# Mathematische Grundlagen

Ziele...

- *Zunächst*: Definition der denotationellen Semantik von **WHILE** im Detail
- *Weitergehend*: Definition von abstrakten Semantiken für Programmanalysen

Wichtig insbesondere...

- Mengen, Relationen, Verbände
- Partielle und vollständige partielle Ordnungen
- Schranken, Fixpunkte und Fixpunkttheoreme

# Mengen und Relationen 1(2)

Sei $M$ eine Menge und $R$ eine Relation auf $M$, d.h. $R \subseteq M \times M$.

Dann heißt $R$...

- *reflexiv* gdw. $\forall\, m \in M.\ m\, R\, m$
- *transitiv* gdw. $\forall\, m, n, p \in M.\ m\, R\, n\ \wedge\ n\, R\, p\ \Rightarrow\ m\, R\, p$
- *antisymmetrisch* gdw. $\forall\, m, n \in M.\ m\, R\, n \wedge n\, R\, m\ \Rightarrow\ m = n$

Darüberhinaus... (in der Folge allerdings weniger wichtig)

- *symmetrisch* gdw. $\forall\, m, n \in M.\ m\, R\, n\ \Longleftrightarrow\ n\, R\, m$
- *total* gdw. $\forall\, m, n \in M.\ m\, R\, n\ \vee\ n\, R\, m$

# Mengen und Relationen 2(2)

Eine Relation $R$ auf $M$ heißt

- *Quasiordnung* gdw. $R$ ist reflexiv und transitiv
- *partielle Ordnung* gdw. $R$ ist reflexiv, transitiv und antisymmetrisch

Zur Vollständigkeit sei ergänzt...

- *Äquivalenzrelation* gdw. $R$ ist reflexiv, transitiv und symmetrisch

...eine partielle Ordnung ist also eine antisymmetrische Quasiordnung, eine Äquivalenzrelation eine symmetrische Quasiordnung.

# Schranken, kleinste, größte Elemente

Sei $(Q, \sqsubseteq)$ eine Quasiordnung, sei $q \in Q$ und $Q' \subseteq Q$.

Dann heißt $q$...

- *obere* (*untere*) *Schranke* von $Q'$, in Zeichen: $Q' \sqsubseteq q$ ($q \sqsubseteq Q'$), wenn für alle $q' \in Q$ gilt: $q' \sqsubseteq q$ ($q \sqsubseteq q'$)
- *kleinste obere* (*größte untere*) *Schranke* von $Q'$, wenn $q$ obere (untere) Schranke von $Q'$ ist und für jede andere obere (untere) Schranke $\widehat{q}$ von $Q'$ gilt: $q \sqsubseteq \widehat{q}$ ($\widehat{q} \sqsubseteq q$)
- *größtes* (*kleinstes*) Element von $Q$, wenn gilt: $Q \sqsubseteq q$ ($q \sqsubseteq Q$)

# Eindeutigkeit von Schranken

- In partiellen Ordnungen sind kleinste obere und größte untere Schranken eindeutig bestimmt, wenn sie existieren.

- Existenz (und damit Eindeutigkeit) vorausgesetzt, wird die kleinste obere (größte untere) Schranke einer Menge $P' \subseteq P$ der Grundmenge einer partiellen Ordnung $(P, \sqsubseteq)$ mit $\bigsqcup P'$ ($\bigsqcap P'$) bezeichnet. Man spricht dann auch vom *Supremum* und *Infimum* von $P'$.

- Analog für kleinste und größte Elemente. Existenz vorausgesetzt, werden sie üblicherweise mit $\bot$ und $\top$ bezeichnet.

# Verbände und vollständige Verbände

Sei $(P, \sqsubseteq)$ eine partielle Ordnung.

Dann heißt $(P, \sqsubseteq)$...

- *Verband*, wenn jede *endliche* Teilmenge $P'$ von $P$ eine kleinste obere und eine größte untere Schranke in $P$ besitzt
- *vollständiger Verband*, wenn *jede* Teilmenge $P'$ von $P$ eine kleinste obere und eine größte untere Schranke in $P$ besitzt

...(vollständige) Verbände sind also spezielle partielle Ordnungen.

# Vollständige partielle Ordnungen

...ein etwas schwächerer, aber in der Informatik oft ausreichender und daher angemessenerer Begriff.

Sei $(P, \sqsubseteq)$ eine partielle Ordnung.

Dann heißt $(P, \sqsubseteq)$...

- *vollständig*, kurz *CPO* (von engl. complete partial order), wenn jede aufsteigende Kette $K \subseteq P$ eine kleinste obere Schranke in $P$ besitzt.

Es gilt:

- Eine CPO $(C, \sqsubseteq)$ (genauer wäre: "kettenvollständige partielle Ordnung (engl. chain complete partial order (CCPO)") besitzt stets ein kleinstes Element, eindeutig bestimmt als Supremum der leeren Kette und üblicherweise mit $\bot$ bezeichnet: $\bot =_{df} \bigsqcup \emptyset$.

# Ketten

Sei $(P, \sqsubseteq)$ eine partielle Ordnung.

Eine Teilmenge $K \subseteq P$ heißt...

- *Kette* in $P$, wenn die Elemente in $K$ total geordnet sind. Für $K = \{k_0 \sqsubseteq k_1 \sqsubseteq k_2 \sqsubseteq \ldots\}$ ($\{k_0 \sqsupseteq k_1 \sqsupseteq k_2 \sqsupseteq \ldots\}$) spricht man auch genauer von einer *aufsteigenden* (*absteigenden*) Kette in $P$.

Eine Kette $K$ heißt...

- *endlich*, wenn $K$ endlich ist, sonst *unendlich*.

# Kettenendlichkeit, endliche Elemente

Eine partielle Ordnung $(P, \sqsubseteq)$ heißt

- *kettenendlich* gdw. $P$ enthält keine unendlichen Ketten

Ein Element $p \in P$ heißt

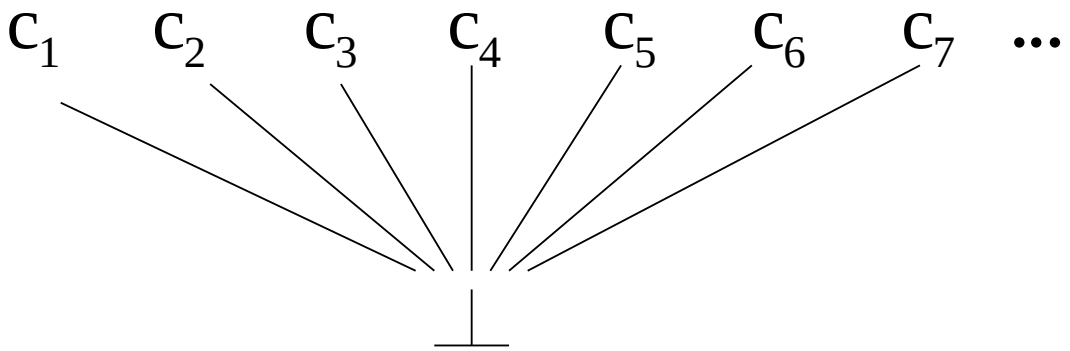
- *endlich* gdw. die Menge $Q =_{df} \{q \in P \mid q \sqsubseteq p\}$ keine unendliche Kette enthält
- *endlich relativ zu* $r \in P$ gdw. die Menge $Q =_{df} \{q \in P \mid r \sqsubseteq q \sqsubseteq p\}$ keine unendliche Kette enthält

# (Standard-) CPO-Konstruktionen 1(4)

*Flache CPOs*...

Sei $(C, \sqsubseteq)$ eine CPO. Dann heißt $(C, \sqsubseteq)$...

- *flach*, wenn für alle $c, d \in C$ gilt: $c \sqsubseteq d \Leftrightarrow c = \bot \ \vee \ c = d$



# (Standard-) CPO-Konstruktionen 2(4)

*Produktkonstruktionen...*

Seien $(P_1, \sqsubseteq_1), (P_2, \sqsubseteq_2), \ldots, (P_n, \sqsubseteq_n)$ CPOs. Dann sind auch...

- das *nichtstrikte* (*direkte*) *Produkt* $(\bigtimes P_i, \sqsubseteq)$ mit
  - $(\bigtimes P_i, \sqsubseteq) = (P_1 \times P_2 \times \ldots \times P_n, \sqsubseteq)$ mit $\forall\, (p_1, p_2, \ldots, p_n), (q_1, q_2, \ldots, q_n) \in \bigtimes P_i.\ (p_1, p_2, \ldots, p_n) \sqsubseteq (q_1, q_2, \ldots, q_n) \Rightarrow \forall\, i \in \{1, \ldots, n\}.\ p_i \sqsubseteq_i q_i$
- und das *strikte* (*direkte*) *Produkt* (*smash Produkt*) mit
  - $(\bigotimes P_i, \sqsubseteq) = (P_1 \otimes P_2 \otimes \ldots \otimes P_n, \sqsubseteq)$, wobei $\sqsubseteq$ wie oben definiert ist, jedoch zusätzlich gesetzt wird:

$$(p_1, p_2, \ldots, p_n) = \bot \Rightarrow \exists\, i \in \{1, \ldots, n\}.\ p_i = \bot_i$$

  CPOs.

# (Standard-) CPO-Konstruktionen 3(4)

*Summenkonstruktion...*

Seien $(P_1, \sqsubseteq_1), (P_2, \sqsubseteq_2), \ldots, (P_n, \sqsubseteq_n)$ CPOs. Dann ist auch...

- die *direkte Summe* $(\bigoplus P_i, \sqsubseteq)$ mit...
  - $(\bigoplus P_i, \sqsubseteq) = (P_1 \dot\cup P_2 \dot\cup \ldots \dot\cup P_n, \sqsubseteq)$ disjunkte Vereinigung der $P_i$, $i \in \{1, \ldots, n\}$ und $\forall p, q \in \bigoplus P_i.\ p \sqsubseteq q \Rightarrow \exists i \in \{1, \ldots, n\}.\ p, q \in P_i \wedge p \sqsubseteq_i q$ und der Identifikation der kleinsten Elemente der $(P_i, \sqsubseteq_i)$, $i \in \{1, \ldots, n\}$, d.h. $\bot =_{df} \bot_i$, $i \in \{1, \ldots, n\}$

  eine CPO.

# (Standard-) CPO-Konstruktionen 4(4)

*Funktionenraum*...

Seien $(C, \sqsubseteq_C)$ und $(D, \sqsubseteq_D)$ zwei CPOs und $[C \to D] =_{df}$ $\{f : C \to D \mid f \text{ stetig}\}$ die Menge der stetigen Funktionen von $C$ nach $D$.

Dann ist auch...

- der *stetige Funktionenraum* $([C \to D], \sqsubseteq)$ eine CPO mit
  - $\forall\, f, g \in [C \to D].\ f \sqsubseteq g \Longleftrightarrow \forall\, c \in C.\ f(c) \sqsubseteq_D g(c)$

# Funktionen auf CPOs / Eigenschaften

Seien $(C, \sqsubseteq_C)$ und $(D, \sqsubseteq_D)$ zwei CPOs und sei $f : C \to D$ eine Funktion von $C$ nach $D$.

Dann heißt $f$...

- *monoton* gdw. $\forall\, c, c' \in C.\ c \sqsubseteq_C c' \Rightarrow f(c) \sqsubseteq_D f(c')$
  (*Erhalt der Ordnung der Elemente*)

- *stetig* gdw. $\forall\, C' \subseteq C.\ f(\bigsqcup_C C') =_D \bigsqcup_D f(C')$
  (*Erhalt der kleinsten oberen Schranken*)

Sei $(C, \sqsubseteq)$ eine CPO und sei $f : C \to C$ eine Funktion auf $C$.

Dann heißt $f$...

- *inflationär* (*vergrößernd*) gdw. $\forall\, c \in C.\ c \sqsubseteq f(c)$

# Funktionen auf CPOs / Resultate

Mit den vorigen Bezeichnungen gilt...

**Lemma**

$f$ ist monoton gdw. $\forall\, C' \subseteq C.\ f(\bigsqcup_C C') \sqsupseteq_D \bigsqcup_D f(C')$

**Korollar**

Eine stetige Funktion ist stets monoton, d.h. $f$ stetig $\Rightarrow$ $f$ monoton.

# (Kleinste und größte) Fixpunkte 1(2)

Sei $(C, \sqsubseteq)$ eine CPO, $f : C \to C$ eine Funktion auf $C$ und sei $c$ ein Element von $C$, also $c \in C$.

Dann heißt $c$ ...

- *Fixpunkt* von $f$ gdw. $f(c) = c$

Ein Fixpunkt $c$ von $f$ heißt...

- *kleinster Fixpunkt* von $f$ gdw. $\forall\, d \in C.\ f(d) = d \Rightarrow c \sqsubseteq d$
- *größter Fixpunkt* von $f$ gdw. $\forall\, d \in C.\ f(d) = d \Rightarrow d \sqsubseteq c$

# (Kleinste und größte) Fixpunkte 2(2)

Seien $d, c_d \in C$. Dann heißt $c_d$ ...

- *bedingter kleinster Fixpunkt* von $f$ bezüglich $d$ gdw. $c_d$ ist der kleinste Fixpunkt von $C$ mit $d \sqsubseteq c_d$, d.h. für alle anderen Fixpunkte $x$ von $f$ mit $d \sqsubseteq x$ gilt: $c_d \sqsubseteq x$.

*Bezeichnungen*:
Der kleinste bzw. größte Fixpunkt einer Funktion $f$ wird oft mit $\mu f$ bzw. $\nu f$ bezeichnet.

# Fixpunktsatz

**Theorem** (Knaster/Tarski, Kleene)
Sei $(C, \sqsubseteq)$ eine CPO und sei $f : C \to C$ eine stetige Funktion auf $C$.

Dann hat $f$ einen kleinsten Fixpunkt $\mu f$ und dieser Fixpunkt ergibt sich als kleinste obere Schranke der Kette (sog. *Kleene*-Kette) $\{\bot, f(\bot), f^2(\bot), \ldots\}$, d.h.

$$\mu f = \bigsqcup_{i \in \mathbb{N}_0} f^i(\bot) = \bigsqcup \{\bot, f(\bot), f^2(\bot), \ldots\}$$