3.2 Application to Predicate Abstraction

Indeed an abstract interpretation of:

- Program points/labels: \( \mathcal{L} \) is finite
- Variables: \( X \) is finite (for a given program)
- Set of values: \( \mathcal{V} \)
- Memory states: \( M = X \rightarrow \mathcal{V} \)

Reference

**Local Versus Global Assertions**

- **Isomorphism** between global and local assertions:
  \[
  \langle p(\mathcal{L} \times \mathcal{M}), \subseteq \rangle \cong_{\alpha_1}^{\gamma_1} \langle \mathcal{L} \longrightarrow p(\mathcal{M}), \subseteq \rangle
  \]
  where:
  \[
  \alpha_1(P) = \lambda \ell . \{ m \mid (\ell, m) \in P \}
  \]
  \[
  \gamma_1(Q) = \{ (\ell, m) \mid \ell \in \mathcal{L} \land m \in Q_\ell \}
  \]
  and \( \subseteq \) is the pointwise ordering:
  \( Q \subseteq Q' \) if and only if \( \forall \ell \in \mathcal{L} : Q_\ell \subseteq Q'_\ell \).

**Predicate Abstraction**

A memory state property \( Q \in p(\mathcal{M}) \) is approximated by the subset of predicates \( p \in \mathcal{P} \) which holds when \( Q \) holds (formally \( Q \subseteq \mathcal{I}[p] \)). This defines a Galois connection:

\[
\langle p(\mathcal{M}), \subseteq \rangle \cong_{\alpha_\mathcal{P}}^{\gamma_\mathcal{P}} \langle p(\mathcal{P}), \supseteq \rangle
\]

where:

\[
\alpha_\mathcal{P}(Q) = \{ p \in \mathcal{P} \mid Q \subseteq \mathcal{I}[p] \}
\]

\[
\gamma_\mathcal{P}(P) = \bigcap \{ \mathcal{I}[p] \mid p \in \mathcal{P} \}
\]

**Syntactic Predicates**

- Choose a set \( \mathcal{P} \) of syntactic predicates such that:
  \[
  \forall S \subseteq \mathcal{P} : (\wedge S) \in \mathcal{P}
  \]
  an interpretation \( \mathcal{I} \in \mathcal{P} \mapsto p(\mathcal{M}) \) such that:
  \[
  \forall S \subseteq \mathcal{P} : \mathcal{I}(\wedge S) = \bigcap_{p \in S} \mathcal{I}[p]
  \]
  It follows that \( \{ \mathcal{I}[p] \mid p \in \mathcal{P} \} \) is a Moore family.

**Pointwise Extension to All Program Points**

By pointwise extension, we have for all program points:

\[
\langle \mathcal{L} \longrightarrow p(\mathcal{M}), \subseteq \rangle \cong_{\alpha_\mathcal{P}}^{\gamma_\mathcal{P}} \langle \mathcal{L} \longrightarrow p(\mathcal{P}), \supseteq \rangle
\]

where:

\[
\alpha_\mathcal{P}(Q) = \lambda \ell . \alpha_\mathcal{P}(Q_\ell)
\]

\[
\gamma_\mathcal{P}(P) = \lambda \ell . \gamma_\mathcal{P}(P_\ell)
\]

\[
P \supseteq P' = \forall \ell \in \mathcal{L} : P_\ell \supseteq P'_\ell
\]
**Boolean Encoding**

- \( P = \{p_1, \ldots, p_k\} \) is finite
- \( B = \{\text{tt}, \text{ff}\} \) is the set of booleans with \( \text{ff} \Rightarrow \text{ff} \Rightarrow \text{tt} \Rightarrow \text{tt} \)
- We can use a boolean encoding of subsets of \( P \):

\[
\langle \alpha_b(P), \supseteq \rangle \leftarrow \frac{\gamma_b}{\alpha_b} \langle \bigcap_{i=1}^{k} B, \subseteq \rangle
\]

where:

\[
\alpha_b(P) = \bigcap_{i=1}^{k} (p_i \in P)
\]

\[
\gamma_b(Q) = \{p_i \mid 1 \leq i \leq k \land Q_i\}
\]

\[
Q \Leftarrow Q' = \forall i : 1 \leq i \leq k : Q_i \Leftarrow Q_i'
\]

**Composition: Pointwise Boolean Encoded Predicate Abstraction**

By composition, we get:

\[
\langle \varphi(L \times M), \subseteq \rangle \leftarrow \frac{\gamma}{\alpha} \langle L \longrightarrow \bigcap_{i=1}^{k} B, \subseteq \rangle
\]

where:

\[
\alpha(P) = \check{\alpha}_b \circ \check{\alpha}_b \circ \alpha(P)
\]

\[
\gamma(Q) = \check{\gamma}_b \circ \check{\gamma}_b \circ \gamma(Q)
\]

**Pointwise Extension to All program Points**

By pointwise extension, we have for all program points:

\[
\langle L \longrightarrow \varphi(P), \supseteq \rangle \leftarrow \frac{\gamma_b}{\alpha_b} \langle L \longrightarrow \bigcap_{i=1}^{k} B, \subseteq \rangle
\]

where:

\[
\check{\alpha}_b(P) = \lambda \ell \cdot \alpha_b(P_\ell)
\]

\[
\check{\gamma}_b(Q) = \lambda \ell \cdot \gamma_b(Q_\ell)
\]

\[
Q \Leftarrow Q' = \forall \ell \in L : Q_\ell \Leftarrow Q'_\ell
\]

**Abstract Predicate Transformer (Sketchy)**

\[
\alpha_P \circ \post[X:=E] \circ \gamma_P(\{q_1, \ldots, q_n\}) \text{ where } \{q_1, \ldots, q_n\} \subseteq \{p_1, \ldots, p_k\}
\]

\[
= \alpha_P \circ \post[X:=E](\bigcap_{i=1}^{n} I[q_i]) \text{ def. } \gamma_P
\]

\[
= \alpha_P(\{\rho[X/E] \mid \rho \in \bigcap_{i=1}^{n} I[q_i]\}) \text{ def. } \post[X:=E]
\]

\[
= \alpha_P(\bigcap_{i=1}^{n} \{\rho[X/E] \mid \rho \in I[q_i]\}) \text{ def. } \bigcap
\]

\[
= \alpha_P(\bigcap_{i=1}^{n} I[q_i[X/E]]) \text{ def. substitution}
\]

\[
= \{p_j \mid I[q_i[X/E]] \Rightarrow p_j\} \text{ def. } \alpha_P
\]

\[
\Rightarrow \{p_j \mid \text{theorem\_prover}(q_i[X/E] \Rightarrow p_j)\}
\]

since \( \text{theorem\_prover}(q_i[X/E] \Rightarrow p_j) \) implies \( I[q_i[X/E] \Rightarrow p_j] \)
2.2.3 Local Completion

See Sec. 9.2 of [POPL ’79].

Non Distributivity [POPL ’79]

- An abstraction \( \rho \) is \( \cup \)-complete or distributive, whenever the union of abstract properties is abstract:

\[
\forall S \subseteq \rho(\Sigma): \bigcup_{P \in S} \rho(P) = \rho(\bigcup_{P \in S} \rho(P))
\]

- Hence, the abstract union of abstract properties looses no information with respect to their concrete one;

- Otherwise it is \( \cup \)-incomplete or non-distributive.

Example of Non Distributivity [POPL ’79]

- Kildall’s constant propagation \( \{0, \mathbb{Z}\} \cup \{\{i \mid i \in \mathbb{Z}\}, \subseteq\} \)

is not distributive:

\[
\rho(\{1\}) \cup \rho(\{2\}) = \{1, 2\} \neq \mathbb{Z} = \rho(\{1\} \cup \{2\}).
\]

Disjunctive Completion [POPL ’79]

- The \( \cup \)-completion or disjunctive completion \( C(\mathcal{A}) \) of an abstract domain \( \mathcal{A} \) is the smallest distributive abstract domain containing \( \mathcal{A} \);

- The disjunctive completion adds all missing joins to the abstract domain:

\[
C(\mathcal{A}) = \bigcup_{i \in \mathbb{N}} \lambda A. \mathcal{M}(\mathcal{A} \cup \{\bigcup_{P \in S} \rho_A(P) \mid \rho_A(\bigcup_{P \in S} \rho_A(P)) \neq \bigcup_{P \in S} \rho_A(P)\})
\]
Example of Disjunctive Completion [POPL’79]

- Kildall’s constant propagation \( \langle \{0, Z\} \cup \{i\} \mid i \in Z \rangle, \subseteq \)

is not distributive;
- The disjunctive completion is \( \langle p(Z), \subseteq \rangle \) (i.e. identity abstraction).

Reference

Local Image Completeness [POPL’79]

- Given \( f \in p(\Sigma) \rightarrow \rightarrow p(\Sigma) \), the abstraction \( \rho \) is \( f \)-complete iff the \( f \)-transformation of abstract properties is abstract:
  \[
  \forall P \in p(\Sigma) : \rho \circ f \circ \rho(P) = f \circ \rho(P)
  \]
- Hence, the abstract transformation of an abstract property looses no information with respect to the concrete one;
- Otherwise \( \rho \) is \( f \)-incomplete.

Reference

Fixpoint Completion

- We want to prove \( \text{lfp} F \subseteq \gamma(I) \) i.e. \( \alpha(\text{lfp} F) \sqsubseteq I \)
- The abstraction is in general incomplete so \( \text{lfp} F \nsqsubseteq I \)
- Hence we look for the most abstract abstraction \( \hat{\alpha} \) which is more precise than \( \alpha \) and is fixpoint complete:
  \[
  \hat{\alpha}(\text{lfp} F) = \text{lfp} \hat{F} \quad \text{where} \quad \hat{F} = \hat{\alpha} \circ F \circ \hat{\gamma}
  \]
- This is sound since \( \text{lfp} \hat{F} \sqsubseteq I \) implies \( \alpha(\text{lfp} F) \sqsubseteq I \) that is \( \text{lfp} F \subseteq \gamma(I) \)
- This is complete since \( \text{lfp} F \subseteq \hat{\gamma}(I) = \gamma(I) \) so \( \hat{\alpha}(\text{lfp} F) \sqsubseteq I \) i.e. \( \text{lfp} \hat{F} \sqsubseteq I \) is now provable in the abstract.

Reference
- See other completion methods in:

Local Image Completion

- The \( f \)-completion \( c_f(A) \) of an abstract domain \( A \) is the smallest \( f \)-complete abstract domain containing \( A \);
- The local image completion adds all missing abstract elements to the abstract domain:
  \[
  c_f(A) = \text{lfp}_c \lambda A \cdot M(A \cup \{\rho_A(P) \mid \rho_A \circ f \circ \rho_A(P) \neq f \circ \rho_A(P)\})
  \quad (1)
  \]

Reference

An Introduction to Abstract Interpretation, P. Cousot, 23/3/03 — 2:37/102 — Idx, Toc
Local Image and Domain Completeness

- When $\overline{F} = \tilde{\alpha} \circ F \circ \tilde{\gamma}$ and $\tilde{\rho} = \tilde{\gamma} \circ \tilde{\alpha}$, the abstract commutation condition $\tilde{\alpha} \circ F = \overline{F} \circ \tilde{\alpha}$ amounts to local domain completeness $\tilde{\rho} \circ F = \tilde{\rho} \circ F \circ \tilde{\rho}$;
- This is different from local image completeness $F \circ \tilde{\rho} = \tilde{\rho} \circ F \circ \tilde{\rho}$ for which we provided a completion construction (1);
- A common particular case is when $F$ has an adjoint $\tilde{g} F$ such that $h P; \times i$ in which case adjoined local image completeness $\tilde{g} F \circ \tilde{\rho} = \tilde{\rho} \circ F \circ \tilde{\rho}$ implies local domain completeness $\tilde{\rho} \circ F = \tilde{\rho} \circ F \circ \tilde{\rho}$.

Predicate Abstraction Completion

Principle of refinement for $\delta P \left( \{ \mathsf{lfp}_0^C \, \lambda \, X \cdot I \cup \mathsf{post}[t] \, X \} \right)$:
- Start from $P = P_0$;
- Iteratively repeat:
  - Check $\{ \mathsf{lfp}_0^C \, \lambda \, X \cdot I \cup \mathsf{post}[t] \, X \} \subseteq S$ by pred. abs. $P_n$
  - If failed, do local domain completion of $P_n$ into $P_{n+1}$ for adjoint $\text{pre}[t]$ until verification done;
- A few convincing practical experiences e.g. [3]

Exact Fixpoint Abstraction by Adjoint Local Image Completion

When $F$ has an adjoint $\tilde{F}$, a sufficient condition to ensure exact fixpoint abstraction $\tilde{\alpha}(\mathsf{lfp} F) = \mathsf{lfp} \overline{F}$ where $\overline{F} = \tilde{\alpha} \circ F \circ \tilde{\gamma}$ is:

- Local dual image completeness that is $\tilde{F} \circ \tilde{\rho} = \tilde{\rho} \circ F \circ \tilde{\rho}$ (i.e. $F \circ \tilde{\rho} = \tilde{\rho} \circ F \circ \tilde{\rho}$ where $\tilde{\rho} = \tilde{\gamma} \circ \tilde{\alpha}$);
- This can be achieved by refining the original abstract domain $\tilde{\rho}$ by the local image fixpoint completion construction (1);
- This implies local domain completeness $\tilde{\rho} \circ F = \tilde{\rho} \circ F \circ \tilde{\rho}$ (i.e. $F \circ \tilde{\rho} = \tilde{\rho} \circ F \circ \tilde{\rho}$);
- This in turn implies exact/precise fixpoint abstraction $\tilde{\alpha}(\mathsf{lfp} F) = \mathsf{lfp} \overline{F}$ in the refined domain.

1. The local dual image completion can be restricted to the fixpoint iterates.
2. In general, the completed domain does not satisfy the ascending chain condition (see the previous constant propagation example).