Verifikation von C-Programmen

Vorlesung 6 vom 04.12.2014: Abstract Interpretation

Christoph Lüth

Universität Bremen

Wintersemester 2014/15

Galois-Connections

Let L, M be lattices and

$$\alpha : L \to M$$
$$\gamma : M \to L$$

with α, γ monotone, then $\langle L, \alpha, \gamma, M \rangle$ is a Galois connection if

$$\gamma \cdot \alpha \sqsupseteq \lambda l.\, l \tag{1}$$
$$\alpha \cdot \gamma \sqsubseteq \lambda m.\, m \tag{2}$$

Example of a Galois Connection

$$
\begin{aligned}
L &= \langle \mathcal{P}(\mathbb{Z}), \subseteq \rangle \\
M &= \langle \textbf{Interval}, \sqsubseteq \rangle \\
\gamma_{ZI}([a, b]) &= \{z \in \mathbb{Z} \mid a \leq z \leq b\} \\
\alpha_{ZI}(Z) &= \begin{cases} \bot & Z = \emptyset \\ [\mathit{inf}(Z), \mathit{sup}(Z)] & \text{otherwise} \end{cases}
\end{aligned}
$$

Constructing Galois Connections

Let $\langle L, \alpha, \beta, M\rangle$ be a Galois connection, and S be a set. Then

(i) $S \to L$, $S \to M$ are lattices with functions ordered pointwise:

$$f \sqsubseteq g \;\longleftrightarrow\; \forall s. f\, s \sqsubseteq g\, s$$

(ii) $\langle S \to L, \alpha', \gamma', S \to M\rangle$ is a Galois connection with

$$\alpha'(f) = \alpha \cdot f$$
$$\gamma'(g) = \gamma \cdot g$$

Generalised Monotone Framework

A Generalised Monotone Framework is given by

- a lattice $L = \langle L, \sqsubseteq \rangle$
- a finite flow $F \subseteq Lab \times Lab$
- a finite set of extremal labels $E \sqsubseteq Lab$
- an extremal label $\iota \in Lab$
- mappings f from $lab(F)$ to $L \times L$ and $lab(E)$ to L

This gives a set of constraints

$$A_\circ(l) \sqsupseteq \bigsqcup \{A_\cdot(l') \mid (l', l) \in F\} \sqcup \iota_E^l \quad (3)$$

$$A_\cdot(l) \sqsupseteq f_l(A_\circ(l)) \quad (4)$$

Correctness

Let R be a correctness relation $R \subseteq V \times L$, and $\langle L, \alpha, \gamma, M\rangle$ be a Galois connection, then we can construct a correctness relation $S \subseteq V \times M$ by

$$v \, S \, m \longleftrightarrow v \, R \, \gamma(m)$$

On the other hand, if B, M is a Generalised Monotone Framework, and $\langle L, \alpha, \gamma, M\rangle$ is a Galois connection, then a solution to the constraints $B^{\sqsubseteq}$ is a solution to $A^{\sqsubseteq}$.

This means: we can transfer the correctness problem from L to M and solve it there.

An Example

The analysis SS is given by the lattice $\mathcal{P}(\textbf{State}), \sqsubseteq$ and given a statement S_*:

- $\mathit{flow}(S_*)$
- extremal labels are $E = \{\mathit{init}(S_*)\}$
- the transfer functions (for $\Sigma \subseteq \textbf{State}$):

$$
\begin{aligned}
f_l^{SS}(\Sigma) &= \{\sigma[x \mapsto \mathcal{A}[\![a]\!]\sigma] \mid \sigma \in \Sigma\} && \text{if } [x := a]^l \text{ is in } S_* \\
f_l^{SS}(\Sigma) &= \Sigma && \text{if } [\texttt{skip}]^l \text{ is in } S_* \\
f_l^{SS}(\Sigma) &= \Sigma && \text{if } [b]^l \text{ is in } S_*
\end{aligned}
$$

Now use the Galois connection $\langle \mathcal{P}(\textbf{State}), \alpha_{ZI}, \gamma_{ZI}, \textbf{Interval} \rangle$ to construct a monotone framework with $\langle \mathit{Interval}, \sqsubseteq \rangle$, with in particular

$$
g_l^{IS}(\sigma) = \sigma[x \mapsto [i,j]] \quad \text{if } [x := a]^l \text{ in } S_*, \text{ and } [i,j] = \alpha_{ZI}(\mathcal{A}[\![a]\!](\gamma_{ZI}(\sigma)))
$$

What's Missing?

- Fixpoints: Widening and narrowing.