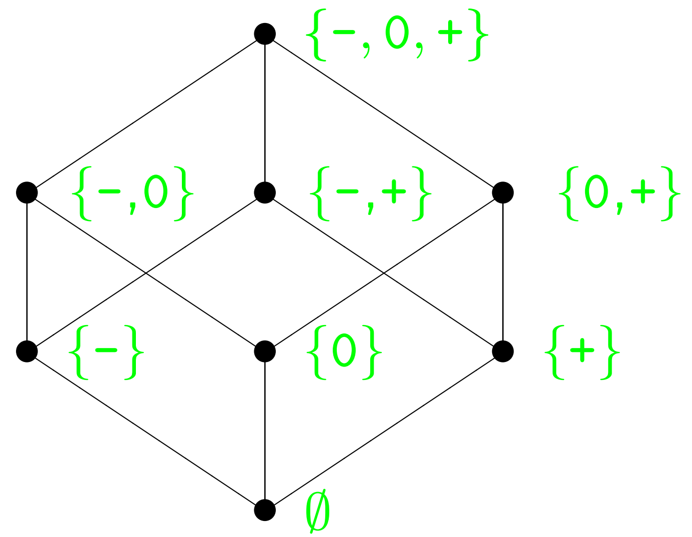
Monotone functions satisfying: $\gamma \circ \alpha \sqsupseteq \lambda l.l \qquad \alpha \circ \gamma = \lambda m.m$

Example (1):

$$(\mathcal{P}(\mathbf{Z}), \alpha_{\text{sign}}, \gamma_{\text{sign}}, \mathcal{P}(\mathbf{Sign}))$$

where sign : $\mathbf{Z} \rightarrow \mathbf{Sign}$ is specified by:

$$\text{sign}(z) = \begin{cases} \text{-} & \text{if } z < 0 \\ 0 & \text{if } z = 0 \\ + & \text{if } z > 0 \end{cases}$$



Is it a Galois insertion?

Example (2):

$$(\mathcal{P}(\mathbf{Z}), \alpha_{\mathsf{signparity}}, \gamma_{\mathsf{signparity}}, \mathcal{P}(\mathbf{Sign} \times \mathbf{Parity}))$$

where $\mathbf{Sign} = \{\texttt{-}, \texttt{0}, \texttt{+}\}$ and $\mathbf{Parity} = \{\mathsf{odd}, \mathsf{even}\}$

and signparity : $\mathbf{Z} \rightarrow \mathbf{Sign} \times \mathbf{Parity}$:

$$\mathsf{signparity}(z) = \begin{cases} (\mathsf{sign}(z), \mathsf{odd}) & \text{if } z \text{ is odd} \\ (\mathsf{sign}(z), \mathsf{even}) & \text{if } z \text{ is even} \end{cases}$$

Is it a Galois insertion?

Properties of Galois Insertions

Lemma: For a Galois connection (L, α, γ, M) the following claims are equivalent:

(i) (L, α, γ, M) is a Galois insertion;

(ii) α is surjective: $\forall m \in M : \exists l \in L : \alpha(l) = m$;

(iii) γ is injective: $\forall m_1, m_2 \in M : \gamma(m_1) = \gamma(m_2) \Rightarrow m_1 = m_2$; and

(iv) γ is an order-similarity: $\forall m_1, m_2 \in M : \gamma(m_1) \sqsubseteq \gamma(m_2) \Leftrightarrow m_1 \sqsubseteq m_2$.

Corollary: A Galois connection specified by an *extraction* function $\eta : V \to D$ is a Galois insertion if and only if η is surjective.

Example (1) reconsidered:

$$(\mathcal{P}(\mathbf{Z}), \alpha_{\text{sign}}, \gamma_{\text{sign}}, \mathcal{P}(\mathbf{Sign}))$$

$$\text{sign}(z) = \begin{cases} \text{-} & \text{if } z < 0 \\ 0 & \text{if } z = 0 \\ + & \text{if } z > 0 \end{cases}$$

is a Galois insertion because sign is surjective.

Example (2) reconsidered:

$$(\mathcal{P}(\mathbf{Z}), \alpha_{\text{signparity}}, \gamma_{\text{signparity}}, \mathcal{P}(\mathbf{Sign} \times \textbf{Parity}))$$

$$\text{signparity}(z) = \begin{cases} (\text{sign}(z), \text{odd}) & \text{if } z \text{ is odd} \\ (\text{sign}(z), \text{even}) & \text{if } z \text{ is even} \end{cases}$$

is not a Galois insertion because signparity is not surjective.

Reduction Operators

Given a Galois connection (L, α, γ, M) it is always possible to obtain a Galois insertion by enforcing that the concretisation function γ is injective.

Idea: remove the superfluous elements from M using a *reduction operator*

$$\varsigma : M \to M$$

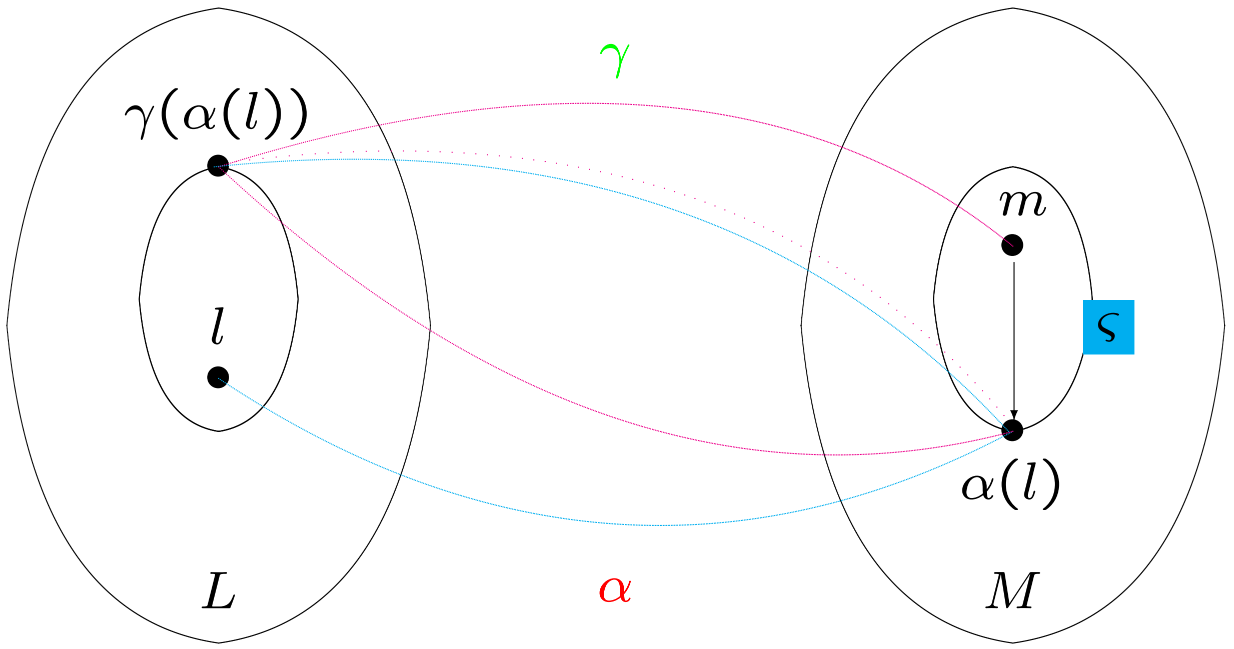
defined from the Galois connection.

Proposition: Let (L, α, γ, M) be a Galois connection and define the reduction operator $\varsigma : M \to M$ by

$$\varsigma(m) = \bigsqcap \{m' \mid \gamma(m) = \gamma(m')\}$$

Then $\varsigma[M] = (\{\varsigma(m) \mid m \in M\}, \sqsubseteq_M)$ is a complete lattice and $(L, \alpha, \gamma, \varsigma[M])$ is a Galois insertion.

The reduction operator $\varsigma : M \to M$



Reduction operators from extraction functions

Assume that the Galois connection $(\mathcal{P}(V), \alpha_\eta, \gamma_\eta, \mathcal{P}(D))$ is given by an extraction function $\eta : V \to D$.

Then the reduction operator ς_η is given by

$$\varsigma_\eta(D') = D' \cap \eta[V]$$

where $\eta[V] = \{d \in D \mid \exists v \in V : \eta(v) = d\}$.

Since $\varsigma_\eta[\mathcal{P}(D)]$ is isomorphic to $\mathcal{P}(\eta[V])$ the resulting Galois insertion is isomorphic to

$$(\mathcal{P}(V), \alpha_\eta, \gamma_\eta, \mathcal{P}(\eta[V]))$$