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 6

Set Transformers

When reasoning on program executions, Computer Scientists propagate properties from one program point to another (e.g. if the array is not empty on procedure call then it is sorted on return from the call). Since properties are sets (all arrays but the empty one on entry and all sorted arrays on exit), this information propagation can be modeled by set transformers (mapping the set of non-empty arrays into the set sorted ones)\(^1\).

These concepts are usually introduced axiomatically in Computer Science (Dijkstra, 1976; Dijkstra and Scholten, 1990) but the axioms are better understood as immediate consequences of simple well-known mathematical concepts and results (Whitehead and Russell, 1910; Tarski, 1928; Birkhoff, 1935; Bourbaki, 1939; Ward and Dilworth, 1939; Birkhoff, 1940; Everett, 1944; Ore, 1944; Riguet, 1948; Schmidt, 1953) that we have grouped in this chapter 6 and in chapter 8 for the relations between these set transformers.

**Example 58.** As an introductory example of set transformer, consider the following total function \( f \in \mathcal{X} \rightarrow \mathcal{X} \) where \( \mathcal{X} \triangleq \{-1, 0, 1\} \) and the corresponding right image transformer \( f^* (X) \triangleq \{ f(x) \mid x \in X \} \) mapping sets in \( \varphi(\mathcal{X}) \) to subsets of the range \( \{-1, 0\} \) of \( f \).

\[
\begin{align*}
\mathcal{X} & = \{-1, 0, 1\} \\
{\mathcal{X}}' & = \{-1, 0\}
\end{align*}
\]

We can imagine that \( f \) describes the effect of the following function (partial on integers).

\(^1\) A more precise specification of sorting would require the sorted array on exit to be a permutation of the unsorted one on entry.
# let f x = match x with
| 1 | 0 -> 0
| -1 | -> -1;

Then the transformer \( f^\star \) transforms a property of the parameter (e.g. \( \{0, 1\} \) meaning that the parameter is positive) into a property of the result returned by the function call \( (f^\star(\{0, 1\}) = \{0\} \) meaning that the result is zero for all positive parameters for which the function is well-defined).

## 6.1 Functional Images

**Definition 59 (Functional images).** A partial map \( f \in \mathcal{X} \vdash \mathcal{Y} \) from set \( \mathcal{X} \) into set \( \mathcal{Y} \) can be extended to set transformers between \( \phi(\mathcal{X}) \) and \( \phi(\mathcal{Y}) \) as follows.

(a) The right image or direct image or postimage or simply image \( f^\star \in \phi(\mathcal{X}) \twoheadrightarrow \phi(\mathcal{Y}) \) is \( f^\star(X) \triangleq \{ f(x) \mid x \in X \cap \text{dom}(f) \} \).

(b) The left image or inverse image or preimage is \( f^\sharp \in \phi(\mathcal{Y}) \xrightarrow{\text{f}^{-}} \phi(\mathcal{X}) \) such that \( f^\sharp(Y) \triangleq \{ x \in \text{dom}(f) \mid f(x) \in Y \} \).

(c) The dual right image \( f^\triangledown \in \phi(\mathcal{X}) \twoheadrightarrow \phi(\mathcal{Y}) \) is \( f^\triangledown \triangleq \neg \circ f^\star \circ \neg \) where \( \neg \) is the set complement.

(d) The dual left image \( f^\blacktriangle \in \phi(\mathcal{Y}) \xrightarrow{\text{f}^{-}} \phi(\mathcal{X}) \) is \( f^\blacktriangle \triangleq \neg \circ f^\blacktriangle \circ \neg \).

---

\(^2\) Various notations are used in Mathematics for the right image \( f^\star(X) \) of a set \( X \) by a function \( f \) such as \( f^\star(X), f_+(X), f^+(X), f_{-+}(X), f_{-}(X), f^-(X), f^\circ X, f[X], f(X), \) etc.

\(^3\) Various notations are used in Mathematics for the left image \( f^\bullet(Y) \) of a set \( Y \) by a function \( f \) such as \( f^{-1}[Y], f_{-1}(Y), f_-(X), f^-(X), f_{-+}(X), f_{-}(X), f^+(X), f^+(X), f^\circ X, f[X], f(X), \) etc. Sometimes \( f^{-1} \) is defined alternatively as \( f^{-1} \in \mathcal{Y} \mapsto \phi(X) \) by \( f^{-1}(y) \triangleq \{ x \in \text{dom}(f) \mid f(x) = y \} \), in which case \( f^\bullet(X) = \bigcup \{ f^{-1}(y) \mid y \in Y \} \).
These definitions are also valid for total maps but then $f^{	riangleright} = f^\star$ and $f^\lefttriangleleft = f^\blacksquare$.

**Lemma 60.** Let $f \in \mathcal{X} \rightarrow \mathcal{Y}$ with $\text{dom}(f) = \mathcal{X}$. Then $f^\lefttriangleleft = f^\star$ and $f^\triangleright = f^\blacksquare$.

**Proof.** Let $f \in \mathcal{X} \rightarrow \mathcal{Y}$ with $\text{dom}(f) = \mathcal{X}$, $X \in \wp(\mathcal{X})$, and $Y \in \wp(\mathcal{Y})$.

\[
\begin{align*}
\text{--- } & \quad f^\triangleright(X) \\
= & \quad \lnot(f^\triangleright(\lnot(X))) \\
= & \quad \lnot(\{f(x) \mid x \in (\lnot(X)) \cap \text{dom}(f)\}) \\
= & \quad \lnot(\{f(x) \mid x \in \lnot(X)\}) \\
= & \quad \{f(x) \mid x \in X\} \\
= & \quad \{f(x) \mid x \in X \cap \text{dom}(f)\} \quad \{\text{by } X \subseteq \mathcal{X} \text{ and totality of } f \text{ so } \text{dom}(f) = \mathcal{X}\} \\
= & \quad f^\triangleright(X) \quad \{\text{def. } f^\triangleright \text{ in definition 59(a)}\}
\end{align*}
\]

\[
\begin{align*}
\text{--- } & \quad f^\blacksquare(X) \\
= & \quad \lnot(f^\blacksquare(\lnot(Y))) \\
= & \quad \lnot(\{x \in \text{dom}(f) \mid f(x) \in \lnot(Y)\}) \\
= & \quad \lnot(\{x \in \mathcal{X} \mid f(x) \in \lnot(Y)\}) \\
= & \quad \{x \in \mathcal{X} \mid f(x) \in Y\} \quad \{\text{by totality of } f \text{ so } \text{dom}(f) = \mathcal{X}\} \\
= & \quad f^\blacksquare(Y) \quad \{\text{def. } f^\blacksquare \text{ in definition 59(b) and } \text{dom}(f) = \mathcal{X}\}
\end{align*}
\]

### 6.2 Relational Images

The idea of functional images can be extended to relations.
**Definition 61 (Relational images).** If \( R \in \wp(X \times Y) \) is a binary relational between sets \( X \) and \( Y \), then image transformers between powersets \( \wp(X) \) and \( \wp(Y) \) are defined as follows:

(a) \( R^\bullet \in X \mapsto \wp(Y) \) is the elementwise right image \( R^\bullet(x) \triangleq \{ y \in Y \mid R(x, y) \} \) of element \( x \) by relation \( R \).

(b) \( R^\bullet \in Y \mapsto \wp(X) \) is the elementwise left image \( R^\bullet(y) \triangleq \{ x \in X \mid R(x, y) \} \) of element \( y \) by relation \( R \) (so that \( R^\bullet = (R^{-1})^\bullet \)).

(c) \( \text{post}[R] \in \wp(X) \mapsto \wp(Y) \) is the right image \( \text{post}[R]X \triangleq \{ y \in Y \mid \exists x \in X : R(x, y) \} = \bigcup_{x \in X} \text{post}[R](\{ x \}) = \bigcup_{x \in X} R^\bullet(x) = \{ y \in Y \mid X \cap R^\bullet(y) \neq \emptyset \} \) of a subset \( X \) of \( X \) by relation \( R \).

(d) \( \text{pre}[R] \in \wp(Y) \mapsto \wp(X) \) is the left image \( \text{pre}[R] \triangleq \text{post}[R^{-1}] \) of a subset \( Y \) of \( Y \) by relation \( R \) so that \( \text{pre}[R]Y = \{ x \in X \mid \exists y \in Y : R(x, y) \} = \bigcup_{x \in X} \text{pre}[R](\{ y \}) = \bigcup_{x \in X} R^\bullet(x) = \{ x \in X \mid Y \cap R^\bullet(x) \neq \emptyset \} \).

(e) \( \text{post}[R] \in \wp(X) \mapsto \wp(Y) \) is the dual right image \( \text{post}[R]X \triangleq \neg \text{post}[R](-X) = \{ y \in Y \mid \forall x : R(x, y) \Rightarrow x \in X \} \).

(f) \( \text{pre}[R] \in \wp(Y) \mapsto \wp(X) \) is the dual left image \( \text{pre}[R]Y \triangleq \neg \text{pre}[R](-Y) = \{ x \in X \mid \forall y : R(x, y) \Rightarrow y \in Y \} \).

---

*Again many different notations are used in mathematics for example \( R^\bullet(x) \) is \( R(x) \) in (Riguet, 1948), \( \text{post}[R]X \) is \( R''X \) in (Whitehead and Russell, 1910), \( \mathcal{R}(X) \) in (Tarski, 1928), \( R(X) \) in (Riguet, 1948; Schmidt, 1953) where \( \text{pre}[R]X = \mathcal{R}(X) \) in (Whitehead and Russell, 1910), \( R^{-1}(X) \), \( \text{post}[R]X/\text{pre}[R]X \) is \( R[X]/R^{-1}[X] \) in (Riguet, 1948; Schmidt, 1953), \( \text{post}[R]X/\text{pre}[R]X \) is \( R(X)/R^{-1}(X) \) in (Schmidt, 1953), etc. Our notations follow (Cousot, 1981).*
CHAPTER 6. SET TRANSFORMERS

\[ \begin{array}{c}
\text{\textbf{dual (right) image}} \quad \text{\underline{\text{post}}}[R]X \\
\text{\textbf{dual inverse/left image}} \quad \text{\underline{\text{pre}}}[R]Y
\end{array} \]

**Proof.**

- \[ \underline{\text{post}}[R](X) \triangleq \neg \text{post}[R](\neg X) \]
  \[ = \neg \{ y \in \mathcal{Y} \mid \exists x \in (\neg X) : R(x, y) \} \] \hspace{1cm} \{ \text{def. post in definition 61.(c)} \}
  \[ = \{ y \in \mathcal{Y} \mid \forall x : x \not\in (\neg X) \lor \neg R(x, y) \} \] \hspace{1cm} \{ \text{def. } \lor \}
  \[ = \{ y \in \mathcal{Y} \mid \forall x : R(x, y) \Rightarrow x \in X \} \] \hspace{1cm} \{ \text{def. } \Rightarrow \}

- \[ \underline{\text{pre}}[R]X \triangleq \neg \text{pre}[R](\neg X) \]
  \[ = \neg \{ x \in \mathcal{X} \mid \exists y : y \in (\neg X) \land R(x, y) \} \] \hspace{1cm} \{ \text{def. pre in definition 61.(d)} \}
  \[ = \{ x \in \mathcal{X} \mid \forall y : y \not\in (\neg X) \land \neg R(x, y) \} \] \hspace{1cm} \{ \text{def. } \land \}
  \[ = \{ x \in \mathcal{X} \mid \forall y : R(x, y) \Rightarrow y \in X \} \] \hspace{1cm} \{ \text{def. } \Rightarrow \} \quad \blacksquare

These relational set transformers are generalization of the functional case, in that:

- \[ \underline{f^\bullet} = \text{post}[\{(x, f(x)) \mid x \in \text{dom}(f)\}] \]
- \[ \underline{f^\bullet} = \text{pre}[\{(x, f(x)) \mid x \in \text{dom}(f)\}] \]
- \[ \underline{\text{post}}[\{(x, f(x)) \mid x \in \text{dom}(f)\}] \]
- \[ \underline{\text{pre}}[\{(x, f(x)) \mid x \in \text{dom}(f)\}] \]

**Proof.**

- \[ \text{\underline{post}}[\{(x, f(x)) \mid x \in \text{dom}(f)\}] \]
  \[ = \{ y \mid \exists x \in X : \{x, f(x)\} \in \{(x, f(x)) \mid x \in \text{dom}(f)\} \} \] \hspace{1cm} \{ \text{def. post} \}
  \[ = \{ f(x) \mid x \in X \cap \text{dom}(f) \} \] \hspace{1cm} \{ \text{def. } \cap \}
  \[ = f^\bullet(X) \] \hspace{1cm} \{ \text{def. } f^\bullet \}
Example 63 (Polarities).

Let

\[ \text{def. } \overline{\text{pre}} \]

\[
\overline{\text{pre}}[(x, f(x)) \mid x \in \text{dom}(f)] Y
= \{x \mid \forall y : (x, y) \in \{(x, f(x)) \mid x \in \text{dom}(f) \} \Rightarrow y \in Y\} \\
= \{x \mid x \in \text{dom}(f) \Rightarrow f(x) \in Y\} \\
= \neg\{x \mid x \in \text{dom}(f) \land f(x) \in \neg Y\} \\
= \neg(f^\bullet(\neg Y)) \\
= f^\bullet(Y) \]

\[ \text{def. } \circ \text{ and } f^\bullet \]

Let us also define Garrett Birkhoff’s polarities (Birkhoff, 1940; Ore, 1944).

Definition 62 (Polarities). (a) The set transformer \( \overline{\text{post}}[R] \in \wp(\mathcal{X}) \leftrightarrow \wp(\mathcal{Y}) \) is the right polarity \( \overline{\text{post}}[R] X \triangleq \neg \overline{\text{post}}[\neg R](X) = \{y \in \mathcal{Y} \mid \forall x \in X : R(x, y)\} = \bigcap_{x \in X} R^\bullet(x) = \{y \in \mathcal{Y} \mid \forall x \in X : \neg R(x, y)\} \)

(b) \( \overline{\text{pre}}[R] \in \wp(\mathcal{Y}) \leftrightarrow \wp(\mathcal{X}) \) is the left polarity \( \overline{\text{pre}}[R] Y \triangleq \neg \overline{\text{pre}}[\neg R](Y) = \{x \in \mathcal{X} \mid \forall y \in Y : R(x, y)\} = \bigcap_{y \in \mathcal{Y}} R^\bullet(y) \).

Proof.

\begin{align*}
\overline{\text{post}}[R] & \triangleq \neg \overline{\text{post}}[\neg R](X) \\
= & \neg\{y \in \mathcal{Y} \mid \exists x \in X : \neg R(x, y)\} \quad \text{\{def. } \overline{\text{post}}\} \\
= & \neg\{y \in \mathcal{Y} \mid \exists x \in X : x \in X \land \neg R(x, y)\} \quad \text{\{def. } \exists\} \\
= & \{y \in \mathcal{Y} \mid \forall x : x \not\in X \lor R(x, y)\} \quad \text{\{def. } \neg\} \\
= & \{y \in \mathcal{Y} \mid \forall x : x \in X \Rightarrow R(x, y)\} \quad \text{\{def. } \Rightarrow\} \\
= & \{y \in \mathcal{Y} \mid \forall x : x \in X \land f(x, y)\} \quad \text{\{def. } \circ \text{ and } f^\bullet\} \\
\end{align*}

Example 63 (Polarities). Let \( \mathcal{S} \) be a set, \( \mathcal{X} = \mathcal{Y} = \wp(\mathcal{S}) \), and \( R = \subseteq \). Then \( \overline{\text{post}}[\subseteq] \in \wp(\wp(\wp(\mathcal{S}))) \leftrightarrow \wp(\wp(\wp(\mathcal{S}))) \) is \( \overline{\text{post}}[\subseteq](\mathcal{X}) = \{Y \in \wp(\wp(\mathcal{S})) \mid \forall X \in \mathcal{X} : X \subseteq Y\} \), that is the set of upper bounds of \( \mathcal{X} \) (larger than or equal to any element of \( \mathcal{X} \)). \( \overline{\text{pre}}[\subseteq] \in \wp(\wp(\wp(\mathcal{S}))) \leftrightarrow \wp(\wp(\wp(\mathcal{S}))) \) is \( \overline{\text{pre}}[\subseteq](\mathcal{Y}) = \{X \in \wp(\wp(\mathcal{S})) \mid \forall Y \in \mathcal{Y} : X \subseteq Y\} \), that is the set of lower bounds of \( \mathcal{Y} \) (smaller than or equal to any element of \( \mathcal{Y} \)).
6.3 Bibliography

Images of sets by relations have been well studied in mathematics (Whitehead and Russell, 1910; Tarski, 1928; Birkhoff, 1935; Bourbaki, 1939; Ward and Dilworth, 1939; Birkhoff, 1940; Everett, 1944; Ore, 1944; Riguet, 1948; Schmidt, 1953).

Backward predicate transformers were introduced in computer science by (Dijkstra, 1975). For forward predicate transformers and their relevance to program verification, see (Cousot and Cousot, 1977a; Cousot, 1981) and chapter 2.

6.4 Exercises

Exercise 6.4-1 Show that an injection \( f : X \rightarrow Y \) has at least one left inverse \( (g \text{ such that } g \circ f = 1_X) \) when \( X \neq \emptyset \), and reciprocally. □

Exercise 6.4-2 Prove that if \( f : X \rightarrow Y \) is total then for all \( X, Y \in \wp(X) \), \( f^*(\neg Y) = \neg f^*(Y) \) and if \( X \cap Y = \emptyset \) then \( f^*(X) \cap f^*(Y) = \emptyset \). Prove that in general, these two properties of the left image \( f^* \) do not hold for the right image \( f^* \). See complements in exercises 9.11.1 and 9.11.2. □

Exercise 6.4-3 Continuing example 1.4, consider the relational semantics of the random assignment \( x := \_ \) defined as \( S^\rho[x := \_] \triangleq \{ \rho, \rho[x := n] \} \mid \rho \in \wp(\mathbb{V} \mapsto \mathbb{Z} \land n \in \mathbb{N}) \).

Calculate the forward predicate transformer in \( \wp(\mathbb{V} \mapsto \mathbb{Z}) \mapsto \wp(\mathbb{V} \mapsto \mathbb{Z}) \) defined by \( \text{post}[x := \_] \triangleq \text{post}[S^\rho[x := \_]] \). □
Exercise 6.4-4  Continuing exercise 6.4-4, calculate the backward predicate transformers in \( \varphi(\mathbb{V} \mapsto \mathbb{Z}) \mapsto \varphi(\mathbb{V} \mapsto \mathbb{Z}) \) defined by \( \text{pre}[x := ?] \triangleq \text{pre}[\varphi[x := ?]] \) and \( \text{pre}[x := ?] \triangleq \text{pre}[\varphi[x := ?]]. \)

Why does (Dijkstra, 1975) define \( \text{wp}[x := ?] \triangleq \text{pre}[x := ?] \cap \text{pre}[x := ?]? \)

Exercise 6.4-5  Given \( R_1 \in \varphi(\mathcal{X} \times \mathcal{Y}) \) and \( R_2 \in \varphi(\mathcal{Y} \times \mathcal{Z}) \), calculate \( \text{post}[R_1 \circ R_2] \), \( \text{pre}[R_1 \circ R_2] \), \( \text{post}[R_1 \circ R_2] \), and \( \text{pre}[R_1 \circ R_2]. \)

Exercise 6.4-6  Consider the program \( P \)

\[
\begin{align*}
^1 x & := 0; \\
^2 \text{while} & (x < n) \text{ do} \\
^3 x & := x + 1 \\
\text{od}.
\end{align*}
\]

Given \( n \in \mathbb{Z} \), define the following relation \( R(n) \) on \( \mathbb{L} \times \mathbb{Z} \) where \( \mathbb{L} \triangleq \{1, 2, 3, 4\}. \)

\[
R(n) \triangleq \{(1, x), (2, 0) | x \in \mathbb{Z}\} \cup \{(2, x), (3, x) | x \in \mathbb{Z} \land x < n\} \cup \{(2, x), (4, x) | x \in \mathbb{Z} \land x \geq n\} \cup \{(3, x), (2, x + 1) | x \in \mathbb{Z}\}
\]

Provide an intuitive interpretation of formula \( R(n) \). Calculate \( \text{post}[R(n)]. \)
Chapter 7

Set Fixpoints

Fixpoints, that is solutions to equations \( x = f(x) \), are everywhere in Computer Science, in particular because all computations and data structures are iterative or recursive, hence defined in terms of themselves. Although, we could make exactly the same presentation of fixpoints using order theory, we have chosen, in the hope of limiting the required background to stick to set theory, and to consider set fixpoints (i.e. \( x \) is a set and \( f \) maps sets to sets)\(^1\). The knowledgeable of order-theoretic fixpoint theory (\( \text{Ok, 2010} \)) will find the results classical so that they can be skipped or referred to later, when needed.

7.1 Fixpoints

An element \( x \in S \) of a set \( S \) is a fixpoint of a function/operator/transformer \( f \in S \mapsto S \) on \( S \) if and only if \( f(x) = x \). It is therefore a solution to the equation \( x = f(x) \) where \( f \) is given and \( x \) is the unknown.

An operator \( f \in S \mapsto S \) on a set \( S \) may have no fixpoint (like \( f(x) \triangleq x + 1 \) on \( \mathbb{N} \)), one or more fixpoints (like \( f(x) \triangleq 0 \) on \( \mathbb{N} \)) or infinitely many fixpoints (like \( f(x) \triangleq x \) on \( \mathbb{N} \) or \( \mathbb{Z} \)).

In case of existence of several fixpoints, there might be a least one for some order (like 0 for \( f(x) \triangleq x \) with order \( \leq \) on \( \mathbb{N} \)) or a greatest one (like 0 for \( f(x) \triangleq x \) with order \( \geq \) on \( \mathbb{N} \)), or there might be neither least nor greatest fixpoint (like for \( f(x) \triangleq x \) with \( \leq \) on \( \mathbb{Z} \)).

In this chapter 7, we study fixpoints of functions of sets.

One of the main uses of fixpoints in Computer Science is to define a subset \( S \) of a universe \( \mathcal{U} \) as a solution of an equation \( X = F(X) \) or an inequation \( F(X) \subseteq X \) where \( F \in S \mapsto S \) (which can be written in the form \( \forall x \in \mathcal{U} : x \in F(X) \Rightarrow x \in X \), in which case

\(^1\)Moreover the generalization is very easy, just replace a power set \( \langle \wp(S), \subseteq, \emptyset, \cup, \cap, \neg \rangle \) by a complete lattice \( \langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap \rangle \) (or complete Boolean lattice \( \langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap, \neg \rangle \) and all results and proofs are generalized by a mere syntactic match of the orders, infimum, supremum, lub, glb, (and complement when needed).
Computer Scientists speak of “Constraint Solving” or “Constraint Satisfaction Problem” e.g. (Aiken, 1999; Apt, 1997; Fähndrich and Aiken, 1997).

Of course for the set $S$ to be well-defined (meaning it exists and is unique) the equation $X = F(X)$ (or inequation $F(X) \subseteq X$) must have a solution, that is $F$ must have at least one fixpoint (or postfixpoint). But there may be many fixpoints (or postfixpoints) whereas the desired solution should be unique (to avoid ambiguities). In that case we need additional requirements on the desired solution, for example that it is the $\subseteq$-smallest or $\subseteq$-largest, if any.

The theorems in this chapter 7 are useful to ensure that such a solution satisfying the desired requirements does exist and, preferably, is unique.

Moreover, this chapter 7 provides iterative definitions of fixpoints which yields effective algorithms to compute fixpoints in the finite case similar to Newton (Newton, 1669; Newton, 1671 (published 1736)), Gauss (Gauss, 1823), and Liouville (Liouville, 1837) method of successive approximations for finding the root of an equation $x = f(x)$ in numerical analysis. Starting with a first point $x_0$ in the basin of attraction of $x$, and letting $x_{n+1} = f(x_n)$ for $n \geq 0$, the sequence $(x_n, n \in \mathbb{N})$ will converge to the desired solution $x$ (under condition to be provided by the convergence theorem).

![Graph of a function and its fixpoints]

### 7.2 Fixpoints of Set Transformers

When considering fixpoints of set operators, an early result is the following Bronislaw Knaster’s theorem (Knaster and (in common with A. Tarski), 1928) (the paper mentioning that the result was obtained in common with Alfred Tarski):

**Theorem 64 (Kaster-Tarski fixpoint theorem).** If $F$ is a function of sets which is in-
creasing and \( A \) is a set which is a postfixpoint of \( F \) (i.e. such that \( F(A) \subseteq A \)) then there exists a subset \( D \) of \( A \) such that \( D = F(D) \).

Theorem 64 says nothing about the possible existence of many different solutions. Fortunately, Tarski generalized to previous theorem 64 to show the existence of extremal solutions (Tarski, 1955). When applied to power sets, Tarski’s (1955) fixpoint theorem states (i.a., see theorem 77 for complements) that

**Theorem 65 (Tarski’s set-theoretic fixpoint theorem).** Let \( F \in \wp(S) \xrightarrow{\subseteq} \wp(S) \) be \( \subseteq \)-increasing. Then the equation \( X = F(X) \) has a \( \subseteq \)-least solution on \( \wp(S) \) (called the least fixpoint of \( F \)) for \( \subseteq \) and denoted \( \text{lfp}^\subseteq F \) such that \( \text{lfp}^\subseteq F = \bigcap\{X \in \wp(S) \mid F(X) \subseteq X\} \) and a \( \subseteq \)-greatest solution on \( \wp(S) \) (called the greatest fixpoint of \( F \)) for \( \subseteq \) and denoted \( \text{gfp}^\subseteq F \) such that \( \text{gfp}^\subseteq F = \bigcup\{X \in \wp(S) \mid X \subseteq F(X)\} \).

---

**Corollary 66.** If \( F \in \wp(S) \xrightarrow{\subseteq} \wp(S) \) is \( \subseteq \)-increasing then \( \text{lfp}^\subseteq F = \bigcap\{X \in \wp(S) \mid F(X) = X\} \).

---

**Proof.** By reflexivity, \( F(X) = X \) implies \( F(X) \subseteq X \) so \( \bigcap\{X \in \wp(S) \mid F(X) = X\} \subseteq \bigcap\{X \in \wp(S) \mid F(X) \subseteq X\} \) which implies, by definition of \( \bigcap \) and theorem 65 that \( \text{lfp}^\subseteq F = \bigcap\{X \in \wp(S) \mid F(X) \subseteq X\} \subseteq \bigcap\{X \in \wp(S) \mid F(X) = X\} \). But \( F(\text{lfp}^\subseteq F) = \text{lfp}^\subseteq F \) so \( \text{lfp}^\subseteq F \) is a fixpoint of \( F \) greater than or equal to \( \text{lfp}^\subseteq F \), written \( \text{lfp}^\subseteq F \), if any (so \( A \subseteq \text{lfp}^\subseteq F = F(\text{lfp}^\subseteq F) \) and for all \( X \in \wp(S) \), \( A \subseteq X = F(X) \) implies \( \text{lfp}^\subseteq F \subseteq X \)).
Corollary 67. Let $F \in \wp(S) \rightarrow \wp(S)$ be $\subseteq$-increasing and $A \in \wp(S)$ such that $A \subseteq F(A)$. Then $\lfp\{ F \}_{A} = \bigcap\{ X \in \wp(S) \mid A \subseteq X \land F(X) \subseteq X \}$.

Notice that theorem 65 corresponds to $A = \emptyset$ in corollary 67.

Proof. Let $S' \triangleq \{ X \cup A \mid X \in S \}$. Observe that $F \in \wp(S') \rightarrow \wp(S')$ since for $Y \in S'$ there is $X \in S$ such that $Y = X \cup A$ so $F(Y) = F(X \cup A) \supseteq F(X) \cup F(A) \supseteq F(X) \cup A$ since $F$ is increasing and $F(A) \supseteq A$. So $F(Y) = F(X) \cup A \in S'$. $F$ is increasing on $S'$ since $S' \subseteq S$ and $F$ is increasing on $S$. By theorem 65, $\lfp \subseteq F$ on $S'$ which is $\lfp \subseteq F$ on $S$ is $\bigcap\{ X \in \wp(S') \mid F(X) \subseteq X \} = \bigcap\{ X \in \wp(S) \mid A \subseteq S \land F(X) \subseteq X \}$. \hfill \qed

7.3 Fixpoint Complement

An immediate consequence of theorem 65 is DAVID PARK’s fixpoint complement theorem (Park, 1969).

Theorem 68 (Park’s set-theoretic fixpoint complement theorem). Let the set transformer $F \in \wp(S) \rightarrow \wp(S)$ be $\subseteq$-increasing. For $X \in \wp(S)$, define $\neg X \triangleq S \setminus X$. Then $\neg \lfp \subseteq F = \gfp \subseteq \neg F \circ \neg$ and $\neg \gfp \subseteq F = \lfp \subseteq \neg F \circ \neg$.

Moreover, $\lfp \subseteq F \cap \lfp \subseteq \neg F \circ \neg = \emptyset$ and $\lfp \subseteq F \cup \lfp \subseteq \neg F \circ \neg = S$ if and only if $F$ has a unique fixpoint.

Proof.

\[ \neg \lfp \subseteq F \]
\[ = \neg \bigcap\{ X \in \wp(S) \mid F(X) \subseteq X \} \quad \{ \text{by theorem 65} \} \]
\[ = \bigcup\{ \neg X \in \wp(S) \mid F(X) \subseteq X \} \quad \{ \text{by De Morgan’s law} \} \]
\[ = \bigcup\{ \neg X \in \wp(S) \mid \neg X \subseteq F(\neg X) \} \quad \{ \text{def. } \neg \text{ and } \subseteq \} \]
\[ = \bigcup\{ Y \in \wp(S) \mid Y \subseteq F(\neg Y) \} \quad \{ \text{letting } Y = \neg X \} \]
\[ = \gfp \subseteq \neg F \circ \neg \quad \{ \text{theorem 65 and def. function composition } \circ \} \]

By order-reversing duality, $\neg \gfp \subseteq F = \lfp \subseteq \neg F \circ \neg$.

\[ \lfp \subseteq F \cap \lfp \subseteq \neg F \circ \neg \]
\[ = \lfp \subseteq F \cap \neg \gfp \subseteq F \quad \{ \text{since } \lfp \subseteq F \subseteq \gfp \subseteq F \} \]
\[ \subseteq \emptyset \quad \{ \text{def. } \neg \} \]
— If $F$ has a unique fixpoint then

$$\text{lfp}^c F \cup \text{lfp}^c \rightarrow \circ F \circ \rightarrow$$

$$= \text{lfp}^c F \cup -\text{gfp}^c F$$

$$= \text{lfp}^c F \cup -\text{lfp}^c F$$ \{unique fixpoint hypothesis\}

$$= S$$ \{def. $\rightarrow$ on $\wp(\mathcal{S})$\}

— Reciprocally, we have to prove fixpoint unicity, or equivalently, by theorem 65, that $\text{gfp}^c F = \text{lfp}^c F$.

$$\text{lfp}^c F \cup \text{lfp}^c \rightarrow \circ F \circ \rightarrow S$$

$$\Rightarrow \text{lfp}^c F \cup -\text{gfp}^c F = S$$

$$\Rightarrow -\text{gfp}^c F \cup \text{lfp}^c F = S$$ \{commutativity\}

$$\Rightarrow \text{gfp}^c F \subseteq \text{lfp}^c F$$ \{by exercise 2.26-10 proving $X \subseteq Y \iff \neg \{X \cup Y = S\}$\}

$$\Rightarrow \text{gfp}^c F = \text{lfp}^c F$$ \{since $\text{lfp}^c F \subseteq \text{gfp}^c F$ by definition and antisymmetry\} ■

### 7.4 Fixpoint Iteration

In (Tarski, 1955), Tarski also showed that least fixpoints of $\cup$-preserving functions can be calculated iteratively.

**Definition 69 (Continuity).** A function $F \in \wp(\mathcal{S}) \mapsto \wp(\mathcal{S})$ is continuous if and only if for any non-empty ascending chain $X_0 \subseteq X_1 \subseteq \ldots \subseteq X_n \subseteq \ldots$, we have $F(\bigcup_{n \in \mathbb{N}} X_n) = \bigcup_{n \in \mathbb{N}} F(X_n)$. The dual notion is cocontinuous. We write $\wp(\mathcal{A}) \downarrow \mapsto \wp(\mathcal{B})$ (respectively $\wp(\mathcal{A}) \downarrow \mapsto \wp(\mathcal{B})$) for the set of continuous (resp. cocontinuous) maps of $\wp(\mathcal{A})$ into $\wp(\mathcal{B})$.

**Lemma 70.** A continuous or cocontinuous function is increasing.

**Proof.** If $F \in \wp(\mathcal{S}) \mapsto \wp(\mathcal{S})$ is continuous and $X \subseteq Y$ then $Y = X \cup Y$ so $F(X) = F(X) \cup F(Y)$ hence $F(X) \subseteq F(Y)$. By order-reversing duality this holds for co-continuous functions since increasing is self-dual. ■

**Theorem 71 (Tarski’s set-theoretic iterative fixpoint theorem).** Let the function $F \in \wp(\mathcal{S}) \mapsto \wp(\mathcal{S})$ be continuous. Then $\text{lfp}^c F = \bigcup_{n \in \mathbb{N}} F_n$, where the iterates $(F_n, n \in \mathbb{N})$ of $F$ are $F_0 \triangleq \emptyset$ and $F_{n+1} \triangleq F(F_n)$. 79
Notice, by a simple recurrence that $\forall n \in \mathbb{N} : F_n = F^n(\emptyset)$ where $F^n$ is the $n$-th power of $F$ defined in section 2.20.

**Proof.** $F_0 = \emptyset \subseteq F_1$ by def. $\emptyset$. If $F_0 \subseteq F_{n+1}$ then $F_{n+1} = F(F_n) \subseteq F(F_{n+1}) = F_{n+2}$ since $F$ is increasing by lemma 70. By recurrence, $\langle F_n, n \in \mathbb{N} \rangle$ is an ascending chain.

It follows by continuity that $F(\bigcup_{n \in \mathbb{N}} F_n) = \bigcup_{n \in \mathbb{N}} F(F_n) = \bigcup_{n \in \mathbb{N}} F_{n+1} = \bigcup_{m>0} F^m(\emptyset) = \bigcup_{m \in \mathbb{N}} F^m(\emptyset)$ since $F_0 = \emptyset$. Therefore $\bigcup_{n \in \mathbb{N}} F_n$ is a fixpoint of $F$.

For another fixpoint $X = F(\emptyset)$ we have $F_0 = \emptyset \subseteq X$ so if $F_0 \subseteq X$ then $F_{n+1} = F(F_n) \subseteq F(X) = X$ since $F$ is increasing. By recurrence, $\forall n \in \mathbb{N} : F_n \subseteq X$ and so $\bigcup_{n \in \mathbb{N}} F_n \subseteq X$, proving that $\bigcup_{n \in \mathbb{N}} F_n = \text{Ifp}_0^\infty F$ is the least fixpoint of $F$.  

**Example 72.** (Fixpoint definition of the reflexive transitive closure) Let $R \in \wp(\mathbb{U} \times \mathbb{U})$ be a binary relation on a set $\mathbb{U}$. In section 2.12, we have defined the reflexive transitive closure of $R$ as $R^* \triangleq \bigcup_{n \in \mathbb{N}} R^n$ where $R^n$ is the $n$-th power of $R$.

Another definition could have been $R^* = \text{Ifp}_0^\infty \lambda X \cdot 1_u \cup R_1^* X$. The function $F \triangleq \lambda X \cdot 1_u \cup R_1^*$ is $\wp(\mathbb{U} \times \mathbb{U})$ is increasing so that by theorem 65, it has a least fixpoint. Moreover, the function $F$ is continuous with iterates $F_0 = \emptyset, F_1 = 1_u, F_2 = 1_u \cup R_1^* 1_u = R_0 \cup R_1^*$. If $F_n = \bigcup_{0 \leq k < n} R_k^*$ then $F_{n+1} = 1_u \cup \bigcup_{0 \leq k < n} R_k^* = R_0 \cup \bigcup_{0 \leq k < n} R_k^*$. Passing to the limit, theorem 71 implies that $\text{Ifp}_0^\infty F = \bigcup_{n \in \mathbb{N}} F_n = \bigcup_{n \in \mathbb{N}} \bigcup_{0 \leq k < n} R_k^* = \bigcup_{n \in \mathbb{N}} R^n = R^*$ as defined in section 2.12. Similarly, $R^* = \text{Ifp}_0^\infty \lambda X \cdot 1_u \cup R_1^* X$.  

When $F \in \mathcal{X} \mapsto \mathcal{X}$ where $\mathcal{X} \in \wp(\wp(S))$ and $\mathcal{X} \neq \wp(S)$, theorem 71 may not be applicable for several reasons. For example, there may be no suitable starting point for the iterates because $\emptyset \notin \mathcal{X}$, or the limit of the iterates may not belong to $\mathcal{X}^2$, or $F$ may not be continuous. In that case, theorem 71 can be refined by starting from a prefixed point and assuming continuity along the iterates only.

**Theorem 73 (Strong Tarski’s set-theoretic iterative fixpoint theorem).** Let $\mathcal{X} \in \wp(\wp(S))$, $F : \mathcal{X} \mapsto \mathcal{X}$, and $A \in \mathcal{X}$ such that $A \subseteq F(A)$. Define $\mathcal{Z} \triangleq \{ F^n(A) \mid n \in \mathbb{N} \}$ to be the iterates of $F$ from $A$. Assume that $\bigcup \mathcal{Z} \in \mathcal{X}$ and $F(\bigcup \mathcal{Z}) = \bigcup \{ F(X) \mid X \in \mathcal{Z} \}$. Then $\bigcup \mathcal{Z}$ is a fixpoint of $F$ in $\mathcal{X}$ including $A$.

Moreover, if $F \cap (\mathcal{Z} \times \mathcal{Z} \cup \{ Y \in \mathcal{X} \mid Y = F(Y) \})$ is increasing then $\text{Ifp}_\mathcal{X}^\infty F = \bigcup \mathcal{Z} \in \mathcal{X}$.

**Proof.** $A \in \mathcal{X}$ and $F \in \mathcal{X} \mapsto \mathcal{X}$ so by recurrence all iterates $\{ F^n(A), n \in \mathbb{N} \}$ are in $\mathcal{X}$. By hypothesis, $\bigcup \mathcal{Z} \in \mathcal{X}$, so $F(\bigcup \mathcal{Z}) \in \mathcal{X}$. By definition of $\mathcal{Z}$, $\mathcal{Z} = \{ A \} \cup \{ F(X) \mid X \in \mathcal{X} \}$.

---

2 For example, if $\wp(S)$ is isomorphic to $\mathbb{Z} \cup \{ \infty \}$, $\mathcal{X}$ is isomorphic to $\mathbb{Z}$, and $F(n) = 1 + n$ where $1 + \infty = \infty$ so $F \in \wp(S) \mapsto \wp(S)$ has $\text{Ifp}_\mathcal{X}^\infty F = \infty$ which is the limit of the iterates 0, $F(0) = 1, \ldots, F(n) = 1 + n, \ldots$, $\bigcup \{ F^n(0) \mid n \geq 0 \} = \infty$. However, $F \in \mathcal{X} \mapsto \mathcal{X}$ has no fixpoint since $\emptyset \notin \mathcal{X}$.
CHAPTER 7. SET FIXPOINTS

\( \mathfrak{F} = \{ F(X) \mid X \in \mathfrak{F} \} \) since \( A \subseteq F(A) \). So, by hypothesis \( F(\bigcup\{ F(X) \mid X \in \mathfrak{F} \}) = F(\bigcup \mathfrak{F}) = \bigcup\{ F(X) \mid X \in \mathfrak{F} \} \) proving that \( \bigcup\{ F(X) \mid X \in \mathfrak{F} \} = \bigcup \mathfrak{F} \) is a fixpoint of \( F \) in \( \mathcal{X} \) including \( A \).

Let \( Y \) a fixpoint of \( F \) in \( \mathcal{X} \) including \( A \). We have \( F^0(A) = A \subseteq Y \). If, by induction hypothesis, \( F^n(A) \subseteq Y \) then \( F^{n+1}(A) = F(F^n(A)) \subseteq F(Y) = Y \) since \( F^n(A) \in \mathfrak{F} \) and \( F \cap (\mathfrak{F} \times \mathfrak{F} \cup \{ Y \in \mathcal{X} \mid Y = F(Y) \}) \) is increasing and by fixpoint property \( Y = F(Y) \).

By recurrence, \( F^n(A) \subseteq Y \) so \( \bigcup \mathfrak{F} \subseteq Y \) proving that \( \bigcup \mathfrak{F} \subseteq \mathcal{X} \).

Example 74. (Fixpoint definition of the reflexive transitive closure (continued)) In example 72, we claimed without proof that \( F \) is continuous. Indeed, by theorem 73, this is not necessary, since we just have to check that the limit is preserves for the iterates. Indeed \( F(\bigcup_{n \in \mathbb{N}} F_n) = F(R^*) = 1_u \cup R^+ ; R^+ = R^+ \).

Theorem 73 can even be made stronger by considering posets (see exercise 7.7-8) and even more using even transfinite iterates, as e.g. in (Cousot and Cousot, 1979a).

### 7.5 Metric Fixpoints (Optional)

As an application of theorems 73 and 87, we show that Stefan Banach fixpoint theorem in metric spaces can be proved by endowing the metric space with a partial order and applying Tarski’s iterative fixpoint theorem. For a direct proof of Banach fixpoint theorem, see e.g. (Khamsi and Kirk, 2001)

#### 7.5.1 Banach Metric Fixpoint Theorem

A metric space is a pair \((\mathcal{M}, \delta)\) where \(\mathcal{M}\) is a set (which elements are called “points”) and \(\delta \in (\mathcal{M} \times \mathcal{M}) \to \mathbb{R}\) is a distance, which by definition satisfies for all \(x, y, z \in \mathcal{M}\),

- (a) \(\delta(x, y) = 0 \iff (x = y)\) (zero distance from a point to itself);
- (b) \(\delta(x, y) = \delta(y, x)\) (symmetry);
- (c) \(\delta(x, z) \leq \delta(x, y) + \delta(y, z)\) (triangle inequality).

If follows that \(\delta(x, y) \geq 0\) (since \(2\delta(x, y) = \delta(x, y) + \delta(x, y) = \delta(x, y) + \delta(y, x) \geq \delta(x, x) = 0\) proving \(\delta(x, y) \geq 0\). By exercise 5.19-1, an example is \(\langle \mathbb{R}, \lambda \langle x, y \rangle \cdot |x - y| \rangle\).

A sequence \(x_0, x_1, x_2 \ldots\) of points in \(\mathcal{M}\) converges to a limit \(\ell\) if and only if \(\forall \varepsilon > 0 : \exists N \in \mathbb{N} : \forall n \geq N : \delta(x_n, \ell) < \varepsilon\). The intuition is that points in the sequence get arbitrary close to the limit \(\ell\) denoted \(\lim_{n \to \infty} x_n = \ell\). The limit, if any, is unique (see exercise 7.7-11).

For example any decreasing sequence of reals bounded from below has unique limit which is its greatest lower bound (see exercise 7.7-12).
A sequence \( x_0, x_1, x_2, \ldots \) of points in \( M \) is an *Augustin-Louis Cauchy sequence* if and only if \( \forall \varepsilon > 0 : \exists N \in \mathbb{N} : \forall n, m \geq N : \delta(x_m, x_n) < \varepsilon \). The intuition is that points in the sequence get arbitrarily close to one another.

A metric space \( M \) is called *complete* if every Cauchy sequence of points in \( M \) has a limit \( \ell \in M \).

A map \( f \in M \mapsto M \) is *contracting* if and only if there exists a *Lipschitz constant* \( \kappa \in (0, 1) \) such that

\[
\forall x, y \in M : \delta(f(x), f(y)) \leq \kappa \delta(x, y). \tag{7.1}
\]

Banach’s fixpoint theorem (Banach, 1932) states that a contracting mapping \( f \) on a non-empty complete metric space \( \langle M, \delta \rangle \) has a unique fixpoint (reached by iterations from any point of \( M \)).

Notice that if \( \kappa = 0 \) then the function \( f \) is constant (since \( \delta(f(x), f(y)) = 0 \) so \( \forall x, y \in M : f(x) = f(y) \)) in which case Banach’s fixpoint theorem is trivial. So we can assume when needed that \( \kappa \in (0, 1) \).

A function \( f \) the metric space \( \langle M, \delta \rangle \) to \( \langle M', \delta' \rangle \) is *pointwise continuous* at a point \( \ell \in M \) if and only if \( \forall \varepsilon > 0 : \exists \varepsilon' > 0 : \forall x \in M : \delta(x, \ell) < \varepsilon' \Rightarrow \delta'(f(x), f(\ell)) < \varepsilon \). The intuition is that \( f(x) \) can get arbitrarily closer to \( f(\ell) \) by having \( x \) getting close enough to \( \ell \).

Any contracting function \( f \in M \mapsto M \) on a metric space \( \langle M, \delta \rangle \) is pointwise continuous (see exercise 7.7-14) and so preserves existing limits i.e. \( \lim_{n \to \infty} f(x_n) = f(\lim_{n \to \infty} x_n) \) (see exercise 7.7-15).

### 7.5.2 Banach Fixpoint Theorem in Posets

The objective is to show that Banach’s fixpoint theorem follows from theorem 73 (rephrased on posets e.g. as in exercise 7.7-8).

The first step is to turn the metric space \( \langle M, \delta \rangle \) into a poset \( \langle M, \sqsubseteq \rangle \) by defining for all \( x, y \in M \)

\[
\begin{align*}
\omega(x) & \triangleq \frac{\delta(x, f(x))}{1 - \kappa} & \text{(weight)} \\
x \sqsubseteq y & \triangleq \delta(x, y) \leq \omega(x) - \omega(y) & \text{(partial order.)}
\end{align*}
\]

**Lemma 75.** \( \langle M, \sqsubseteq \rangle \) is a poset.

---

\(^3\)A counter-example is the sequence 3, 3.1, 3.14, 3.141, 3.1415, 3.14159, \ldots of rational approximations of \( \pi \) with more and more decimals, with limit \( \pi \), which is not a rational. So \( \langle \mathbb{Q}, \lambda \langle x, y \rangle \cdot |x - y| \rangle \) is not complete while \( \langle \mathbb{R}, \lambda \langle x, y \rangle \cdot |x - y| \rangle \) is complete.
CHAPTER 7. SET FIXPOINTS

Proof. — (Reflexivity) We have $\delta(x, x) = 0$ so $\delta(x, x) \leq \omega(x) - \omega(x)$ which implies $x \subseteq x$.

— (Antisymmetry) If $x \subseteq y \land y \subseteq x$ then $\delta(x, y) \leq \omega(x) - \omega(y) \land \delta(y, x) \leq \omega(y) - \omega(x)$ with $\delta(x, y) = \delta(y, x)$ so $2\delta(x, y) \leq \omega(x) - \omega(y) + \omega(y) - \omega(x)$ proving $\delta(x, y) \leq 0$ so $\delta(x, y) = 0$ proving $x = y$.

— (Transitivity)

$x \subseteq y \land y \subseteq z$

$\Rightarrow \delta(x, y) \leq \omega(x) - \omega(y) \land \delta(y, z) \leq \omega(y) - \omega(z)$

$\Rightarrow \delta(x, y) + \delta(y, z) \leq \omega(x) - \omega(z)$

$\Rightarrow \delta(x, z) \leq \omega(x) - \omega(z)$

$x \subseteq z$

The second step is to show that the iterates can start from any point $a \in \mathcal{M}$ and the iterates are $\sqsubseteq$-increasing since $f$ is $\sqsubseteq$-extensive.

Lemma 76. $\forall a \in \mathcal{M} : a \sqsubseteq f(a)$.

Proof. $f$ is contracting so $\forall x, y \in \mathcal{M} : \delta(f(x), f(y)) \leq \kappa \delta(x, y)$ which, for $x = a$ and $y = f(a)$, implies that

$\delta(f(a), f(f(a))) \leq \kappa \delta(a, f(a))$

$\Rightarrow \delta(f(a), f(f(a))) \leq \delta(a, f(a)) - (1 - \kappa)\delta(a, f(a))$ \hspace{1cm} \{def. $\sqsubseteq$\}

$\Rightarrow (1 - \kappa)\delta(a, f(a)) \leq \delta(a, f(a)) - \delta(f(a), f(f(a)))$ \hspace{1cm} \{def. $\leq$\}

$\Rightarrow \delta(a, f(a)) \leq \frac{\delta(a, f(a))}{1 - \kappa} \frac{\delta(f(a), f(f(a)))}{1 - \kappa}$ \hspace{1cm} \{$\kappa \in [0, 1) \text{ so } \kappa > 0$\}

$\Rightarrow \delta(a, f(a)) \leq \omega(a) - \omega(f(a))$ \hspace{1cm} \{def. $\omega$\}

$\Rightarrow a \sqsubseteq f(a)$ \hspace{1cm} \{def. $\sqsubseteq$\} ■

The iterates of $f$ from $a$ are $\langle x_n, n \in \mathbb{N} \rangle$ such that $x_0 = a$ and $x_{n+1} = f(x_n)$.

Corollary 77. The iterates $f$ starting from $a$ are $\sqsubseteq$-increasing.

Proof. By lemma 76, $\forall n \in \mathbb{N} : x_n \sqsubseteq f(x_n) = x_{n+1}$ ■

The third step is to show that the iterates of $f$ from any $a$ have a least upper bound for the partial order $\sqsubseteq$ in $\mathcal{M}$.
Lemma 78. Let \( \langle x_n, n \in \mathbb{N} \rangle \) be the iterates of \( f \) from \( a \). Then the weighted sequence \( \langle \omega(x_n), n \in \mathbb{N} \rangle \) is decreasing and non-negative so has a non-negative limit \( w = \inf_{n \in \mathbb{N}} \omega(x_n) \in \mathbb{R}^+ \).

Proof. \( \omega(x_n) = \frac{\delta(x, f(x))}{1-n} \geq 0 \) since \( \delta(x, f(x)) \geq 0 \) and \( \kappa \in [0, 1) \). By lemma 76, \( x_n \subseteq f(x_n) = x_{n+1} \) so \( 0 \leq \delta(x_n, x_{n+1}) \leq \omega(x_n) - \omega(x_{n+1}) \) proving \( \langle \omega(x_n), n \in \mathbb{N} \rangle \) to be decreasing and non-negative. By exercise 7.7-12, \( \langle \omega(x_n), n \in \mathbb{N} \rangle \) has a non-negative limit \( w \in \mathbb{R}^+ \) which is the greatest lower bound \( w = \inf_{n \in \mathbb{N}} \omega(x_n) \) of \( \langle \omega(x_n), n \in \mathbb{N} \rangle \).

Lemma 79. Let \( \langle x_n, n \in \mathbb{N} \rangle \) be the iterates of \( f \) from \( a \). If \( m \geq n \) then \( \omega(x_m) \leq \kappa^{m-n} \omega(x_n) \).

Proof. By recurrence on \( m \). This is trivially true for \( m = n \) since \( \kappa^0 = 1 \). For the induction step, assume, by induction hypothesis, that \( \omega(x_m) \leq \kappa^{m-n} \omega(x_n) \). \( f \) is contracting so \( \delta(f(x_m), f(f(x_m))) \leq \kappa \delta(x_m, f(x_m)) \). It follows that \( \omega(x_{m+1}) = \omega(f(x_m)) = \frac{\delta(f(x_m), f(f(x_m)))}{1-m} \leq \kappa \frac{\delta(x_m, f(x_m))}{1-m} \leq \kappa \omega(x_m) \leq \kappa \kappa^{m-n} \omega(x_n) = \kappa^{m+1-n} \omega(x_n) \).

Lemma 80. The iterates \( \langle x_n, n \in \mathbb{N} \rangle \) of \( f \) from \( a \) are a Cauchy sequence (hence have a limit \( \ell \in \mathcal{M} \) since \( \langle \mathcal{M}, \delta \rangle \) is complete).

Proof. Assume \( m \geq n \).

\[
\begin{align*}
x_n \subseteq x_m & \quad \text{(the iterates are increasing)} \\
\Rightarrow \quad \delta(x_n, x_m) & \leq \omega(x_n) - \omega(x_m) \quad \text{(def. } \subseteq) \\
\Rightarrow \quad \delta(x_n, x_m) & \leq \omega(x_n) \quad \text{(since } \omega(x_m) \geq 0 \text{ by lemma 78)} \\
\Rightarrow \quad \delta(x_n, x_m) & \leq \kappa^n \omega(a) \quad \text{(by lemma 79 with } m, n := n, 0 \text{ and } x_0 = a) \\
\end{align*}
\]

Given \( \epsilon > 0 \), there exists \( N \in \mathbb{N} \) large enough such that \( \kappa^N \omega(a) < \epsilon \) since \( \omega(a) \geq 0 \) and \( \kappa \in [0, 1) \). For \( m \geq n \geq N \), we have \( \delta(x_n, x_m) \leq \kappa^n \omega(a) \leq \kappa^N \omega(a) < \epsilon \), proving since \( \delta(x_m, x_n) = \delta(x_n, x_m) \) that \( \forall \epsilon > 0 : \exists N \in \mathbb{N} : \forall n, m \geq N : \delta(x_m, x_n) < \epsilon \).

Lemma 81. Let \( \ell \) be the limit of iterates \( \langle x_n, n \in \mathbb{N} \rangle \) of \( f \) from \( a \) in lemma 80 and \( w \) be the limit of the weighted sequence \( \langle \omega(x_n), n \in \mathbb{N} \rangle \) in lemma 78. Then \( w = \omega(\ell) \).

Proof. Let us overestimate
CHAPTER 7. SET FIXPOINTS

\[
|\omega(x_n) - \omega(\ell)| = \left| \frac{\delta(x_n, f(x_n)) - \delta(\ell, f(\ell))}{1 - \kappa} \right| \quad \text{[def. } \omega] \\
= \frac{1}{1 - \kappa} \left| \delta(x_n, f(x_n)) - \delta(\ell, f(\ell)) \right| \quad \text{[} 1 - \kappa > 0 \text{]} \\
= \frac{1}{1 - \kappa} \left| (\delta(x_n, f(x_n)) - \delta(x_n, f(\ell))) - (\delta(\ell, f(\ell)) - \delta(x_n, f(\ell))) \right| \quad \text{[def. } - \delta] \\
\leq \frac{1}{1 - \kappa} \left| (\delta(f(x_n), f(\ell)) - (\delta(\ell, f(\ell)) - \delta(x_n, f(\ell))) \right| \quad \text{(7.1)} \\
\text{by the triangle inequality } \delta(a, b) + \delta(b, c) \geq \delta(a, c) \text{ so } \delta(a, b) - \delta(a, c) \geq -\delta(b, c) \text{ and therefore } \delta(a, c) - \delta(a, b) \leq \delta(b, c) \text{ } [\delta] \\
\text{— If } (\delta(\ell, f(\ell)) - \delta(x_n, f(\ell))) \geq 0 \\
(7.1) \leq \frac{1}{1 - \kappa} \left| (\delta(f(x_n), f(\ell)) + \delta(\ell, x_n)) \right| \quad \text{[by exercise 5.19-1 and } \delta(x, y) > 0 \text{]} \\
\leq \frac{1}{1 - \kappa} \left| (\delta(f(x_n), f(\ell)) + \delta(\ell, x_n)) \right| \quad \text{by the triangle inequality } \delta(a, b) + \delta(b, c) \geq \delta(a, c) \text{ so } \delta(a, b) - \delta(a, c) \geq -\delta(b, c) \text{ and therefore } \delta(c, a) - \delta(b, a) \leq \delta(b, c) \text{ so that } \delta(\ell, x_n) \geq \left| (\delta(\ell, f(\ell)) - \delta(x_n, f(\ell))) \right| \geq 0 \text{ } [\delta] \\
\text{— Otherwise } (\delta(\ell, f(\ell)) - \delta(x_n, f(\ell))) \leq 0 \\
(7.1) \leq \frac{1}{1 - \kappa} \left| (\delta(f(x_n), f(\ell)) + (\delta(x_n, f(\ell)) - \delta(\ell, f(\ell))) \right| \quad \text{[by } a - (-b) = a + b \text{]} \\
= \frac{1}{1 - \kappa} \left( \delta(f(x_n), f(\ell)) + (\delta(x_n, f(\ell)) - \delta(\ell, f(\ell)) \right) \quad \text{[since } \delta(x_n, f(\ell)) - \delta(\ell, f(\ell)) \geq 0 \text{]} \\
\leq \frac{1}{1 - \kappa} \left( \delta(f(x_n), f(\ell)) + \delta(\ell, x_n) \right) \quad \text{[by the triangle inequality]} \\
\text{— Grouping both cases,} \\
\left| \omega(x_n) - \omega(\ell) \right| \\
\leq \frac{1}{1 - \kappa} \left( \kappa \delta(x_n, \ell) + \delta(\ell, x_n) \right) \quad \text{[f contracting]} \\
\leq \frac{1 + \kappa}{1 - \kappa} \delta(x_n, \ell) \quad \text{[symmetry]}
\]
It follows that $\forall \varepsilon > 0 : \exists \varepsilon' = \frac{1-\kappa}{1+\kappa} \varepsilon > 0 : \forall x \in \mathcal{M} : \delta(x, \ell) < \varepsilon' \Rightarrow \delta(\omega(x), \omega(\ell)) \leq \frac{1+\kappa}{1-\kappa} \delta(x, \ell) < \frac{1+\kappa}{1+\kappa} \delta(\omega(x), \omega(\ell)) = \varepsilon$ proving $\omega$ to be continuous at point $\ell$. By lemma 80, $\ell$ is the limit of $(x_n, \ n \in \mathbb{N})$ so at point $\ell$, we have $w = \lim_{n \to \infty} \omega(x_n) = \omega(\lim_{n \to \infty} x_n) = \omega(\ell)$ by exercise 7.7-15.

\textbf{Lemma 82.} The limit $\ell$ of the iterates $(x_n, \ n \in \mathbb{N})$ of $f$ from $a$ is their $\sqsubseteq$-least upper bound $\bigcup_{n \in \mathbb{N}} x_n \in \mathcal{M}$.

\textbf{Proof.} Let us first prove that $\ell$ is an upper bound of the iterates, that is $\forall n \in \mathbb{N} : x_n \sqsubseteq \ell$. The iterates are increasing, so if $m > n$ then $x_n \sqsubseteq x_m$ which implies $\delta(x_m, x_n) \leq \omega(x_m) - \omega(x_n)$. When $m \to +\infty$, $\delta(x_n, x_m) = \delta(\ell, x_m) \leq \omega(x_m) - \omega(\ell)$ proving $x_n \sqsubseteq \ell$.

Let $\ell' \in \mathcal{M}$ be any upper bound of the iterates, that is $\forall n \in \mathbb{N} : x_n \sqsubseteq \ell'$. We have $\delta(x_n, \ell') \leq \omega(x_n) - \omega(\ell')$ so when $n \to +\infty$, we have $x_n \to \ell$ so $\delta(\ell, \ell') \leq \omega(\ell) - \omega(\ell')$ proving $\ell \sqsubseteq \ell'$ so that $\ell$ is the least upper bound of the iterates.

\textbf{Corollary 83.} The limit of $(f(x_n), \ n \in \mathbb{N})$ is $\bigcup_{n \in \mathbb{N}} f(x_n)$.

\textbf{Proof.} $(f(x_n), \ n \in \mathbb{N})$ is $(x_n, \ n \in \mathbb{N}^+)$ and so has the same limit as $(x_n, \ n \in \mathbb{N})$ which, by lemma 82, is $\bigcup_{n \in \mathbb{N}} x_n = \bigcup_{n \in \mathbb{N}^+} x_n = \bigcup_{n \in \mathbb{N}} f(x_n)$.

The fourth step is to show that the function $f$ is increasing and preserves the lub of the iterates.

\textbf{Lemma 84.} Let $(x_n, \ n \in \mathbb{N})$ be the iterates of $f$ from $a$ and $\mathcal{F} \triangleq \{x_n | n \in \mathbb{N}\} = \{f^n(a) | n \in \mathbb{N}\}$, $f$ is $\sqsubseteq$-increasing on $\mathcal{F} \cup \{y | f(y) = y\}$.

\textbf{Proof.} $f$ is $\sqsubseteq$-increasing on $\mathcal{F}$ because the iterates are increasing and on $\{y | f(y) = y\}$ by the fixpoint property.

If $f(x) = x, y \in \mathcal{F}$, and $x \sqsubseteq y$, we have $y \sqsubseteq f(y)$ so $x \sqsubseteq f(y)$ by transitivity, proving $f(x) \sqsubseteq f(y)$ by the fixpoint property.

In case $x \in \mathcal{F}, f(y) = y$, and $x \sqsubseteq y$, we must show that $f(x) \sqsubseteq f(y) = y$ that is $\delta(f(x), y) \leq \omega(f(x)) - \omega(y)$ hence $\delta(f(x), y) \leq \omega(f(x))$ since $\omega(y) \triangleq \frac{\delta(y, f(y))}{1-\kappa} = 0$. This follows from $\omega(f(x)) \triangleq \frac{\delta(x, f(x))}{1-\kappa} \geq \delta(f(x), y)$ since $\kappa \in [0, 1)$.

\textbf{Lemma 85.} $f$ preserves the limit of its iterates $(x_n, \ n \in \mathbb{N})$ from any $a \in \mathcal{M}$ (i.e. $f(\bigcup \mathcal{F}) = \bigcup f^+(\mathcal{F})$ where $f^+(\mathcal{F}) = \{f(x) | x \in \mathcal{F}\}$ and $\mathcal{F} \triangleq \{f^n(a) | n \in \mathbb{N}\}$).

\textbf{Proof.} By lemma 82, $f(\bigcup \mathcal{F}) = f(\lim_{n \to \infty} x_n)$ and, by exercise 7.7-14, $f$ is contracting hence pointwise continuous, so, by exercise 7.7-15, preserves existing limits, that is $f(\lim_{n \to \infty} x_n) = \lim_{n \to \infty} f(x_n)$, which by corollary 83, is $\bigcup f(x_n) = \bigcup \{f(x) | x \in \mathcal{F}\} = \bigcup f^+(\mathcal{F})$.

Then, we have to check the conditions of theorem 87 for $f$ on $(\mathcal{M}, \sqsubseteq)$.
CHAPTER 7. SET FIXPOINTS

Theorem 86 (Banach fixpoint theorem). Any iteration of a contracting mapping \( f \) on a non-empty complete metric space \( (\mathcal{M}, \delta) \) converges to a unique fixpoint.

Proof. Let \( \mathfrak{F} \triangleq \{ f^n(a) \mid n \in \mathbb{N} \} \) be the iterates of \( f \in \mathcal{M} \mapsto \mathcal{M} \) from any \( a \in \mathcal{M} \). By lemma 76, \( a \subseteq f(a) \). By lemma 75, \( (\mathcal{M}, \subseteq) \) hence its subset \( (\mathfrak{F}, \subseteq) \) is a poset. By lemma 82, the lub \( \bigsqcup \mathfrak{F} \in \mathcal{M} \) is well-defined and by lemma 85, \( F(\bigsqcup \mathfrak{F}) = \bigcup \{ f(x) \mid x \in \mathfrak{F} \} \). By lemma 84, \( f \) is \( \subseteq \)-increasing on \( \mathfrak{F} \cup \{ y \mid f(y) = y \} \) so \( f \cap (\mathfrak{F} \times \mathfrak{F} \cup \{ y \in \mathcal{M} \mid y = f(y) \}) \) is \( \subseteq \)-increasing.

By theorem 87, \( \mathrm{lfp} f = \bigsqcup \mathfrak{F} \in \mathcal{M} \).

Fixpoint unicity does not follow from theorem 87 (which is more general so can prove less). If \( f(x) = x \) and \( f(y) = y \) then \( \delta(f(x), f(y)) = \delta(x, y) \) and since \( f \) is contracting \( \delta(f(x), f(y)) \leq \kappa \delta(x, y) \) so \( \delta(x, y) \leq \kappa \delta(x, y) \) where \( \kappa \in [0, 1) \), which implies \( \delta(x, y) = 0 \) that is \( x = y \).

7.6 Bibliography

(Dedekind, 1893) proved corollary 67 and the generalization of theorem 71 in exercise 7.7-3 in the special case where \( f^* \in \wp(S) \mapsto \wp(S) \) is the right image of sets by a function \( f \in S \mapsto S \), that is \( f^*(X) = \{ f(x) \mid x \in X \} \), see exercise ?? in that case \( f^* \) is join-preserving, which implies continuity.

In Tarški’s (1955) proof of theorem 71, the transformer \( F \) is assumed to preserve arbitrary joins, not only joins of ascending chains. But this hypothesis is too strong since, in Tarški’s proof, the lub (least upper bound) \( \sqcup \) is only applied to the ascending chain of iterates, and so the theorem is easily generalized to continuous functions. For the same reason, the theorem is easily extended to complete partial orders (partial orders with an infimum such that any ascending chain has a lub) (Abian and Brown, 1961). Again continuity ia a too strong hypothesis since it is only applied to the iterates, as shown in theorem 73. Moreover, the iterates generalize to increasing functions (Cousot and Cousot, 1979a; Escardó, 2003) and to extensive functions (Bourbaki, 1949) through transfinite iterations (see exercise 7.7-1).

Although there are historical antecedents, theorem 71 is often attributed to Stephen Cole Kleene, maybe by reference to his fixpoint recursion theorem (Kleene, 1938; Kleene, 1952) and Kleene’s star (Kleene, 1951) (as used in regular expressions, see exercises ?? and ??).

Notice that theorem 65 implies that the least solutions to equations \( X = F(X) \) and inequations \( F(X) \subseteq X \) are the same (and similarly for Theorem 71), so that there is no essential difference between fixpoint calculation and constraint solving (Apt, 1997; Cousot and Cousot, 1995).

For an introduction to metric spaces, fixpoints, and topology, as used in section 7.5, see (O’Searcoid, 2006; Bryant, 1985; Dugundji and Granas, 2003; Sutherland, 2009; Kelley, 1955; Dugundji, 1966).
Banach’s metric fixpoint theorem (Banach, 1932) is a generalization of Charles Émile Picard Iteration who gave the contraction condition (7.1) in (Picard, 1890, Chapitre V, Quelques remarques sur les équations différentielles ordinaires, p. 198) and successfully revived Liouville’s (1837) method of successive approximations to prove the existence of solutions to differential equations.

Our proof of Banach’s fixpoint theorem is simplified variant of (Baranga, 1991; Edalat and Heckmann, 1998; Weihrauch and Schreiber, 1981) themselves following (DeMarr, 1965) to embed a metric space into a poset. The interest of this proof of theorem is to show that the metric fixpoint semantics of programs (Arnold and Nivat, 1980; de Bakker and de Vink, 1996; Seda and Hitzler, 2010) can be translated in terms of partial orders.

The use of fixpoints in Computer Science originates from (Ginsburg and Rice, 1962) and (Schützenberger, 1962) for Noam Chomsky’s context free syntax (Chomsky, 1956) (see exercise 7.7-6) and from Dana Scott for the semantics of programming languages (Scott, 1970) (see exercise ??).

7.7 Exercises

Exercise 7.7-1 Study the consequences of the definition of continuity where chains are defined as subsets of a poset such that any two elements are comparable (and compare to the definition of continuity given in theorem 71).

The following exercise is useful to \(\subseteq\)-overapproximate fixpoints, as usual in static analysis (Cousot and Cousot, 1977a).

Exercise 7.7-2 Let \(F, G \in \wp(S) \rightarrow \wp(S)\) be \(\subseteq\)-increasing such that \(F \subseteq G \triangleq \forall X \in \wp(S) : F(X) \subseteq G(X)\). Prove that if \(A \subseteq F(A)\) then \(\text{lfp}_{A}^{\subseteq} F \subseteq \text{lfp}_{A}^{\subseteq} G\).

The following exercise generalize theorem 71 to \(\text{lfp}_{A}^{\subseteq} F\) as considered in corollary 67.

Exercise 7.7-3 Assume that \(A \in \wp(S)\) and \(F \in \wp(S) \rightarrow \wp(S)\). Let \(\text{lfp}_{A}^{\subseteq} F\) be the least fixpoint of \(F\) greater than or equal to \(A\), if any \(^{4}\). Assume that the function \(F\) is continuous and that \(A \subseteq F(A)\). The iterates \(\langle F_{n}, n \in \mathbb{N} \rangle\) of \(F\) from \(A\) are \(F_{0} \triangleq A\) and \(F_{n+1} \triangleq F(F_{n})\). Prove that \(\text{lfp}_{A}^{\subseteq} F = \bigcup_{n \in \mathbb{N}} F_{n}\).

Exercise 7.7-4 Show that if \(F \in \wp(S) \rightarrow \wp(S)\) is increasing and \(A \in \wp(S)\) is such that \(A \subseteq F(A)\) then \(\text{lfp}_{A}^{\subseteq} F = \text{lfp}_{\wp(S)}^{\subseteq} \lambda X \cdot A \cup F(X)\).

\(^{4}\) So \(A \subseteq \text{lfp}_{A}^{\subseteq} F = F(\text{lfp}_{A}^{\subseteq} F)\) and if \(A \subseteq X = F(X)\) then \(\text{lfp}_{A}^{\subseteq} F \subseteq X\).
CHAPTER 7. SET FIXPOINTS

Exercise 7.7-5 (Tarski’s dual set-theoretic iterative fixpoint theorem)
Let \( S' \) be a set and the function \( F \in \wp(S') \mapsto \wp(S') \) be \( \subseteq \)-increasing, with iterates \( \langle F_n, n \in \mathbb{N} \rangle \) such that \( F_0 \triangleq S' \) and \( F_{n+1} \triangleq F(F_n) \). Assume that \( F(\bigcap_{n \in \mathbb{N}} F_n) = \bigcap_{n \in \mathbb{N}} F_{n+1} \). Prove that \( \text{gfp}^\exists F = \bigcap_{n \in \mathbb{N}} F_n \).

Exercise 7.7-6 Consider the context-free grammar \( X ::= a \mid bx \) on the terminal alphabet \( \Sigma = \{a, b\} \) defining the language \( \mathcal{W} = \{b^n a \mid n \in \mathbb{N}\} \) where \( b^0 = \epsilon \) is the empty sentence, \( b^1 = b \), and \( b^{n+1} = bb^n \) (see chapter 7). Prove that \( \mathcal{W} = \text{lfp}_0 F \) where \( F \triangleq \lambda X \cdot \{a\} \cup \{b \sigma \mid \sigma \in X\} \).

Exercise 7.7-7 Continuing exercise 6.4-6, let \( I \triangleq \{1, x \mid x \in \mathbb{Z}\} \). Calculate the limit of the iterates of \( \lambda X \cdot I \cup \text{post}[R(n)]X \) from \( \emptyset \). What is the intuitive interpretation of this formula in term of the program executions?

Exercise 7.7-8 Prove the following generalization 73 of theorem 71 to posets.

Theorem 87 (Strong Tarski’s iterative fixpoint theorem for posets). Let \( \mathcal{X} \) be a set equipped with a binary relation \( \sqsubseteq \), \( F \in \mathcal{X} \mapsto \mathcal{X} \), and \( A \in \mathcal{X} \) such that \( A \sqsubseteq F(A) \). Define \( \mathfrak{I} \triangleq \{F^n(A) \mid n \in \mathbb{N}\} \) to be the iterates of \( F \) from \( A \). Assume that \( \langle \mathfrak{I}, \sqsubseteq \rangle \) is a poset (with partially defined lub \( \sqcup \)) such that \( \sqcup \mathfrak{I} \in \mathcal{X} \) and \( F(\sqcup \mathfrak{I}) = \sqcup\{F(X) \mid X \in \mathfrak{I}\} \). Then \( \sqcup \mathfrak{I} \) is a fixpoint of \( F \) in \( \mathcal{X}, \sqsubseteq \) greater than or equal to \( A \).

Moreover, if \( F \cap (\mathfrak{I} \times \mathfrak{I} \cup \{Y \in \mathcal{X} \mid Y = F(Y)\}) \) is \( \sqsubseteq \) increasing then \( \text{lfp}_A^\exists F = \sqcup \mathfrak{I} \in \mathcal{X} \).

Exercise 7.7-9 Prove the Banach and Tarski’s (1924) decomposition theorem: given non-empty sets \( \mathcal{X}, \mathcal{Y} \), and maps \( f \in \mathcal{X} \mapsto \mathcal{Y} \) and \( g \in \mathcal{Y} \mapsto \mathcal{X} \), prove that there exists sets \( \mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}_1, \) and \( \mathcal{Y}_2 \) such that \( \mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2, \mathcal{Y} = \mathcal{Y}_1 \cup \mathcal{Y}_2, f^*(\mathcal{X}_1) = \mathcal{Y}_1 \) and \( g^*(\mathcal{Y}_2) = \mathcal{X}_2 \). (Hint: study the fixpoints of \( F \in \wp(\mathcal{X}) \mapsto \wp(\mathcal{Y}) \) defined as \( F(X) = \mathcal{X} \setminus g^*(\mathcal{Y} \setminus f^*(X)) \).)

The Georg Cantor-Schröder-Felix Bernstein theorem (1895–1897, and published by Émile L. Borel citing Cantor-Rad Bernard Bernstein (Borel, 1898, Note 1, La notion des puissances, pp. 102–107)) follows from Banach and Tarski’s (1924) decomposition theorem (the iterates of \( F \) are used instead in Borel’s proof).

Exercise 7.7-10 Let \( \mathcal{X} \) and \( \mathcal{Y} \) non-empty sets and \( f \in \mathcal{X} \mapsto \mathcal{Y} \) and \( g \in \mathcal{Y} \mapsto \mathcal{X} \) be two injections. Then there exists a bijection from \( \mathcal{X} \) onto \( \mathcal{Y} \).

Exercise 7.7-11 Show that the limit of a convergent sequence in a metric space is unique.
Exercise 7.7-12  Prove that any decreasing sequence of reals which is bounded from below converges to a limit which is the greatest lower bound of the sequence.

Exercise 7.7-13  Prove that any convergent sequence in a metric space \( (M,\delta) \) is a Cauchy sequence.

Exercise 7.7-14  Show that any pointwise continuous function \( f \in M \mapsto M \) on a metric space \( (M,\delta) \) is pointwise continuous.

Exercise 7.7-15  Show that any contracting function \( S \) is said to be a simulation of \( R \) if and only if \( S \) preserves existing limits (if \( \lim_{n \to \infty} x_n = \ell \) then \( \lim_{n \to \infty} f(x_n) = f(\ell) \)).

Exercise 7.7-16 (Bisimulation)  Given sets \( A \) (of actions), \( S, S' \) (of states) and relations \( R, R' \in A \mapsto \wp(\Sigma \times \Sigma) \) and \( R, R' \in \wp(\Sigma' \times \Sigma') \), ROBIN MILNER defines a simulation (Milner, 1971) to be a relation \( S \in \wp(\Sigma \times \Sigma') \) such that

\[
\forall a \in A : \forall x, y \in S, x' \in S' : (S(x, x') \wedge R(a)(x, y)) \Rightarrow (\exists y' \in S' : R'(a)(x', y') \wedge S(y, y'))
\]

\[
\Leftrightarrow \forall a \in A : \forall y \in S, x' \in S' : (\exists x \in S : S^{-1}(x, x') \wedge R(a)(x, y)) \Rightarrow (\exists y' \in S' : R'(a)(x', y') \wedge S^{-1}(y, y'))
\]

\[
(\text{def. } \exists \Rightarrow, \text{ and } -1)
\]

\[
\Leftrightarrow \forall a \in A : \forall y \in S, x' \in S' : (S^{-1}(x, x') \wedge R(a)(x, y)) \Rightarrow (R'(a) \circ S^{-1})(x', y') \quad (\text{def. } \subseteq)
\]

in which case \( S \) is said to be a simulation of \( R \) by \( R' \) or \( R' \) is said to simulate \( R \) by \( S \).

Park defines a bisimulation (Park, 1981) to be a simulation \( S \) of \( R \) by \( R' \) such that \( S^{-1} \) is a simulation of \( R' \) by \( R \).

\[
\forall a \in A : S^{-1} \subseteq R(a) \subseteq R'(a) \wedge S \subseteq R'(a) \subseteq R(a) \subseteq S.
\]

(a)  Prove that two relations can be similar to one another (maybe through different simulation relations \( S \)) while not being bisimilar.

(b)  Prove that \( S \) is a bisimulation between \( R \) and \( R' \) if and only if \( S \subseteq \mathcal{B}_{R,R'}(S) \) where

\[
\mathcal{B}_{R,R'}(S) \triangleq \{ \langle x, x' \rangle \mid \forall a \in A : (\forall y \in S : R(a)(x, y) \Rightarrow (R'(a) \circ S^{-1})(x', y))
\]

\[
\wedge (\forall y' \in S' : R'(a)(x', y') \Rightarrow (R(a) \circ S)(x, y')) \}
\]

(c)  Prove that for any two relations \( R \) and \( R' \) there is a \( \subseteq \)-greatest bisimulation between them and provide a fixpoint characterization.

(d)  Assuming \( S \) to be finite, design an algorithm which, given an input \( R \), will compute the \( \subseteq \)-greatest bisimulation \( \sim \) between the relation \( R \) and itself. Prove that the algorithm terminates and returns \( \sim \).

(e)  Prove that in (d), \( \sim \) is an equivalence relation.