2.2 A Short Introduction to Abstract Interpretation Theory (see Sec. 5 of [POPL ’79])

Properties

- We represent properties $P$ of objects $s \in \Sigma$ as sets of objects $P \in p(\Sigma)$ (which have the property in question);

**Example:** the property "to be an even natural number" is $\{0, 2, 4, \ldots\}$.
Complete Lattice of Properties

- The set of properties of objects $\Sigma$ is a complete boolean lattice:
  
  $$(\mathcal{P}(\Sigma), \subseteq, \emptyset, \Sigma, \cup, \cap, \neg).$$

Direction of Approximation

- Approximation from above: approximate $P$ by $\overline{P}$ such that $P \subseteq \overline{P}$;
- Approximation from below: approximate $P$ by $\underline{P}$ such that $\underline{P} \subseteq P$ (dual).

Abstraction

A reasoning/computation such that:

- only some properties can be used;
- the properties that can be used are called "abstract";
- so, the (other concrete) properties must be approximated by the abstract ones;

Abstract Properties

- Abstract Properties: a set $\mathcal{A} \subseteq \mathcal{P}(\Sigma)$ of properties of interest (the only one which can be used to approximate others).
In Absence of (Upper) Approximation

- What to say when some property has no (computable) abstraction?
  - loop?
  - block?
  - ask for help?
  - say something!

I Don’t Know

- Any property should be approximable from above by I don’t know (i.e. “true” or $\Sigma$).

Minimal Approximations

- A concrete property $P \in \rho(\Sigma)$ is most precisely abstracted by any minimal upper approximation $\overline{P} \in \overline{A}$:
  \[ P \subset \overline{P} \]
  \[ \exists \overline{P}' \in \overline{A} : P \subset \overline{P}' \subset \overline{P} \]
- So, an abstract property $\overline{P} \in \overline{A}$ is best approximated by itself.

Which Minimal Approximation is Most Useful?

- Which minimal approximation is most useful depends upon the circumstances;
- Example (rule of signs):
  - $0$ is better approximated as positive in “$3 + 0$”;
  - $0$ is better approximated as negative in “$-3 + 0$”.
Avoiding Backtracking

- We don’t want to exhaustively try all minimal approximations;
- We want to use only one of the minimal approximations;

Which Minimal Abstraction to Use?

- Which minimal abstraction to choose?
  - make a circumstantial choice¹;
  - make a definitive arbitrary choice²;
  - require the existence of a best choice³.

Best Abstraction

- We require that all concrete property $P \in \wp(\Sigma)$ have a best abstraction $\overline{P} \in \overline{A}$:
  \[
  \forall P' \in \overline{A} : (P \subseteq P') \implies (\overline{P} \subseteq \overline{P}')
  \]
- So, by definition of the greatest lower bound/meet $\cap$:
  \[
  \overline{P} = \bigcap \{ P' \in \overline{A} \mid P \subseteq P' \} \in \overline{A}
  \]

Moore Family

- So, the hypothesis that any concrete property $P \in \wp(\Sigma)$ has a best abstraction $\overline{P} \in \overline{A}$ implies that:
  \[
  \overline{A}
  \]
  i.e. it is closed under intersection $\cap$:
  \[
  \forall S \subseteq \overline{A} : \bigcap S \in \overline{A}
  \]
- In particular $\bigcap \emptyset = \Sigma \in \overline{A}$.

Reference

¹ [JLC ’92] uses a concretization function.
² [JLC ’92] uses an abstraction function.
³ [JLC ’92] uses an abstraction/concretization Galois connection (this talk).
Example of Moore Family-Based Abstraction

![Diagram of Moore Family-Based Abstraction]

2.2.2 Closure Operator-Based Abstraction

See Sec. 5.2 of [POPL’79]).

Reference


The Lattice of Abstractions (1)

- The set $\mathcal{M}(\rho(\Sigma))$ of all abstractions i.e. of Moore families on the set $\rho(\Sigma)$ of concrete properties is the complete lattice of abstractions

$$\langle \mathcal{M}(\rho(\Sigma)), \supseteq, \rho(\Sigma), \{\Sigma\}, \lambda S \cdot \mathcal{M}(\cup S), \cap \rangle$$

where:

$$\mathcal{M}(\overline{A}) = \{ \cap S \mid S \subseteq \overline{A} \}$$

is the $\subseteq$-least Moore family containing $\overline{A}$.

Closure Operator Induced by an Abstraction

The map $\rho_{\overline{A}}$ mapping a concrete property $P \in \rho(\Sigma)$ to its best abstraction $\rho_{\overline{A}}(P)$ in $\overline{A}$ is:

$$\rho_{\overline{A}}(P) = \cap \{ \overline{P} \in \overline{A} \mid P \subseteq \overline{P} \}.$$ 

It is a closure operator:
- extensive,
- idempotent,
- isotone/monotonic;

such that

$$P \in \overline{A} \iff P = \rho_{\overline{A}}(P)$$

hence

$$\overline{A} = \rho_{\overline{A}}(\rho(\Sigma)).$$
**Abstraction Induced by a Closure Operator**

- Any closure operator $\rho$ on the set of properties $\rho(\Sigma)$ induces an abstraction: 
  $$\rho(\rho(\Sigma)).$$

**Examples:**
- $\lambda P \cdot P$ the most precise abstraction (identity),
- $\lambda P \cdot \Sigma$ the most imprecise abstraction (I don’t know).

- Closure operators are isomorphic to the Moore families (i.e. their fixpoints).

---

**The Lattice of Abstractions (2)**

- The set $\text{clo}(\rho(\Sigma) \longmapsto \rho(\Sigma))$ of all abstractions, i.e. isomorphically, closure operators $\rho$ on the set $\rho(\Sigma)$ of concrete properties is the complete lattice of abstractions for pointwise inclusion:

  $$\langle \text{clo}(\rho(\Sigma) \longmapsto \rho(\Sigma)), \subseteq, \lambda P \cdot P, \lambda P \cdot \Sigma, \lambda S \cdot \text{ide}(\cup S), \cap \rangle$$

  where:
  - the lub $\lambda S \cdot \text{ide}(\cup S)$ is the reduced product;
  - $\text{ide}(\rho) = \text{lfp}_\rho \lambda f \cdot f \circ f$ is the $\subseteq$-least idempotent operator on $\rho(\Sigma)$ $\subseteq$-greater than $\rho$.

---

**Example of Closure Operator-Based Abstraction**

---

**2.2.4 Galois Connection-Based Abstraction**

See Sec. 5.3 of [POPL ’79].

---

**Reference**

Correspondance Between Concrete and Abstract Properties

- For closure operators $\rho$, we have:
  \[ \rho(P) \subseteq \rho(P') \iff P \subseteq \rho(P') \]
  written:
  \[ \langle p(S), \subseteq \rangle \xrightarrow{\rho^{-1}} \langle p(S), \subseteq \rangle \]
  where 1 is the identity and:
  \[ \langle p(S), \subseteq \rangle \xrightarrow{\gamma} \langle D, \subseteq \rangle \]
  means that $(\alpha, \gamma)$ is a Galois connection:
  - $\forall P \in p(S), \overline{P} \in D : \alpha(P) \subseteq \overline{P} \iff P \subseteq \gamma(\overline{P})$;
  - $\alpha$ is onto (equivalently $\alpha \circ \gamma = 1$ or $\gamma$ is one-to-one).

Galois Surjection

- We have the Galois surjection:
  \[ \langle p(S), \subseteq \rangle \xrightarrow{\iota \circ \rho^{-1}} \langle D, \subseteq \rangle \]
- More generally:
  \[ \langle p(S), \subseteq \rangle \xrightarrow{\gamma} \langle D, \subseteq \rangle \]
  denoting (again) the fact that:
  - $\forall P \in p(S), \overline{P} \in D : \alpha(P) \subseteq \overline{P} \iff P \subseteq \gamma(\overline{P})$;
  - $\alpha$ is onto (equivalently $\alpha \circ \gamma = 1$ or $\gamma$ is one-to-one).

Abstract Domain

- **Abstract Domain**: an isomorphic representation $D$ of the set $A \subseteq p(S) = \rho(p(S))$ of abstract properties (up to some order-isomorphism $\iota$).

Example of Galois Surjection-Based Abstraction

Galois Connection

- Relaxing the condition that \( \alpha \) is onto:
  \[
  (\rho(\Sigma), \subseteq) \xleftarrow{\gamma} (\overline{\mathcal{D}}, \subseteq)
  \]
  that is to say:
  \[
  \forall P \in \rho(\Sigma), \overline{P} \in \overline{\mathcal{D}} : \alpha(P) \subseteq \overline{P} \iff P \subseteq \gamma(\overline{P});
  \]
  - i.e. \( \rho \) is now \( \gamma \circ \alpha \);
  - We can now have different representations of the same abstract property.

Abstraction \( \alpha \)

The Abstraction \( \alpha \) is Monotone

Concretization \( \gamma \)
The Concretization $\gamma$ is Monotone

$X \subseteq Y \Rightarrow \gamma(X) \subseteq \gamma(Y)$

The $\alpha \circ \gamma$ Composition is Reductive

$\alpha \circ \gamma(Y) = \subseteq Y$

The $\gamma \circ \alpha$ Composition is Extensive

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

Composition of Galois Connections

The composition of Galois connections:

$\langle L, \leq \rangle \xleftarrow{\gamma_1 / \alpha_1} \langle M, \subseteq \rangle$

and:

$\langle M, \subseteq \rangle \xleftarrow{\gamma_2 / \alpha_2} \langle N, \leq \rangle$

is a Galois connection:

$\langle L, \leq \rangle \xleftarrow{\gamma_1 \circ \gamma_2 / \alpha_2 \circ \alpha_1} \langle N, \leq \rangle$
2.2.5 Function Abstraction

See Sec. 7.2 of [POPL ’79].

Function Abstraction

\[ F^\sharp = \alpha \circ F \circ \gamma \]

i.e. \( F^\sharp = \rho \circ F \)

\[ \left< P, \subseteq \right> \xleftarrow{\gamma} \left< Q, \subseteq \right> \Rightarrow \]

\[ \left< P, \text{mon}, \subseteq \right> \xleftarrow{\lambda P, \gamma, [\alpha]} \left< Q, \text{mon}, \subseteq \right> \]

Approximate Fixpoint Abstraction

\[ \alpha(\lfp F) \subseteq \lfp F^\sharp \]

See Sec. 7.1 of [POPL ’79].
Exact Abstraction:
\[ \alpha(\text{lfp } F) = \text{lfp } F \]

Exact Fixpoint Abstraction

Approximate Abstraction:
\[ \alpha(\text{lfp } F) \preceq \text{lfp } F \]

2.3 Application to Reachability

Transition systems

- \((S, t)\) where:
  - \(S\) is a set of states/vertices/…
  - \(t \in \wp(S \times S)\) is a transition relation/set of arcs/…
Example of transition system

- $t$  
- $\circ$  
- $\circ$  
- $\circ$  
- $\circ$  
- $\circ$

Reflexive transitive closure

- Composition:
  - $t \circ t' \equiv \{(s, s'') | \exists s' : (s, s') \in t \land (s', s'') \in t'\}$
- Powers:
  - $t^0 \equiv \{s, s | s \in S\}$
  - $t^{n+1} \equiv t^n \circ t \quad n \geq 0$
- Reflexive transitive closure:
  - $t^* = \bigcup_{n \geq 0} t^n$

Example of transitive reflexive closure

- $t^*$

Reflexive transitive closure in fixpoint form

$$t^* = \text{lfp} \subseteq \lambda X. t^0 \cup X \circ t$$

Proof

- $X^0 = \emptyset$
- $X^1 = t^0 \cup X^0 \circ t = t^0$
- $X^2 = t^0 \cup X^1 \circ t = t^0 \cup t^1$
- $\ldots \ldots$
- $X^n = \bigcup_{0 \leq i < n} t^i$ (induction hypothesis)
\[ X^{n+1} = t_0 \cup X^n \circ t \]
\[ = t_0 \cup (\bigcup_{0 \leq i < n} t^i) \circ t \]
\[ = t_0 \cup \bigcup_{0 \leq i < n} (t^i \circ t) \]
\[ = t_0 \cup \bigcup_{1 \leq i+1 < n+1} (t^i+1) \]
\[ = t_0 \cup \bigcup_{1 \leq j < n+1} t^j \circ t \]
\[ = t_0 \cup t^i \quad (0 \leq i < n+1) \]
\[ \ldots \ldots \]

\[ X^\omega = \bigcup_{n \geq 0} X^n \]
\[ = \bigcup_{n \geq 0} \bigcup_{0 \leq i < n} t^i \]
\[ = \bigcup_{n \geq 0} t^n \]
\[ = t^* \]

\[ X^{\omega+1} = t_0 \cup X^\omega \circ t \]
\[ = t_0 \cup (\bigcup_{n \geq 0} t^n) \circ t \]
\[ = t_0 \cup \bigcup_{n \geq 0} (t^n \circ t) \]
\[ = t_0 \cup \bigcup_{n \geq 0} t^n+1 \]
\[ = \bigcup_{k \geq 1} t^k \]
\[ = t^* \]

\[ \text{Iterates} \]

\[ X^0 \quad X^1 \quad X^2 \]
\[ X^3 \quad X^4 \quad X^5 = t^* \]
Post-image

\[
\text{post}[t]I = \{s' \mid \exists s \in I : (s, s') \in t\}
\]

We have \(\text{post}\left[\bigcup_{t \in \Delta} t^\ast\right]I = \bigcup_{t \in \Delta} \text{post}[t^\ast]I\) so \(\alpha = \lambda t \cdot \text{post}[t]I\) is the lower adjoint of a Galois connection.

An Introduction to Abstract Interpretation, P. Cousot, 23/3/03 — 2:70/102 — Ø < Ø > → 1 < Ø ? > Ý, Toc

Fixpoint abstraction, once again

Let \(F \in L \mapsto L\) and \(\mathcal{F} \in \mathcal{L} \mapsto \mathcal{L}\) be respective monotone maps on the cpos \((L, \bot, \sqsubseteq)\) and \((\mathcal{L}, \mathcal{I}, \sqsubseteq)\) and \((L, \sqsubseteq) \xrightarrow{\gamma} (\mathcal{L}, \sqsubseteq)\) such that \(\alpha \circ F \subseteq \gamma \subseteq \mathcal{F}\). Then \(\gamma\):

- \(\forall \delta \in \Theta: \alpha(F^\delta) \subseteq F^\delta\) (iterates from the infimum);
- The iteration order of \(\mathcal{F}\) is \(\leq\) to that of \(F\);
- \(\alpha(\text{lfp} F) \subseteq \text{lfp} F\);

Soundness: \(\text{lfp} F \subseteq \text{lfp} F \Rightarrow \text{lfp} F \subseteq \gamma(F)\).

---

Reachable states

\[
\text{post}[t^\ast]I
\]

An Introduction to Abstract Interpretation, P. Cousot, 23/3/03 — 2:72/102 — Ø < Ø > → 1 < Ø ? > Ý, Toc

Postimage Galois connection

Given \(I \in \wp(S)\),

\[
\langle \wp(S \times S), \subseteq \rangle \xrightarrow{\gamma} \langle \wp(S), \subseteq \rangle
\]

\(\text{post}[t]I \subseteq R\)

\[
\equiv \{s' \mid \exists s \in I : \langle s, s' \rangle \in t\} \subseteq R
\]

\(\forall s' \in S : (\exists s \in I : \langle s, s' \rangle \in t) \Rightarrow (s' \in R)\)

\(\forall s', s \in S : (s \in I \land \langle s, s' \rangle \in t) \Rightarrow (s' \in R)\)

\(\forall s', s \in S : \langle s, s' \rangle \in t \Rightarrow ((s \in I) \Rightarrow (s' \in R))\)

\(t \subseteq \{(s, s') \mid (s \in I) \Rightarrow (s' \in R)\}\) \(\equiv \gamma(R)\)

An Introduction to Abstract Interpretation, P. Cousot, 23/3/03 — 2:71/102 — Ø < Ø > → 1 < Ø ? > Ý, Toc

Numerous variants!

Fixpoint abstraction (continued)

Moreover, the commutation condition $F' \circ \alpha = \alpha \circ F$ implies:

- $F' = \alpha \circ F \circ \gamma$, and
- $\alpha(\text{lfp} F) = \text{lfp} F$.

Completeness: $\text{lfp} F \subseteq \gamma(F) \Rightarrow \text{lfp} F \subseteq F$.

\[\text{Discovering } F \text{ by calculus}\]

\[\alpha \circ (\lambda X \cdot t^0 \cup X \circ t) = \lambda X \cdot (t^0 \cup X \circ t) = \lambda X \cdot (t^0) \cup \alpha(X \circ t) = \lambda X \cdot \text{post}[t^0]I \cup \text{post}[X \circ t]I\]

Reachable states in fixpoint form

\[\text{post}[t^*]I, \ I \text{ given}\]
\[= \alpha(t^*) \quad \text{where } \alpha(t) = \text{post}[t]I = \{s' \mid \exists s \in I : \langle s, s' \rangle \in t\}\]
\[= \alpha(\text{lfp} \lambda X \cdot t^0 \cup X \circ t)\]
\[= \text{lfp} \subseteq F \subseteq F\]
\[= \text{post}[t^0]I\]
\[= \{s' \mid \exists s \in I : \langle s, s' \rangle \in t^0\}\]
\[= \{s' \mid \exists s \in I : \langle s, s' \rangle \in \{\{s, s \mid s \in S\}\} \}
\[= \{s' \mid \exists s \in I\}
\[= I\]
\[
\text{post}[X \circ t]I
= \{s' \mid \exists s \in I : \langle s, s' \rangle \in (X \circ t)\}
= \{s' \mid \exists s \in I : \exists s'' \in S : \langle s, s'' \rangle \in X \land \langle s', s'' \rangle \in t\}
= \{s' \mid \exists s \in I : \exists s'' \in S \cup \{s'\} : s'' \in X \land \langle s', s'' \rangle \in t\}
= \{s' \mid \exists s'' \in S : s'' \in post[X]I \land \langle s', s'' \rangle \in t\}
= \text{post}[t](\alpha(X))
\]

\[
\alpha \circ (\lambda X \cdot t^0 \cup X \circ t)
= \ldots
= \lambda X \cdot \text{post}[t^0]I \cup \text{post}[X \circ t]I
= \lambda X \cdot I \cup \text{post}[t](\alpha(X))
= \lambda X \cdot F(\alpha(X))
\]

by defining:
\[
F = \lambda X \cdot I \cup \text{post}[t](X)
\]
proving:
\[
\text{post}[t^*](I) = \text{lfp}^{\subseteq} \lambda X \cdot I \cup \text{post}[t](X) \tag{2}
\]