Background material for the Course
GCSCI-GA.3033-011 “Principles of Software Security”, New York University, CIMS, CS, Fall 2013

Patrick Cousot
CIMS, NYU

September 3, 2013
Chapter 11

Fixpoint Abstraction

Many problems in program static analysis (Cousot and Cousot, 1977a) and verification (Cousot and Cousot, 1979b) amount to proving a property of a program fixpoint \( \text{lfp} \subseteq F \) where the transformer \( F[P] \) is defined by induction on the syntax program \( P \) to be verified.

For decidable verification problems for \( P \), the fixpoint \( \text{lfp} \subseteq F \) may not be computable but an abstraction of the fixpoint might be. To effectively solve the problem, the abstraction must often be exact as studied in section 11.2.

For undecidable verification problems for \( P \) (chapter 10), the fixpoint \( \text{lfp} \subseteq F \) is in general not computable and its abstractions are either not effectively computable or too abstract to solve the problem. In that case an approximate solution can nevertheless be effectively computed as studied in section 11.1.

So, given a fixpoint \( \text{lfp} \subseteq F \) of a \( \subseteq \)-increasing set transformer \( F \in \wp(C) \rightarrow \wp(C) \) as in chapter 7, and a Galois connection \( \langle \wp(C), \subseteq \rangle \rightleftarrows \langle \wp(A), \subseteq \rangle \) we study in this chapter 11 how to calculate exactly or approximate \( \alpha(\text{lfp} \subseteq F) \) in the abstract domain \( \langle \wp(A), \subseteq \rangle \) only.

11.1 Fixpoint Overapproximation

The objective of static analysis or verification is to infer or check properties of a program \( P \) that can be shown to be the least fixpoint \( \text{lfp} \subseteq F[P] \) of a computer-representable set transformer \( F[P] \) that we can automatically computed from the text of the program \( P \).

The problem is that \( \text{lfp} \subseteq F[P] \) is not automatically computable since the property inference problem is undecidable (as soon as the property to be inferred is not trivial). In that case the iterates of theorem 71 are in general convergent only after infinitely many iterations steps.

The solution in static analysis, typing, etc. is to invent a Galois connection to approximate the desired property in the abstract thanks to a computable fixpoint calculated in the abstract domain only. The crucial point is that Galois connections preserve limits (theorem 162) hence fixpoints, which is made precise in theorem 165 from (Cousot and Cousot, 1977a, § 8.1) (Cousot, 1978) (Cousot and Cousot, 1979b, Theorem 7.1.0.4.(2)).
Theorem 165. If \( \langle \varphi(C), \subseteq \rangle \xrightarrow{\gamma} \langle \varphi(A), \subseteq \rangle \), \( F \in \varphi(C) \xrightarrow{\alpha} \varphi(C) \) and \( \mathcal{F} \in \varphi(A) \xrightarrow{\alpha} \varphi(A) \) are increasing then \( \alpha \circ F \subseteq \mathcal{F} \circ \alpha \) if and only if \( \mathcal{F} \circ \gamma \subseteq \mathcal{F} \circ \alpha \), either implying \( \alpha \circ F \circ \gamma \subseteq \mathcal{F} \circ \alpha \circ \gamma \) and \( \alpha(\text{lfp}^\subseteq F) \subseteq \text{lfp}^\subseteq_{\alpha(A)} \mathcal{F} \) when \( A \subseteq F(A) \).

The situation described by theorem 165 is illustrated by the following schema where \( \alpha(\text{lfp}^\subseteq F) \subseteq \text{lfp}^\subseteq \mathcal{F} \) so that the abstraction \( \alpha(\text{lfp}^\subseteq F) \) of the concrete fixpoint is strictly more precise than the abstract fixpoint \( \text{lfp}^\subseteq \mathcal{F} \). The benefit of this abstraction is in general that the concrete fixpoint \( \text{lfp}^\subseteq F \) hence its abstraction \( \alpha(\text{lfp}^\subseteq F) \) is not computable whereas \( \text{lfp}^\subseteq \mathcal{F} \) is computable and so provides the information that the concrete fixpoint is definitely below \( \gamma(\text{lfp}^\subseteq \mathcal{F}) \).

PROOF. Let us prove that \( \alpha \circ F \subseteq \mathcal{F} \circ \alpha \) if and only if \( \mathcal{F} \circ \gamma \subseteq \mathcal{F} \circ \alpha \circ \gamma \).

\[
\begin{align*}
\alpha \circ F & \subseteq \mathcal{F} \circ \alpha \quad \text{\{pointwise def.} \ 
\Rightarrow \quad & \alpha \circ F \circ \gamma \subseteq \mathcal{F} \circ \alpha \circ \gamma \quad \text{\{pointwise def.}} \ 
\Rightarrow \quad & F \circ \gamma \subseteq \mathcal{F} \circ \alpha \circ \gamma \quad \text{\{def.} \ \langle \varphi(C), \subseteq \rangle \xrightarrow{\gamma} \langle \varphi(A), \subseteq \rangle \} \ 
\Rightarrow \quad & F \circ \gamma \subseteq \mathcal{F} \circ \alpha \quad \text{\{\gamma \circ \alpha \text{ reductive, \mathcal{F} increasing and transitivity}} \} \ 
\Rightarrow \quad & F \subseteq \mathcal{F} \circ \alpha \quad \text{\{\alpha \circ \gamma \text{ reductive, \mathcal{F} increasing and transitivity}} \} \ 
\Rightarrow \quad & \alpha \circ F \subseteq \mathcal{F} \circ \alpha \quad \text{\{def.} \ \langle \varphi(C), \subseteq \rangle \xrightarrow{\alpha} \langle \varphi(A), \subseteq \rangle \} \ 
\end{align*}
\]

which, together with \( \mathcal{F} \in \varphi(A) \xrightarrow{\alpha} \varphi(A) \) increasing, implies that \( \text{lfp}^\subseteq_{\alpha(A)} \mathcal{F} \) is well-defined.
CHAPTER 11. FIXPOINT ABSTRACTION

\[ F \circ \gamma \subseteq \gamma \circ F \tag*{\text{by hypothesis}} \]
\[ \Rightarrow F \circ \gamma (\text{lfp}^c_{\alpha(A)} F) \subseteq \gamma \circ F(\text{lfp}^c_{\alpha(A)} F) \tag*{\text{pointwise def.} \subseteq} \]
\[ \Rightarrow F(\gamma (\text{lfp}^c_{\alpha(A)} F)) \subseteq \gamma (\text{lfp}^c_{\alpha(A)} F) \tag*{\text{fixpoint definition}} \]
\[ \Rightarrow \gamma (\text{lfp}^c_{\alpha(A)} F) \in \{ X \in \wp(C) \mid A \subseteq X \land F(X) \subseteq X \} \tag*{\text{by} \alpha(A) \subseteq \text{lfp}^c_{\alpha(A)} F \text{so} A \subseteq \gamma (\text{lfp}^c_{\alpha(A)} F) \text{by G.C. and def.} \subseteq} \]
\[ \Rightarrow \gamma (\text{lfp}^c_{\alpha(A)} F) \supseteq \bigcap \{ X \in \wp(C) \mid A \subseteq X \land F(X) \subseteq X \} \tag*{\text{def. glb}} \]
\[ \Rightarrow \gamma (\text{lfp}^c_{\alpha(A)} F) \supseteq \text{lfp}^c_{\alpha} F \tag*{\text{Tarski’s fixpoint corollary 67}} \]
\[ \Rightarrow \alpha (\text{lfp}^c_{\alpha} F) \subseteq \text{lfp}^c_{\alpha(A)} F \tag*{\text{by def.} \langle \wp(C), \subseteq \rangle \overset{\gamma}{\longrightarrow} \langle \wp(A), \subseteq \rangle} \]

While fixpoint approximation theorem 165 is based on fixpoint iteration theorem 71, the following one (Cousot and Cousot, 1997, Theorem 10) is based on Tarski’s fixpoint theorem 65, that is the over-approximation of postfixpoints.

**Theorem 166.** Assume that \( F \in \wp(C) \overset{\longrightarrow}{\rightarrow} \wp(A) \) is increasing, \( F \in \wp(A) \overset{\longrightarrow}{\rightarrow} \wp(A) \), \( \alpha \in \wp(C) \overset{\longrightarrow}{\rightarrow} \wp(A) \) is increasing and satisfies the postfixpoint approximation condition
\[
\forall Y \in \wp(A) : F(Y) \subseteq Y \Rightarrow \exists X \in \wp(A) : \alpha(X) \subseteq Y \land F(X) \subseteq X
\]
then \( \alpha (\text{lfp}^c F) \subseteq \text{lfp}^c_{\alpha(A)} F \).

**Proof.** We have
\[
\alpha (\text{lfp}^c F) = \alpha (\bigcap \{ X \in \wp(C) \mid F(X) \subseteq X \}) \tag*{\text{Tarski’s fixpoint theorem ??}}
\subseteq \bigcap \{ \alpha(X) \in \wp(A) \mid F(X) \subseteq X \} \tag*{\alpha increasing and exercise 2.26-8}
\subseteq \bigcap \{ Y \in \wp(A) \mid \alpha(X) \subseteq Y \land F(X) \subseteq X \} \tag*{\text{def. glb} \bigcap}
\subseteq \bigcap \{ Y \in \wp(A) \mid F(Y) \subseteq Y \} \tag*{postfixpoint approximation condition so \( Y \in \wp(A) \mid F(Y) \subseteq Y \subseteq \{ Y \in \wp(A) \mid F(X) \subseteq X \} \text{ and def. glb} \bigcap}
= \alpha (\text{lfp}^c F) \tag*{\text{Tarski’s fixpoint theorem ??}}
\]

**Dual theorems 165 and 165** apply to the greatest fixpoint \( \text{gfp} \).

### 11.2 Exact Fixpoint Abstraction

In some cases the abstraction is exact which means that the abstraction of the concrete fixpoint can be exactly computed in the abstract domain only as shown by the following theorem 167 from (Cousot, 1978), (Cousot and Cousot, 1979b, Theorem 7.1.0.4(3)), (de Bakker, Meyer and Zucker, 1983, lemma 4.3), (Apt and Plotkin, 1986, fact 2.3).
Theorem 167. Assume \( \langle \wp(C), \subseteq \rangle \leadsto \langle \wp(A), \subseteq \rangle \), \( F \in \wp(C) \rightarrow \wp(C) \) is increasing and \( F \in \wp(A) \rightarrow \wp(A) \) satisfies the commutation condition \( \alpha \circ F = F \circ \alpha \). Then

(a) if \( \langle \wp(C), \subseteq \rangle \xrightarrow{\gamma}{\alpha} \langle \wp(A), \subseteq \rangle \) then \( F = \alpha \circ F \circ \gamma \) (so \( F \) is increasing);

(b) If \( F \) is increasing and \( A \subseteq F(A) \) then \( \alpha(lfp^C \ F) = lfp^C_{\alpha(A)} F \).

The situation described by theorem 167 is illustrated by the following schema and corresponds to the ideal situation where the abstraction of the concrete fixpoint \( \alpha(lfp^C \ F) = lfp^C_{\alpha(A)} F \) can be computed exactly in the abstract with no need to compute the concrete fixpoint \( lfp^C \ F \) at all.

\[
\begin{array}{c}
lfp^C F \quad \gamma \quad \alpha \\
\downarrow \\
lfp^C F = \alpha(lfp^C F)
\end{array}
\]

Proof.

\[
\begin{align*}
\alpha \circ F &= F \circ \alpha & \{ \text{by hypothesis} \} \\
\Rightarrow \alpha \circ F \circ \gamma &= F \circ \alpha \circ \gamma & \{ \text{function application} \} \\
\Rightarrow \alpha \circ F \circ \gamma &= F & \{ \text{since } \langle \wp(C), \subseteq \rangle \xrightarrow{\gamma}{\alpha} \langle \wp(A), \subseteq \rangle \text{ implies } \gamma \circ \alpha = 1_{\wp(A)} \} \\
\end{align*}
\]

Then \( F = \alpha \circ F \circ \gamma \) is the composition of increasing function so is increasing.

\[
\begin{align*}
A \subseteq F(A) & \{ \text{by hypothesis} \} \\
\Rightarrow \alpha(A) \subseteq \alpha(F(A)) & \{ \alpha \text{ increasing by theorem 162} \} \\
\Rightarrow \alpha(A) \subseteq F(\alpha(A)) & \{ \text{by the commutation condition so } lfp^C_{\alpha(A)} F \text{ is well-defined} \} \\
\Rightarrow \alpha \circ F &= F \circ \alpha & \{ \text{function application} \} \\
\Rightarrow \alpha(F(lfp^C_{\alpha(A)} F)) &= F(\alpha(lfp^C_{\alpha(A)} F)) & \{ \text{fixpoint definition} \} \\
\Rightarrow \alpha(lfp^C_{\alpha(A)} F) &= F(\alpha(lfp^C_{\alpha(A)} F)) & \{ \text{def. least fixpoint and } A \subseteq lfp^C_{\alpha(A)} F \text{ so } \alpha(A) \subseteq \alpha(lfp^C_{\alpha(A)} F) \} \\
\Rightarrow lfp^C_{\alpha(A)} F &= \alpha(lfp^C_{\alpha(A)} F) & \{ \text{theorem 165 and antisymmetry} \}
\end{align*}
\]
CHAPTER 11. FIXPOINT ABSTRACTION

The reciprocal of $167.(a)$ does not hold in that we may have $\langle \wp(C), \subseteq \rangle \xrightarrow{\gamma / \alpha} \langle \wp(A), \subseteq \rangle$, $F \in \wp(C) \xrightarrow{\rightarrow} \wp(C)$ is $\subseteq$-increasing, $F \triangleq \alpha \circ F \circ \gamma$, and $\alpha \circ F \subsetneq F \circ \alpha$.

**Counter-example 168.** In the following counter-example,

![Diagram](image)

we have $\alpha \circ F(\emptyset) = \emptyset \subsetneq \{0\} = F \circ \alpha(\emptyset)$ which is the composition of increasing functions hence increasing.

**Remark 169.** In order to apply fixpoint abstraction theorem 167 when knowing $\langle \wp(C), \subseteq \rangle \xrightarrow{\alpha} \langle \wp(A), \subseteq \rangle$ and $F \in \wp(C) \xrightarrow{\rightarrow} \wp(C)$, we have to discover an abstract transformer $F$ satisfying $\alpha \circ F = F \circ \alpha$. The abstract transformer $F$ can be discovered by calculus. Starting from expression $\alpha \circ F(X)$ where $X \in \wp(C)$, we expand this expression and transform it so as to push the abstraction $\alpha$ inside this expression to make it appear as the parameter of a transformed expression $\text{expr} \circ \alpha(X)$ that can be taken as the definition of $F \triangleq \text{expr}$.

This methodological remark is illustrated by the following examples 170 and 171.

**Example 170.** Let $R^* \in \wp(\mathcal{U} \times \mathcal{U})$ be a binary relation on a set $\mathcal{U}$. To prove $(R^*)^{-1} = (R^{-1})^*$, we can observe, by exercise 8.12-2 that

$$\langle \wp(\mathcal{X} \times \mathcal{Y}), \subseteq \rangle \xrightarrow{\lambda \mathcal{R} \cdot \mathcal{X}^{-1} / \lambda \mathcal{R} \cdot \mathcal{X}^{-1}} \langle \wp(\mathcal{Y} \times \mathcal{X}), \subseteq \rangle.$$ (G.C. (8.35))

and, by example 72, $R^* = \text{lpf} \subseteq \lambda \mathcal{X} \cdot 1_\mathcal{U} \cup R^*_\mathcal{Y}$ so $(R^*)^{-1} = (\text{lpf} \subseteq \lambda \mathcal{X} \cdot 1_\mathcal{U} \cup R^*_\mathcal{Y})^{-1}$. Applying theorem 167, we get the fixpoint form by calculating $(Y \in \wp(\mathcal{U} \times \mathcal{U}))$

$$\left( \lambda \mathcal{X} \cdot (R^{-1} \circ \lambda \mathcal{X} \cdot 1_\mathcal{U} \cup R^*_\mathcal{Y}) \right)(Y)$$

$$= (1_\mathcal{U} \cup R^*_\mathcal{Y})^{-1}$$  \(\text{def. function composition } \circ \text{ and } \lambda\text{-application}\)

$$= (1_\mathcal{U})^{-1} \cup (R^*_\mathcal{Y})^{-1} \quad \{ \text{def. inverse }^{-1} \}$$

147
$$= 1 \cup (Y)^{-1} \circ (R)^{-1} \quad \text{\{def. inverse}^{-1}\}$$
$$= (\lambda X \cdot 1 \cup X \circ (R)^{-1} \circ \lambda R \cdot (R)^{-1})(Y) \quad \text{\{def. function composition \circ and \lambda-application}\}$$

so that \((\operatorname{lfp}_\alpha \lambda X \cdot 1 \cup X \circ (R)^{-1})^{-1} = \operatorname{lfp}_\alpha \lambda X \cdot 1 \cup X \circ (R)^{-1} = (R^{-1})^*\) by example 72.

**Example 171.** In examples 72 and 74, we have shown that the reflexive transitive closure of a relation \(R \in \wp(\mathcal{U} \times \mathcal{U})\) is \(R^* = \operatorname{lfp}_\alpha F\) where \(F(X) \triangleq 1 \cup X \circ R\). Recall the Galois connection \(\langle \wp(\mathcal{U} \times \mathcal{U}), \subseteq \rangle \xrightarrow{\lambda Y \cdot \{ (x, y) | x \in \mathcal{I}, \exists y \in \mathcal{U} \} \circ \lambda R \cdot \operatorname{post}[R](\mathcal{I}) \rangle \xleftarrow{G.C. \ (8.19)} \langle \wp(\mathcal{U}), \subseteq \rangle \) from theorem 111. Our objective is to find a fixpoint characterization of \(\operatorname{post}[R^*](\mathcal{I}) = \operatorname{post}[\operatorname{lfp}_\alpha F](\mathcal{I})\).

So we let \(X \in \wp(\mathcal{U} \times \mathcal{U})\) and calculate

\[
\begin{align*}
&= \operatorname{post}[F(X)](\mathcal{I}) \\
&= \operatorname{post}[1 \cup X \circ R](\mathcal{I}) \quad \text{\{def. F\}} \\
&= \{ y \in \mathcal{U} | \exists x \in \mathcal{I} : 1 \cup x \circ (X \circ R) (y, x) \} \\
&= \mathcal{I} \cup \{ y \in \mathcal{U} | \exists x \in \mathcal{I} : (X \circ R)(x, y) \} \\
&= \mathcal{I} \cup \{ y \in \mathcal{U} | \exists z \in \mathcal{U} : (X \circ R)(x, z) \} \\
&= \mathcal{I} \cup \{ y \in \mathcal{U} | \exists z \in \mathcal{U} : (X \circ R)(x, z) \} \\
&= \mathcal{I} \cup \{ y \in \mathcal{U} | \exists z \in \mathcal{U} : (X \circ R)(x, z) \} \\
&= \mathcal{I} \cup \{ y \in \mathcal{U} | \exists z \in \mathcal{U} : (X \circ R)(x, z) \} \\
&= \mathcal{I} \cup \{ y \in \mathcal{U} | \exists z \in \mathcal{U} : (X \circ R)(x, z) \} \\
&= \mathcal{I} \cup \{ y \in \mathcal{U} | \exists z \in \mathcal{U} : (X \circ R)(x, z) \} \\
&= \mathcal{I} \cup \{ y \in \mathcal{U} | \exists z \in \mathcal{U} : (X \circ R)(x, z) \} \\
&= \mathcal{I} \cup \{ y \in \mathcal{U} | \exists z \in \mathcal{U} : (X \circ R)(x, z) \} \\
&= \mathcal{I} \cup \{ y \in \mathcal{U} | \exists z \in \mathcal{U} : (X \circ R)(x, z) \} \\
&= \mathcal{I} \cup \{ y \in \mathcal{U} | \exists z \in \mathcal{U} : (X \circ R)(x, z) \} \\
&= \mathcal{I} \cup \{ y \in \mathcal{U} | \exists z \in \mathcal{U} : (X \circ R)(x, z) \} \\
&= \mathcal{I} \cup \{ y \in \mathcal{U} | \exists z \in \mathcal{U} : (X \circ R)(x, z) \} \\
&= \mathcal{I} \cup \{ y \in \mathcal{U} | \exists z \in \mathcal{U} : (X \circ R)(x, z) \} \\
&= \mathcal{I} \cup \{ y \in \mathcal{U} | \exists z \in \mathcal{U} : (X \circ R)(x, z) \} \\
&= \mathcal{I} \cup \{ y \in \mathcal{U} | \exists z \in \mathcal{U} : (X \circ R)(x, z) \}
\end{align*}
\]

By 167.(a), \(F\) is increasing and so, by 167.(b), \(\operatorname{post}[R^*](\mathcal{I}) = \operatorname{lfp}_\alpha \lambda X \cdot \mathcal{I} \cup \operatorname{post}[R](\mathcal{I})\).

We observe that we can get rid of the hypothesis that \(\mathcal{I} \neq \emptyset\) in theorem 111 since \(\operatorname{post}[R^*](\emptyset) = \operatorname{lfp}_\alpha \lambda X \cdot \operatorname{post}[R](\mathcal{I}) = \emptyset\). Observing that \(\text{pre}[R] = \operatorname{post}[R^{-1}]\) and \((R^*)^{-1} = (R^{-1})^*\) by example 170, we conclude that
CHAPTER 11. FIXPOINT ABSTRACTION

**Theorem 172.** Let $X$ be a set, $I \in \wp(X)$ be a subset of $X$, and $R \in \wp(X \times Y)$ be a relation on $X$. Then \(\text{post} [R^*] I = \text{lfp}_s \lambda X \cdot I \cup \text{post}[R](X)\) and \(\text{pre}[R^*] I = \text{lfp}_s \lambda X \cdot I \cup \text{pre}[R](X)\).

When the concrete transformer is continuous, we can strengthen the fixpoint abstraction result e.g. (Cousot, 2002, Theorem 3).

**Theorem 173 (Exact iterative fixpoint abstraction).** Let $F \in \phi(C) \mapsto \wp(C)$ be a $\subseteq$-continuous transformer, let $I_F \triangleq \{ F_n \mid n \in \mathbb{N} \} \cup \{ \bigcup_{n \in \mathbb{N}} F_n \}$ be the set of iterates of $F$ (such that $F_0 \triangleq \emptyset$ and $F_{n+1} \triangleq F(F_n)$), assume $\langle I_F, \subseteq \rangle \xrightarrow{\alpha} \langle \wp(A), \subseteq \rangle$ to be an abstraction along the iterates of $F$, and that $F \in \wp(A) \mapsto \wp(A)$ satisfies the commutation property $\alpha \circ F = F \circ \alpha$ on $I_F$. Then

(a) $\alpha(\text{lfp} \uparrow F) = \bigcup_{n \in \mathbb{N}} F^n$ is a fixpoint of $F$, not necessarily the least one, if any.

(b) If $\alpha$ surjective then $F = \alpha \circ F \circ \gamma$ and $F$ is $\subseteq$-increasing.

(c) If $F$ is $\subseteq$-increasing then $\alpha(\text{lfp} \uparrow F) = \bigcup_{n \in \mathbb{N}} F^n = \text{lfp} \uparrow \text{post}[F]$ is the least fixpoint of $F$.

**Proof.** We have $\emptyset \in I_F$ and $\emptyset \subseteq \gamma(\emptyset)$ so $\alpha(\emptyset) = \emptyset$ proving $\alpha(F_0) = \emptyset = F^0$. If, by recurrence hypothesis, $\alpha(F_n) = F^n$ for $n \in \mathbb{N}$ then, by definition of the iterates and the commutation condition, $\alpha(F_{n+1}) = \alpha(F(F_n)) = F(\alpha(F_n)) = F(F^n) = F^{n+1}$. By recurrence, $\forall n \in \mathbb{N} : \alpha(F_n) = F^n$.

If $X = F(X)$ is a fixpoint of $F$ then $\alpha(X) = \alpha(F(X)) = F(\alpha(X))$ so $\alpha(X)$ is a fixpoint of $F$. In particular, $\alpha(\text{lfp} \uparrow F)$ is a fixpoint of $F$.

By theorem 71, $\text{lfp} \uparrow F = \bigcup_{n \in \mathbb{N}} F_n$ so $\alpha(\text{lfp} \uparrow F) = \alpha(\bigcup_{n \in \mathbb{N}} F_n) = \bigcup_{n \in \mathbb{N}} \alpha(F_n)$ by $\langle I_F, \subseteq \rangle \xrightarrow{\alpha} \langle \wp(A), \subseteq \rangle$ and theorem 162. But $\forall n \in \mathbb{N} : \alpha(F_n) = F^n$, so $\alpha(\text{lfp} \uparrow F) = \bigcup_{n \in \mathbb{N}} F^n$ is a fixpoint of $F$. The following counter-example shows that this is not necessarily the least fixpoint, if any.
If $\alpha$ is surjective, then by the commutation property, $\alpha \circ F \circ \gamma = \overline{F} \circ \alpha \circ \gamma = F$ since $\alpha \circ \gamma$ is the identity by theorem 120. $F$ is continuous hence increasing so $\overline{F}$ is the composition of increasing functions hence increasing.

Assume $\overline{F}$ to be increasing. Let $Y = \overline{F}(Y)$ be any fixpoint of $\overline{F}$. We have $\overline{F}^0 = \emptyset \subseteq Y$. Assume $\overline{F}^n \subseteq Y$ by recurrence hypothesis. $\overline{F}^{n+1} = \overline{F}(\overline{F}^n) \subseteq \overline{F}(Y) = Y$ since $\overline{F}$ is increasing and by the fixpoint property. By recurrence, $\forall n \in \mathbb{N} : \overline{F}^n \subseteq Y$ so $\alpha(\text{lfp} \subseteq F) = \bigcup_{n \in \mathbb{N}} \overline{F}^n \subseteq Y$ proving that $\alpha(\text{lfp} \subseteq F) = \bigcup_{n \in \mathbb{N}} \overline{F}^n = \text{lfp} \subseteq F$. ■

The fixpoint abstraction can also be based on the abstraction of postfixpoints (Cousot and Cousot, 1997, Theorem 12) (Cousot, 2002, Theorem 4).

**Theorem 174.** Assume that $F \in \wp(\mathcal{C}) \twoheadrightarrow \wp(\mathcal{C})$ and $\overline{F} \in \wp(\mathcal{A}) \twoheadrightarrow \wp(\mathcal{A})$ are increasing and $\alpha \in \{X \in \wp(\mathcal{C}) \mid F(X) \subseteq X\} \mapsto \wp(\mathcal{A})$ satisfies

(a) $\alpha$ preserves meets $\bigcap^a$  
(b) $F \circ \alpha \subseteq \alpha \circ F$  
(c) $\forall Y \in \wp(\mathcal{A}) : \overline{F}(Y) \subseteq Y \Rightarrow \exists X \in \wp(\mathcal{A}) : \alpha(X) \subseteq Y \land F(X) \subseteq X$

then $\alpha(\text{lfp} \subseteq F) = \text{lfp} \subseteq \overline{F}$.

---or equivalently $\langle \wp(\mathcal{A}), \subseteq \rangle \xrightarrow{\alpha} \langle \wp(\mathcal{C}), \subseteq \rangle$, by theorem 162.

**Proof.** We have

$\alpha(\text{lfp} \subseteq F)$

$= \alpha(\bigcap\{X \in \wp(\mathcal{C}) \mid F(X) \subseteq X\})$

(by Tarski’s fixpoint theorem ??)
CHAPTER 11. FIXPOINT ABSTRACTION

\[ \bigcap \{ \alpha(X) \in \wp(A) \mid F(X) \subseteq X \} \tag{11.1} \]

\[ \subseteq \bigcap \{ Y \in \wp(A) \mid \alpha(X) \subseteq Y \land F(X) \subseteq X \} \]

\[ \subseteq \bigcap \{ Y \in \wp(A) \mid F(Y) \subseteq Y \} \]

\[ \text{\[postfix\ approximation\ condition \ so \} \{ Y \in \wp(A) \mid F(Y) \subseteq Y \} \subseteq \{ Y \in \wp(A) \mid \alpha(X) \subseteq Y \land F(X) \subseteq X \} \text{ and def. glb } \bigcap \]}

\[ \bigcap \{ Y \in \wp(A) \mid F(Y) \subseteq Y \} \]

\[ \supseteq \bigcap \{ Y \in \wp(A) \mid F(Y) \subseteq Y \} \]

\[ \bigcap \{ Y \in \wp(A) \mid F(Y) \subseteq Y \} \subseteq \{ Y \in \wp(A) \mid \alpha(X) \subseteq Y \land F(X) \subseteq X \} \text{ and def. glb } \bigcap \]

\[ \bigcap \{ Y \in \wp(A) \mid F(Y) \subseteq Y \} \]

\[ \bigcap \{ Y \in \wp(A) \mid F(Y) \subseteq Y \} \]

\[ \alpha(\text{lfp } \subseteq F) \]

\[ \text{\{Tarski’s fixpoint theorem \[\}\} } \]

Dual theorems 167 and 174 apply to the greatest fixpoint gfp.

11.3 Bibliography

Exact fixpoint abstraction is the basis for establishing correspondences between various semantics of programs (Cousot, 2002). Many grammar manipulating algorithms compute fixpoints exactly abstracting the grammar semantics, see exercise 11.4-2 for an example and (Cousot and Cousot, 2003; Cousot and Cousot, 2006; Cousot and Cousot, 2011) in full generality.

Fixpoint approximation is the basis for finding approximate solutions to undecidable problems expressed as an uncomputable concrete fixpoint, as found in static program analysis (Cousot and Cousot, 1977a; Cousot and Cousot, 1979b), typing (Cousot and Cousot, 1977b; Cousot, 1997), abstract model checking (Cousot, 2000), etc.

11.4 Exercises

Exercise 11.4-1 Let \( C \) and \( \mathcal{A} \) be sets, \( f \in C \mapsto \mathcal{C}, \mathcal{F} \in \mathcal{A} \mapsto \mathcal{A} \), and \( \alpha \in C \mapsto \mathcal{A} \) such that\( \alpha \circ f = \mathcal{F} \circ \alpha \). Prove that \( \alpha(\text{lfp } f^*) = \text{lfp } \mathcal{F}^* \).

Exercise 11.4-2 The terminal language generated by the following context free grammar (where \( \varepsilon \) denotes the empty sentence \( \varepsilon \), see exercise 7.7-6)

\[
X ::= \forall a
\]

\[
Y ::= bX \mid \varepsilon
\]
for each non-terminal $N \in \mathbb{N} \triangleq \{x, y\}$ is $\text{lfp}^\subseteq F$ where

$$F((X, Y)) \triangleq \langle \{\omega a \mid \omega \in Y\}, \{b\omega \mid \omega \in X\} \cup \{\epsilon\} \rangle.$$  

Consider the first abstraction 

$$\text{First}^2((X, Y)) \triangleq \langle \text{First}^* (X), \text{First}^* (Y) \rangle$$

$$\text{First}^* \triangleq \{\text{First}(\omega) \mid \omega \in X\}$$

$$\text{First}(\epsilon) \triangleq \epsilon$$

$$\text{First}(T\omega) \triangleq T \quad \text{when } T \in T \triangleq \{a, b\}$$

Let $\mathbb{T}^*$ be the set of all sentences made out of elements of the alphabet $\mathbb{T}$ and including the empty sentence $\epsilon$. Prove that $\text{First}$ establishes a Galois retraction between terminal languages in $\wp(\mathbb{T}^*)$ and $\wp(\mathbb{T} \cup \{\epsilon\})$. Provide a fixpoint characterization of $\text{First}(\text{lfp}^\subseteq F)$. Calculate this fixpoint to determine the first terminals starting sentences in the languages deriving from $x$ and $y$ (plus $\epsilon$ if these languages contain the empty sentence). 

**Exercise 11.4-3** Continuing example 171, provide a fixpoint characterization of $\text{post}[R^*](\mathcal{I})$ and $\text{pre}[R^*](\mathcal{I})$ for the reflexive transitive closure $R^*$ of a relation $R \in \wp(\mathcal{U} \times \mathcal{U})$. 

A slight generalization of theorem 167 follows (the abstraction need to apply to the concrete [post]fixpoints only).

**Exercise 11.4-4** Prove the following theorem 175.

---

**Theorem 175 (Exact fixpoint abstraction).** Let $F \in \wp(C) \mapsto \wp(C)$ be a $\subseteq$-increasing map, $\mathcal{P}_F \triangleq \{X \in \wp(C) \mid F(X) \subseteq X\}$ and $\langle \mathcal{P}_F, \subseteq \rangle \xrightarrow{\gamma} \langle \wp(A), \subseteq \rangle$ be an abstraction on $\mathcal{P}_F$.

If $\overline{F} \in \wp(A) \mapsto \wp(A)$ is increasing and satisfies the commutation property $\alpha \circ F = F \circ \alpha$ then $\alpha(\text{lfp}^\subseteq F) = \text{lfp}^\subseteq \overline{F}$. Moreover, if $\alpha$ surjective then $\overline{F} = \alpha \circ F \circ \gamma$. 

---

152