

## 8. Einfache Fixpunkttheorie

Fragestellung:

- was unter einem (kleinsten) Fixpunkt zu verstehen ist

$$t(x) = x \quad \wedge \quad \forall y : D. t(y) = y \Rightarrow x \sqsubseteq y$$

- wann ein Fixpunkt existiert

monotone Funktionen über CPOs haben einen kleinsten Fixpunkt

- wie ein Fixpunkt charakterisiert werden kann

$$x_f = \sup\{f_i(\perp) \mid i \in \mathbb{N}\}$$

- welche Beweisprinzipien für Aussagen über Fixpunkte es gibt

$$(P(\perp) \wedge \forall i : \mathbb{N}. P(f^i(\perp))) \Rightarrow P(f^{i+1}(\perp)) \Rightarrow P(\mu(f))$$

# Grundlagen (1)

$D$  sei eine Menge mit Halbordnungsrelation  $\sqsubseteq$ ,  
 $A$  eine Teilmenge von  $D$ .

**Definition** obere Schranke  $ub(s, A)$

$s \in D$  heißt obere Schranke von  $A$  in  $D$ , wenn gilt  $\forall a \in A. a \sqsubseteq s$

**Definition** kleinste obere Schranke oder Supremum  $lub(s, A)$

$s \in D$  heißt kleinste obere Schranke von  $A$  in  $D$ , wenn gilt

$$ub(s, A) \wedge \forall u \in D. ub(u, A) \Rightarrow s \sqsubseteq u$$

Wenn eine kleinste obere Schranke von  $A$  existiert, ist sie eindeutig, und man kann schreiben  $\sup A$ .

## Grundlagen (2)

$D$  sei eine Menge mit Halbordnungsrelation  $\sqsubseteq$ ,  
 $A$  eine Teilmenge von  $D$ .

### **Definition** Kette

Eine Teilmenge  $K = \{a_i \mid i \in \mathbb{N}\}$  heißt Kette, wenn sie durch  $\sqsubseteq$  linear geordnet ist und eine aufsteigende Folge  $a_0 \sqsubseteq a_1 \sqsubseteq \dots \sqsubseteq a_i \sqsubseteq a_{i+1} \sqsubseteq \dots$  bildet.

### **Definition** kettenvollständig

$D$  heißt kettenvollständig, wenn jede Kette  $K$  in  $D$  ein Supremum  $\sup K$  in  $D$  hat.

## Grundlagen (3)

$D$  sei eine Menge mit Halbordnungsrelation  $\sqsubseteq$ ,  
 $A$  eine Teilmenge von  $D$ .

**Definition** complete partial order, CPO

$D$  ist ein CPO, wenn  $D$  ein kleinstes Element  $\perp$  besitzt und kettenvollständig bezüglich  $\sqsubseteq$  ist.

Jede Menge  $D$  kann zu einem primitiven CPO gemacht werden:

- *Lifting* von  $D$ :  $D_{\perp} := M \cup \{\perp\}$
- Definition einer *flachen* Ordnungsrelation  $\sqsubseteq$ :  
 $\forall x, y : D. x \sqsubseteq y \Leftrightarrow (x = \perp \vee x = y)$

Motivation: partielle Funktionen mit explizitem Wert für „undefiniert“.

## Grundlagen (4)

Seien  $D$  und  $E$  CPOs mit Relation  $\sqsubseteq$

**Definition** monotone Funktion

$f : D \rightarrow E$  heißt monoton, wenn sie die Ordnung respektiert, d. h. wenn gilt  
$$x \sqsubseteq y \Rightarrow f(x) \sqsubseteq f(y)$$

**Definition** stetige Funktion

$f : D \rightarrow E$  heißt stetig, wenn sie Suprema respektiert, d. h. wenn für jede Kette  $K$  in  $D$  gilt

$$f(\sup K) = \sup\{f(a) \mid a \in K\}$$

Im folgenden werden alle Definitions- und Wertebereiche von Funktionen als CPOs vorausgesetzt.

# Eigenschaften (1)

## Eigenschaften stetiger Funktionen

1. Eine stetige Funktion  $f : D \rightarrow E$  ist auch monoton.
2. Die Identitätsfunktion und die konstanten Funktionen sind stetig.

Induzierte „punktweise“ Ordnung auf Funktionen zwischen CPOs:

$$f \sqsubseteq g \Leftrightarrow \forall x. f(x) \sqsubseteq g(x)$$

Interpretation von  $f \sqsubseteq g$ :

$f$  ist weniger definiert (oder gleich)  $g$

## Eigenschaften (2)

**Theorem:** Stetige Funktionen bilden CPO

Seien  $D$  und  $E$  CPOs. Die Menge der Funktionen von  $D$  nach  $E$  bilden mit der punktweisen Ordnung  $\sqsubseteq$  auf Funktionen und der Funktion  $\perp_f := \{x \in D \mapsto \perp_E\}$  als Minimum ein CPO.

Beweis:

- Kettenvollständigkeit:

Jede Kette  $f_0 \sqsubseteq f_1 \sqsubseteq \dots \sqsubseteq f_i \sqsubseteq f_{i+1} \sqsubseteq \dots$  von Funktionen hat ein Supremum  $f_{\text{sup}}(x) := \sup\{f_i(x) \mid i \in \mathbb{N}\}$

- Supremum  $f_{\text{sup}}$  ist eine stetige Funktion

# Beispiel

Anwendung: Supremum einer Kette partieller Funktionen

$$f_0(x) = \perp \text{ für alle } x \in \mathbb{N}$$

$$f_1(x) = \mathbf{if } x = 0 \mathbf{ then } 1 \mathbf{ else } \perp$$

$$f_2(x) = \mathbf{if } x = 0 \mathbf{ then } 1 \mathbf{ else if } x = 1 \mathbf{ then } 1 \mathbf{ else } \perp$$

...

$$f_{i+1}(x) = \mathbf{if } x = 0 \mathbf{ then } 1 \mathbf{ else } x \cdot f_i(x - 1)$$

## Beispiel (2)

Bildungsgesetz:

- Funktional  $\tau : [\mathbb{N} \rightarrow \mathbb{N}] \rightarrow [\mathbb{N} \rightarrow \mathbb{N}]$   
$$\tau(f)(x) = [\text{if } x = 0 \text{ then } 1 \text{ else } x \cdot f(x - 1)]$$
- $t^0(f)(x) := x$  und  $t^{n+1}(f)(x) := \tau(\tau^n(x))$
- Somit:  $f_{i+1}(x) = \tau(f_i)(x)$  bzw.  $f_i(x) = \tau^i(\perp)(x)$

Aus der Definition der Folge  $f_0 \sqsubseteq f_1 \sqsubseteq \dots \sqsubseteq f_i \sqsubseteq f_{i+1} \sqsubseteq \dots$  folgt:

$$f_{\text{sup}} := \sup\{f_i\} \text{ existiert.}$$

# Fixpunkt

- Was ist  $f_{\text{sup}} := \sup\{f_i\}$ ?

- Vergleich mit

$$fac(x) = \mathbf{if } x = 0 \mathbf{ then } 1 \mathbf{ else } x \cdot fac(x - 1)$$

- es gilt also:  $fac = \tau(fac)$

- $fac$  ist Fixpunkt von  $\tau$ , somit ist auch  $f_{\text{sup}} \sqsubseteq fac$

- $f_i$  ist „i-te Approximation“ von  $fac$ :

$$f_i(x) = \begin{cases} fac(x) & \text{für } x < i \\ \perp & \text{sonst} \end{cases}$$

- Daher gilt:  $f_i \sqsubseteq fac$  für alle  $i \in \mathbb{N}$ , somit auch  $f_{\text{sup}} \sqsubseteq fac$

## Definition: Fixpunkt

Seien  $\langle D, \sqsubseteq, \perp \rangle$  ein CPO und  $\tau : D \rightarrow D$ .

### Definition Fixpunkt

$x \in D$  heißt Fixpunkt von  $t$ , wenn gilt:

$$t(x) = x$$

### Definition kleinster Fixpunkt

$x \in D$  heißt kleinster Fixpunkt von  $t$ , wenn  $x$  Fixpunkt von  $t$  ist und in jedem anderen Fixpunkt enthalten ist:

$$t(x) = x \wedge \forall y : D. t(y) = y \Rightarrow x \sqsubseteq y$$

# Fixpunktsatz

## Theorem: Fixpunktsatz

Sei  $\langle D, \sqsubseteq, \perp \rangle$  ein CPO.

Jede monotone Funktion  $f$  hat einen kleinsten Fixpunkt  $x_f$  in  $D$ .

Ist  $f$  zudem stetig, so gilt:  $x_f = \sup\{f^i(\perp) \mid i \in \mathbb{N}\}$

In PVS:

KnasterTarski: THEOREM

FORALL(f: Monotonic[D,D](<=,<=)): lfp\_exists?(<=)(f)

bottom\_iterations(<=)(f): set[D] =

seq\_to\_set(LAMBDA n: iterate(f, n)(bottom(<=)))

Kleene\_fixpoint\_theorem: THEOREM

FORALL (g:Continuous[D,D](<=,<=)):

lfp?(<=)(g)(lub[D](<=)(bottom\_iterations(<=)(g)))

# Fixpunktoperator

- Wenn ein kleinster Fixpunkt existiert, so ist er eindeutig
- Operator, der einer Funktion ihren kleinsten Fixpunkt zuordnet:

$$\mathbf{fix}_d : (D \rightarrow D) \rightarrow D \quad \mathbf{fix}_d(f) := \sup\{f^i(\perp)\}$$

- Meist wird der Fixpunkt mit  $\mu$  (bzw.  $\mu$ ) bezeichnet.

In PVS:

```
while(b,f) : PartialFunction =  
  mu! (x:PartialFunction):  
    IF b THEN f ++ x ELSE skip ENDIF
```

```
% while(b,f) : PartialFunction =  
%   mu(LAMBDA (x:PartialFunction):  
%     IF b THEN f ++ x ELSE skip ENDIF)
```

# Fixpunkt-Induktion

Idee: ähnlich der strukturellen Induktion über  $\mathbb{N}$

Aus

1.  $P(0)$

2.  $\forall n : \mathbb{N}. P(n) \Rightarrow P(n + 1)$

Schließe  $\forall n : \mathbb{N}. P(n)$

## Fixpunkt-Induktion (2)

Induktion über die endlichen Approximationen eines Fixpunkts: Aus

$$1. Q(\perp) \quad ( = Q(t^0(\perp)) )$$

$$2. \forall x : D. Q(x) \Rightarrow Q(t(x))$$

für stetige  $t$ :

$$\forall n : \mathbb{N}. Q(t^n(\perp)) \Rightarrow Q(t^{n+1}(\perp))$$

Schließe  $Q(\mu(t))$

für stetige  $t$ :  $Q(\sup\{t^i(\perp)\})$

# Zulässige Prädikate

Fixpunkt-Induktion ist nicht für alle Aussagen möglich:

## **Definition** zulässiges Prädikat

Ein Prädikat  $P$  ist zulässig für Fixpunkt-Induktion, wenn für jede aufsteigende Kette  $\{x_i \mid i \in \mathbb{N}\}$  gilt:

$$(\forall i \in \mathbb{N}. P(x_i)) \Rightarrow P(\sup\{x_i\})$$

Beispiel:

Die Aussage  $Q(f) := \exists x : \mathbb{N}. f(x) = \perp$  für das Fakultäts-Funktional  $\tau$  ist *nicht* zulässig:

- $Q(f_i)$  ist wahr für jedes  $f_i := \tau^i(\perp)$
- aber  $Q(\sup\{f_i\})$  ist falsch

## Fixpunkt-Induktion (2)

**Theorem:** Fixpunkt-Induktion, Scott-Induktion

Sei  $\langle D, \sqsubseteq, \perp \rangle$  ein CPO,  $f : D \rightarrow D$  eine monotone Funktion,  $P$  ein zulässiges Prädikat auf  $D$ .

Für den Beweis von  $P(\mu(f))$  genügt es zu zeigen:

1.  $P(\perp)$

2.  $\forall x : D. P(x) \Rightarrow P(f(x))$

# Fixpunkt-Induktion: Park's Lemma

**Theorem:** Park's Lemma, *recursion induction*

Sei  $\langle D, \sqsubseteq, \perp \rangle$  ein CPO,  $f : D \rightarrow D$  eine monotone Funktion.

Gilt die Fixpunkt-Ungleichung  $t(x) \sqsubseteq x$  für beliebige  $x \in D$ , so gilt auch

$$\mu(t) \sqsubseteq x$$