Semantics and Verification of Software

Lecture 6: Denotational Semantics of WHILE II (CCPOs and Continuous Functions)

Thomas Noll

Lehrstuhl für Informatik 2
(Software Modeling and Verification)

RWTH AACHEN UNIVERSITY

noll@cs.rwth-aachen.de

http://www-i2.informatik.rwth-aachen.de/i2/svsw13/

Summer Semester 2013

Outline

Semantics of Statements

Definition (Denotational semantics of statements)

The (denotational) semantic functional for statements,

$$\mathfrak{C}[\![.]\!] : Cmd \to (\Sigma \dashrightarrow \Sigma),$$

is given by:

$$\begin{aligned}
\mathfrak{C}[\![\texttt{skip}]\!] &:= \mathrm{id}_\Sigma \\
\mathfrak{C}[\![x \texttt{ := } a]\!]\sigma &:= \sigma[x \mapsto \mathfrak{A}[\![a]\!]\sigma] \\
\mathfrak{C}[\![c_1\,\texttt{;}\,c_2]\!] &:= \mathfrak{C}[\![c_2]\!] \circ \mathfrak{C}[\![c_1]\!] \\
\mathfrak{C}[\![\texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2]\!] &:= \mathrm{cond}(\mathfrak{B}[\![b]\!], \mathfrak{C}[\![c_1]\!], \mathfrak{C}[\![c_2]\!]) \\
\mathfrak{C}[\![\texttt{while } b \texttt{ do } c]\!] &:= \mathrm{fix}(\Phi)
\end{aligned}$$

where $\Phi : (\Sigma \dashrightarrow \Sigma) \to (\Sigma \dashrightarrow \Sigma) : f \mapsto \mathrm{cond}(\mathfrak{B}[\![b]\!], f \circ \mathfrak{C}[\![c]\!], \mathrm{id}_\Sigma)$

Characterization of fix(Φ) I

Now $\mathsf{fix}(\Phi)$ can be characterized by:

- $\mathsf{fix}(\Phi)$ is a fixpoint of Φ, i.e.,

$$\Phi(\mathsf{fix}(\Phi)) = \mathsf{fix}(\Phi)$$

- $\mathsf{fix}(\Phi)$ is minimal with respect to $\sqsubseteq$, i.e., for every $f_0 : \Sigma \dashrightarrow \Sigma$ such that $\Phi(f_0) = f_0$,

$$\mathsf{fix}(\Phi) \sqsubseteq f_0$$

(where $f \sqsubseteq g \iff$ for every $\sigma, \sigma' \in \Sigma : f(\sigma) = \sigma' \Rightarrow g(\sigma) = \sigma'$)

Example

For `while true do skip` we obtain for every $f : \Sigma \dashrightarrow \Sigma$:

$$\Phi(f) = \mathsf{cond}(\mathfrak{B}[\![\mathsf{true}]\!], f \circ \mathfrak{C}[\![\mathtt{skip}]\!], \mathsf{id}_\Sigma) = f$$

$\Rightarrow \mathsf{fix}(\Phi) = f_\emptyset$ where $f_\emptyset(\sigma) :=$ undefined for every $\sigma \in \Sigma$
(that is, $\mathsf{graph}(f_\emptyset) = \emptyset$)

Characterization of fix(Φ) II

Goals:

- Prove existence of fix(Φ) for $\Phi(f) = \text{cond}(\mathfrak{B}[\![b]\!], f \circ \mathfrak{C}[\![c]\!], \text{id}_\Sigma)$
- Show how it can be "computed" (more exactly: approximated)

Sufficient conditions:

on domain $\Sigma \dashrightarrow \Sigma$: chain-complete partial order

on function Φ: continuity

Outline

Partial Orders

Definition 6.1 (Partial order)

A partial order (PO) $(D, \sqsubseteq)$ consists of a set D, called domain, and of a relation $\sqsubseteq \subseteq D \times D$ such that, for every $d_1, d_2, d_3 \in D$,

reflexivity: $d_1 \sqsubseteq d_1$

transitivity: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_3 \Rightarrow d_1 \sqsubseteq d_3$

antisymmetry: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_1 \Rightarrow d_1 = d_2$

It is called total if, in addition, always $d_1 \sqsubseteq d_2$ or $d_2 \sqsubseteq d_1$.

Partial Orders

Definition 6.1 (Partial order)

A partial order (PO) $(D, \sqsubseteq)$ consists of a set D, called domain, and of a relation $\sqsubseteq \subseteq D \times D$ such that, for every $d_1, d_2, d_3 \in D$,

reflexivity: $d_1 \sqsubseteq d_1$

transitivity: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_3 \Rightarrow d_1 \sqsubseteq d_3$

antisymmetry: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_1 \Rightarrow d_1 = d_2$

It is called total if, in addition, always $d_1 \sqsubseteq d_2$ or $d_2 \sqsubseteq d_1$.

Example 6.2

1. $(\mathbb{N}, \leq)$ is a total partial order

Partial Orders

Definition 6.1 (Partial order)

A partial order (PO) $(D, \sqsubseteq)$ consists of a set D, called domain, and of a relation $\sqsubseteq \subseteq D \times D$ such that, for every $d_1, d_2, d_3 \in D$,

reflexivity: $d_1 \sqsubseteq d_1$

transitivity: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_3 \Rightarrow d_1 \sqsubseteq d_3$

antisymmetry: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_1 \Rightarrow d_1 = d_2$

It is called total if, in addition, always $d_1 \sqsubseteq d_2$ or $d_2 \sqsubseteq d_1$.

Example 6.2

1. $(\mathbb{N}, \leq)$ is a total partial order
2. $(2^{\mathbb{N}}, \subseteq)$ is a (non-total) partial order

Partial Orders

Definition 6.1 (Partial order)

A partial order (PO) $(D, \sqsubseteq)$ consists of a set D, called domain, and of a relation $\sqsubseteq \subseteq D \times D$ such that, for every $d_1, d_2, d_3 \in D$,

reflexivity: $d_1 \sqsubseteq d_1$

transitivity: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_3 \Rightarrow d_1 \sqsubseteq d_3$

antisymmetry: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_1 \Rightarrow d_1 = d_2$

It is called total if, in addition, always $d_1 \sqsubseteq d_2$ or $d_2 \sqsubseteq d_1$.

Example 6.2

1. $(\mathbb{N}, \leq)$ is a total partial order
2. $(2^{\mathbb{N}}, \subseteq)$ is a (non-total) partial order
3. $(\mathbb{N}, <)$ is not a partial order

Partial Orders

Definition 6.1 (Partial order)

A partial order (PO) $(D, \sqsubseteq)$ consists of a set D, called domain, and of a relation $\sqsubseteq \subseteq D \times D$ such that, for every $d_1, d_2, d_3 \in D$,

reflexivity: $d_1 \sqsubseteq d_1$

transitivity: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_3 \Rightarrow d_1 \sqsubseteq d_3$

antisymmetry: $d_1 \sqsubseteq d_2$ and $d_2 \sqsubseteq d_1 \Rightarrow d_1 = d_2$

It is called total if, in addition, always $d_1 \sqsubseteq d_2$ or $d_2 \sqsubseteq d_1$.

Example 6.2

1. $(\mathbb{N}, \leq)$ is a total partial order
2. $(2^{\mathbb{N}}, \subseteq)$ is a (non-total) partial order
3. $(\mathbb{N}, <)$ is not a partial order (since not reflexive)

Application to fix(Φ)

Lemma 6.3

$(\Sigma \dashrightarrow \Sigma, \sqsubseteq)$ *is a partial order.*

Application to $\mathrm{fix}(\Phi)$

Lemma 6.3

$(\Sigma \dashrightarrow \Sigma, \sqsubseteq)$ *is a partial order.*

Proof.

using the equivalence $f \sqsubseteq g \iff \mathrm{graph}(f) \subseteq \mathrm{graph}(g)$ and the partial-order property of $\subseteq$ □

Chains and Least Upper Bounds I

Definition 6.4 (Chain, (least) upper bound)

Let $(D, \sqsubseteq)$ be a partial order and $S \subseteq D$.

1. S is called a **chain** in D if, for every $s_1, s_2 \in S$,

$$s_1 \sqsubseteq s_2 \text{ or } s_2 \sqsubseteq s_1$$

(that is, S is a totally ordered subset of D).

Chains and Least Upper Bounds I

Definition 6.4 (Chain, (least) upper bound)

Let $(D, \sqsubseteq)$ be a partial order and $S \subseteq D$.

1. S is called a chain in D if, for every $s_1, s_2 \in S$,

$$s_1 \sqsubseteq s_2 \text{ or } s_2 \sqsubseteq s_1$$

   (that is, S is a totally ordered subset of D).
2. An element $d \in D$ is called an upper bound of S if $s \sqsubseteq d$ for every $s \in S$ (notation: $S \sqsubseteq d$).

Chains and Least Upper Bounds I

Definition 6.4 (Chain, (least) upper bound)

Let $(D, \sqsubseteq)$ be a partial order and $S \subseteq D$.

1. S is called a chain in D if, for every $s_1, s_2 \in S$,
$$s_1 \sqsubseteq s_2 \text{ or } s_2 \sqsubseteq s_1$$
(that is, S is a totally ordered subset of D).
2. An element $d \in D$ is called an upper bound of S if $s \sqsubseteq d$ for every $s \in S$ (notation: $S \sqsubseteq d$).
3. An upper bound d of S is called least upper bound (LUB) or supremum of S if $d \sqsubseteq d'$ for every upper bound d' of S (notation: $d = \bigsqcup S$).

Chains and Least Upper Bounds II

Example 6.5

1. Every subset $S \subseteq \mathbb{N}$ is a chain in $(\mathbb{N}, \leq)$.
   It has a LUB (its greatest element) iff it is finite.

Chains and Least Upper Bounds II

Example 6.5

1. Every subset $S \subseteq \mathbb{N}$ is a chain in $(\mathbb{N}, \leq)$.
   It has a LUB (its greatest element) iff it is finite.
2. $\{\emptyset, \{0\}, \{0, 1\}, \ldots\}$ is a chain in $(2^{\mathbb{N}}, \subseteq)$ with LUB $\mathbb{N}$.

Chains and Least Upper Bounds II

Example 6.5

1. Every subset $S \subseteq \mathbb{N}$ is a chain in $(\mathbb{N}, \leq)$.
   It has a LUB (its greatest element) iff it is finite.
2. $\{\emptyset, \{0\}, \{0,1\}, \ldots\}$ is a chain in $(2^{\mathbb{N}}, \subseteq)$ with LUB $\mathbb{N}$.
3. Let $x \in Var$, and let $f_i : \Sigma \dashrightarrow \Sigma$ for every $i \in \mathbb{N}$ be given by

   $$f_i(\sigma) := \begin{cases} \sigma[x \mapsto \sigma(x) + 1] & \text{if } \sigma(x) \leq i \\ \text{undefined} & \text{otherwise} \end{cases}$$

   Then $\{f_0, f_1, f_2, \ldots\}$ is a chain in $(\Sigma \dashrightarrow \Sigma, \sqsubseteq)$, since for every $i \in \mathbb{N}$ and $\sigma, \sigma' \in \Sigma$:

   $$\begin{array}{rl} & f_i(\sigma) = \sigma' \\ \Rightarrow & \sigma(x) \leq i, \sigma' = \sigma[x \mapsto \sigma(x) + 1] \\ \Rightarrow & \sigma(x) \leq i + 1, \sigma' = \sigma[x \mapsto \sigma(x) + 1] \\ \Rightarrow & f_{i+1}(\sigma) = \sigma' \\ \Rightarrow & f_i \sqsubseteq f_{i+1} \end{array}$$

Chain Completeness

Definition 6.6 (Chain completeness)

A partial order is called chain complete (CCPO) if every of its chains has a least upper bound.

Chain Completeness

Definition 6.6 (Chain completeness)

A partial order is called chain complete (CCPO) if every of its chains has a least upper bound.

Example 6.7

1. $(2^{\mathbb{N}}, \subseteq)$ is a CCPO with $\bigsqcup S = \bigcup_{M \in S} M$ for every chain $S \subseteq 2^{\mathbb{N}}$.

Chain Completeness

Definition 6.6 (Chain completeness)

A partial order is called chain complete (CCPO) if every of its chains has a least upper bound.

Example 6.7

1. $(2^{\mathbb{N}}, \subseteq)$ is a CCPO with $\bigsqcup S = \bigcup_{M \in S} M$ for every chain $S \subseteq 2^{\mathbb{N}}$.
2. $(\mathbb{N}, \leq)$ is not chain complete

Chain Completeness

Definition 6.6 (Chain completeness)

A partial order is called chain complete (CCPO) if every of its chains has a least upper bound.

Example 6.7

1. $(2^{\mathbb{N}}, \subseteq)$ is a CCPO with $\bigsqcup S = \bigcup_{M \in S} M$ for every chain $S \subseteq 2^{\mathbb{N}}$.
2. $(\mathbb{N}, \leq)$ is not chain complete (since, e.g., the chain $\mathbb{N}$ has no upper bound).

Least Elements in CCPOs

Corollary 6.8

Every CCPO has a least element $\bigsqcup \emptyset$.

Least Elements in CCPOs

Corollary 6.8

Every CCPO has a least element $\bigsqcup \emptyset$.

Proof.

Let $(D, \sqsubseteq)$ be a CCPO.

- By definition, $\emptyset$ is a chain in D.

Least Elements in CCPOs

Corollary 6.8

Every CCPO has a least element $\bigsqcup \emptyset$.

Proof.

Let $(D, \sqsubseteq)$ be a CCPO.

- By definition, $\emptyset$ is a chain in D.
- By definition, every $d \in D$ is an upper bound of $\emptyset$.

Least Elements in CCPOs

Corollary 6.8

Every CCPO has a least element $\bigsqcup \emptyset$.

Proof.

Let $(D, \sqsubseteq)$ be a CCPO.

- By definition, $\emptyset$ is a chain in D.
- By definition, every $d \in D$ is an upper bound of $\emptyset$.
- Thus $\bigsqcup \emptyset$ exists and is the least element of D.

□

Application to fix(Φ)

Lemma 6.9

- $(\Sigma \dashrightarrow \Sigma, \sqsubseteq)$ *is a CCPO with least element* $f_\emptyset$ *where* $\mathrm{graph}(f_\emptyset) = \emptyset$.
- *In particular, for every chain* $S \subseteq \Sigma \dashrightarrow \Sigma$,

$$\mathrm{graph}\left(\bigsqcup S\right) = \bigcup_{f \in S} \mathrm{graph}(f).$$

Application to $\mathrm{fix}(\Phi)$

Lemma 6.9

- $(\Sigma \dashrightarrow \Sigma, \sqsubseteq)$ *is a CCPO with least element* $f_\emptyset$ *where* $\mathrm{graph}(f_\emptyset) = \emptyset$.
- *In particular, for every chain* $S \subseteq \Sigma \dashrightarrow \Sigma$,

$$\mathrm{graph}\left(\bigsqcup S\right) = \bigcup_{f \in S} \mathrm{graph}(f).$$

Proof.

on the board □

Application to $\text{fix}(\Phi)$

Lemma 6.9

- *$(\Sigma \dashrightarrow \Sigma, \sqsubseteq)$ is a CCPO with least element $f_\emptyset$ where $\text{graph}(f_\emptyset) = \emptyset$.*
- *In particular, for every chain $S \subseteq \Sigma \dashrightarrow \Sigma$,*

$$\text{graph}\left(\bigsqcup S\right) = \bigcup_{f \in S} \text{graph}(f).$$

Proof.

on the board □

Example 6.10 (cf. Example 6.5(3))

Let $x \in Var$, and let $f_i : \Sigma \dashrightarrow \Sigma$ for every $i \in \mathbb{N}$ be given by

$$f_i(\sigma) := \begin{cases} \sigma[x \mapsto \sigma(x) + 1] & \text{if } \sigma(x) \leq i \\ \text{undefined} & \text{otherwise} \end{cases}$$

Then $S := \{f_0, f_1, f_2, \ldots\}$ is a chain (Example 6.5(3)) with $\bigsqcup S = f$ where

$$f : \Sigma \to \Sigma : \sigma \mapsto \sigma[x \mapsto \sigma(x) + 1]$$

Outline

1. Recapitulation: Denotational Semantics of WHILE
2. Chain-Complete Partial Orders
3. Monotonic and Continuous Functions
4. The Fixpoint Theorem

Monotonicity I

Definition 6.11 (Monotonicity)

Let $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$ be partial orders, and let $F : D \to D'$. F is called monotonic (w.r.t. $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$) if, for every $d_1, d_2 \in D$,

$$d_1 \sqsubseteq d_2 \Rightarrow F(d_1) \sqsubseteq' F(d_2).$$

Monotonicity I

Definition 6.11 (Monotonicity)

Let $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$ be partial orders, and let $F : D \to D'$. F is called monotonic (w.r.t. $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$) if, for every $d_1, d_2 \in D$,

$$d_1 \sqsubseteq d_2 \Rightarrow F(d_1) \sqsubseteq' F(d_2).$$

Interpretation: monotonic functions "preserve information"

Monotonicity I

Definition 6.11 (Monotonicity)

Let $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$ be partial orders, and let $F : D \to D'$. F is called monotonic (w.r.t. $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$) if, for every $d_1, d_2 \in D$,

$$d_1 \sqsubseteq d_2 \Rightarrow F(d_1) \sqsubseteq' F(d_2).$$

Interpretation: monotonic functions “preserve information”

Example 6.12

1. Let $T := \{S \subseteq \mathbb{N} \mid S \text{ finite}\}$. Then $F_1 : T \to \mathbb{N} : S \mapsto \sum_{n \in S} n$ is monotonic w.r.t. $(2^{\mathbb{N}}, \subseteq)$ and $(\mathbb{N}, \leq)$.

Monotonicity I

Definition 6.11 (Monotonicity)

Let $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$ be partial orders, and let $F : D \to D'$. F is called monotonic (w.r.t. $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$) if, for every $d_1, d_2 \in D$,

$$d_1 \sqsubseteq d_2 \Rightarrow F(d_1) \sqsubseteq' F(d_2).$$

Interpretation: monotonic functions "preserve information"

Example 6.12

1. Let $T := \{S \subseteq \mathbb{N} \mid S \text{ finite}\}$. Then $F_1 : T \to \mathbb{N} : S \mapsto \sum_{n \in S} n$ is monotonic w.r.t. $(2^{\mathbb{N}}, \subseteq)$ and $(\mathbb{N}, \leq)$.
2. $F_2 : 2^{\mathbb{N}} \to 2^{\mathbb{N}} : S \mapsto \mathbb{N} \setminus S$ is not monotonic w.r.t. $(2^{\mathbb{N}}, \subseteq)$ (since, e.g., $\emptyset \subseteq \mathbb{N}$ but $F_2(\emptyset) = \mathbb{N} \not\subseteq F_2(\mathbb{N}) = \emptyset$).

Application to fix(Φ)

Lemma 6.13

Let $b \in BExp$, $c \in Cmd$, *and* $\Phi : (\Sigma \dashrightarrow \Sigma) \to (\Sigma \dashrightarrow \Sigma)$ *with* $\Phi(f) := \mathrm{cond}(\mathfrak{B}[\![b]\!], f \circ \mathfrak{C}[\![c]\!], \mathrm{id}_\Sigma)$*. Then* Φ *is monotonic w.r.t.* $(\Sigma \dashrightarrow \Sigma, \sqsubseteq)$*.*

Application to fix(Φ)

Lemma 6.13

Let $b \in BExp$, $c \in Cmd$, *and* $\Phi : (\Sigma \dashrightarrow \Sigma) \to (\Sigma \dashrightarrow \Sigma)$ *with* $\Phi(f) := \mathrm{cond}(\mathfrak{B}[\![b]\!], f \circ \mathfrak{C}[\![c]\!], \mathrm{id}_\Sigma)$. *Then* Φ *is monotonic w.r.t.* $(\Sigma \dashrightarrow \Sigma, \sqsubseteq)$.

Proof.

on the board □

Monotonicity II

The following lemma states how chains behave under monotonic functions.

Lemma 6.14

Let $(D, \sqsubseteq)$ *and* $(D', \sqsubseteq')$ *be CCPOs,* $F : D \to D'$ *monotonic, and* $S \subseteq D$ *a chain in* D*. Then:*

1. $F(S) := \{F(d) \mid d \in S\}$ *is a chain in* D'*.*
2. $\bigsqcup F(S) \sqsubseteq' F(\bigsqcup S)$*.*

The following lemma states how chains behave under monotonic functions.

Lemma 6.14

Let $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$ be CCPOs, $F : D \to D'$ monotonic, and $S \subseteq D$ a chain in D. Then:

1. $F(S) := \{F(d) \mid d \in S\}$ *is a chain in* D'.
2. $\bigsqcup F(S) \sqsubseteq' F(\bigsqcup S)$.

Proof.

on the board □

Continuity

A function F is continuous if the order of applying F and taking LUBs can be reversed:

Definition 6.15 (Continuity)

Let $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$ be CCPOs and $F : D \to D'$ monotonic. Then F is called continuous (w.r.t. $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$) if, for every non-empty chain $S \subseteq D$,

$$F\left(\bigsqcup S\right) = \bigsqcup F(S).$$

Continuity

A function F is continuous if the order of applying F and taking LUBs can be reversed:

Definition 6.15 (Continuity)

Let $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$ be CCPOs and $F : D \to D'$ monotonic. Then F is called continuous (w.r.t. $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$) if, for every non-empty chain $S \subseteq D$,

$$F\left(\bigsqcup S\right) = \bigsqcup F(S).$$

Lemma 6.16

Let $b \in BExp$, $c \in Cmd$, and $\Phi(f) := \mathrm{cond}(\mathfrak{B}[\![b]\!], f \circ \mathfrak{C}[\![c]\!], \mathrm{id}_\Sigma)$. Then Φ is continuous w.r.t. $(\Sigma \dashrightarrow \Sigma, \sqsubseteq)$.

Continuity

A function F is continuous if the order of applying F and taking LUBs can be reversed:

Definition 6.15 (Continuity)

Let $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$ be CCPOs and $F : D \to D'$ monotonic. Then F is called continuous (w.r.t. $(D, \sqsubseteq)$ and $(D', \sqsubseteq')$) if, for every non-empty chain $S \subseteq D$,

$$F\left(\bigsqcup S\right) = \bigsqcup F(S).$$

Lemma 6.16

Let $b \in BExp$, $c \in Cmd$, and $\Phi(f) := \mathrm{cond}(\mathfrak{B}[\![b]\!], f \circ \mathfrak{C}[\![c]\!], \mathrm{id}_\Sigma)$. Then Φ is continuous w.r.t. $(\Sigma \dashrightarrow \Sigma, \sqsubseteq)$.

Proof.

omitted □

Outline

1. Recapitulation: Denotational Semantics of WHILE
2. Chain-Complete Partial Orders
3. Monotonic and Continuous Functions
4. The Fixpoint Theorem

The Fixpoint Theorem

Alfred Tarski (1901–1983)

Bronislaw Knaster (1893–1990)

Theorem 6.17 (Fixpoint Theorem by Tarski and Knaster)

Let $(D, \sqsubseteq)$ be a CCPO and $F : D \to D$ continuous. Then

$$\text{fix}(F) := \bigsqcup \left\{ F^n \left(\bigsqcup \emptyset \right) \mid n \in \mathbb{N} \right\}$$

is the least fixpoint of F where

$$F^0(d) := d \text{ and } F^{n+1}(d) := F(F^n(d)).$$

The Fixpoint Theorem

Alfred Tarski (1901–1983)

Bronislaw Knaster (1893–1990)

Theorem 6.17 (Fixpoint Theorem by Tarski and Knaster)

Let $(D, \sqsubseteq)$ be a CCPO and $F : D \to D$ continuous. Then

$$\text{fix}(F) := \bigsqcup \left\{ F^n \left(\bigsqcup \emptyset \right) \mid n \in \mathbb{N} \right\}$$

is the least fixpoint of F where

$$F^0(d) := d \text{ and } F^{n+1}(d) := F(F^n(d)).$$

Proof.

on the board □

Application to $\mathrm{fix}(\Phi)$

Altogether this completes the definition of $\mathfrak{C}[\![.]\!]$. In particular, for the `while` statement we obtain:

Corollary 6.18

Let $b \in BExp$, $c \in Cmd$, *and* $\Phi(f) := \mathrm{cond}(\mathfrak{B}[\![b]\!], f \circ \mathfrak{C}[\![c]\!], \mathrm{id}_\Sigma)$. *Then*

$$\mathrm{graph}(\mathrm{fix}(\Phi)) = \bigcup_{n \in \mathbb{N}} \mathrm{graph}(\Phi^n(f_\emptyset))$$

Application to $\text{fix}(\Phi)$

Altogether this completes the definition of $\mathfrak{C}[\![.]\!]$. In particular, for the `while` statement we obtain:

Corollary 6.18

Let $b \in BExp$, $c \in Cmd$, *and* $\Phi(f) := \text{cond}(\mathfrak{B}[\![b]\!], f \circ \mathfrak{C}[\![c]\!], \text{id}_\Sigma)$. *Then*

$$\text{graph}(\text{fix}(\Phi)) = \bigcup_{n \in \mathbb{N}} \text{graph}(\Phi^n(f_\emptyset))$$

Proof.

Using

- Lemma 6.9
  - $(\Sigma \dashrightarrow \Sigma, \sqsubseteq)$ CCPO with least element $f_\emptyset$
  - LUB = union of graphs
- Lemma 6.16 (Φ continuous)
- Theorem 6.17 (Fixpoint Theorem)

□