# **IMP/ASSN**: Hoare-Tripel für totale Korrektheit

Totale Korrektheitsaussage $[A]\,S\,[A']$ mit $A, A' \in \mathrm{Frm}$, $S \in \mathrm{Stm}$

Gültigkeitsrelation $I \in \mathit{Val}$, $\sigma \in \Sigma$, $A, A' \in \mathrm{Frm}$

$$I, \sigma \models [A]\,S\,[A'] \iff (I, \sigma \models A \Rightarrow \mathcal{S}[\![S]\!]\,\sigma \neq \bot \wedge I, \mathcal{S}[\![S]\!]\,\sigma \models_{\perp\!\!\!\perp} A')$$

- $I \models [A]\,S\,[A'] \iff \forall \sigma \in \Sigma\,.\, I, \sigma \models [A]\,S\,[A']$
- $\models \{A\}\,S\,\{A'\} \iff \forall I \in \mathit{Val},\ \sigma \in \Sigma\,.\, I, \sigma \models [A]\,S\,[A']$

Ableitbarkeitsrelation

- $\vdash$ gemäß Hoare-Kalkül für totale Korrektheit

# **IMP/ASSN**: Hoare-Kalkül für totale Korrektheit

Analog zu partieller Korrektheit

(while$_{\text{ht}}$) $$\frac{[A \wedge b \wedge X = t]\, S\, [A \wedge \neg(X \leq t)]}{[A]\, \texttt{while}\ b\ \texttt{do}\ S\, [A \wedge \neg b]}, \quad \text{falls } \models A \wedge b \Rightarrow 0 \leq t$$

wobei $X \notin \mathrm{flog}(A) \cup \mathrm{flog}(t)$

# **IMP/ASSN**: Bereichstheoretische Charakterisierung

Semantische Funktion $\mathcal{F}[\![-]\!] : \mathrm{Frm} \to (\mathit{Val} \to \Sigma \to \mathbb{B})$

$$\mathcal{F}[\![A]\!]\, I\, \sigma = \begin{cases} \mathit{tt}, & \text{falls } I, \sigma \models A \\ \mathit{ff}, & \text{falls } I, \sigma \not\models A \end{cases}$$

$p_{\mathrm{f}}, p_{\mathrm{t}} : \mathbb{B} \to \{\top\}_\perp$

$$p_{\mathrm{f}}\, x = \begin{cases} \perp, & \text{falls } x = \mathit{tt} \\ \top, & \text{falls } x = \mathit{ff} \end{cases} \qquad p_{\mathrm{t}}\, x = \begin{cases} \top, & \text{falls } x = \mathit{tt} \\ \perp, & \text{falls } x = \mathit{ff} \end{cases}$$

$$I \models \{A\}\, S\, \{A'\} \iff (p_{\mathrm{f}} \circ \mathcal{F}[\![A']\!]\, I)_{\perp\!\!\perp} \circ \mathcal{S}[\![S]\!] \sqsubseteq p_{\mathrm{f}} \circ \mathcal{F}[\![A]\!]\, I$$

$$I \models [A]\, S\, [A'] \iff p_{\mathrm{t}} \circ \mathcal{F}[\![A]\!]\, I \sqsubseteq (p_{\mathrm{t}} \circ \mathcal{F}[\![A']\!]\, I)_{\perp\!\!\perp} \circ \mathcal{S}[\![S]\!]$$

# Scott-Topologie

**Definition** Sei $P$ ein Präbereich. Eine Menge $X \subseteq P$ heißt **Scott-offen** (in $P$), falls mit $x \in X$ auch $y \in X$ für $x \sqsubseteq_P y$; und falls $\bigsqcup_P Y \in X$ für eine $\omega$-Kette $Y \subseteq P$, so $X \cap Y \neq \emptyset$.

**Satz** Sei $(P, \sqsubseteq)$ ein Präbereich und sei $\mathcal{O}_P$ die Menge der Scott-offenen Mengen von $P$. Dann ist $\mathcal{O}_P$ eine Topologie über $P$.

**Definition** Die Menge $\mathcal{O}_P$ der Scott-offenen Mengen von $P$ heißt **Scott-Topologie** von $P$.

# Sicherheitseigenschaften

**Definition** Sei $P$ ein Präbereich. Eine Menge $X \subseteq P$ heißt eine **Sicherheitseigenschaft** (von $P$), falls mit $x \in X$ auch $y \in X$ für $y \sqsubseteq_P x$; und, falls $Y \subseteq X$ eine $\omega$-Kette ist, auch $\bigsqcup_P Y \in X$ ist.

**Satz** Sei $(P, \sqsubseteq)$ ein Präbereich. Eine Menge $X \subseteq P$ ist genau dann eine Sicherheitseigenschaft, falls $X$ eine abgeschlossene Menge bzgl. der Scott-Topologie $\mathcal{O}_P$ von $P$ ist.

# Algebraische Bereiche

**Definition** Sei $P$ ein Präbereich. Ein Element $p \in P$ heißt endlich, falls für jede $\omega$-Kette $(p_n)_{n\in\mathbb{N}}$ in $P$ gilt: Ist $p \sqsubseteq_P \bigsqcup_P \{p_n \mid n \in \mathbb{N}\}$, dann gibt es ein $n \in \mathbb{N}$, sodaß $p \sqsubseteq_P p_n$. Die Menge der endlichen Elemente von $P$ wird mit $\mathscr{K}(P)$ bezeichnet.

**Definition** Ein Präbereich $P$ heißt algebraisch, falls für jedes Element $p \in P$ gilt: Es gibt eine $\omega$-Kette $(e_n)_{n\in\mathbb{N}}$ in $\mathscr{K}(P)$, sodaß $p = \bigsqcup_P \{e_n \mid n \in \mathbb{N}\}$.

# **IMP/ASSN**: Sicherheitseigenschaften

Lemma Seien $A, A' \in \mathrm{Frm}$ und $I \in \mathit{Val}$. Seien $f = p_{\mathrm{f}} \circ \mathcal{F}[\![A']\!]\, I$ und $g = p_{\mathrm{f}} \circ \mathcal{F}[\![A]\!]\, I$. Dann ist

$$Z = \{h \in [\Sigma \to \Sigma_\perp] \mid f_{\perp\!\!\perp} \circ h \sqsubseteq_{[\Sigma \to \Sigma_\perp]} g\}$$

eine Sicherheitseigenschaft von $[\Sigma \to \Sigma_\perp]$.

$Z$ algebraischer Präbereich, falls $\Sigma$ abzählbar

- endliche Elemente $h$ $\quad |\{\sigma \in \Sigma \mid h\,\sigma \neq \perp\}| < \infty$

# Scott-Abschluß

**Definition** Sei $P$ ein algebraischer Präbereich. Der **Scott-Abschluß** einer Menge $X \subseteq P$ ist gegeben durch die Menge $\overline{X} = \{p \in P \mid \forall e \in \mathscr{K}(P) \,.\, e \sqsubseteq_P p \Rightarrow \exists x \in X \,.\, e \sqsubseteq_P x\}$.

**Lemma** Sei $P$ ein algebraischer Präbereich und $X \subseteq P$. Dann ist der Scott-Abschluß $\overline{X}$ der Abschluß von $X$ bzgl. der Scott-Topologie $\mathscr{O}_P$ von $P$.

# Lebendigkeitseigenschaften

**Definition** Sei $P$ ein algebraischer Präbereich. Eine Menge $X \subseteq P$ heißt Lebendigkeitseigenschaft (von $P$), falls für alle $e \in \mathscr{K}(P)$ ein $x \in X$ existiert mit $e \sqsubseteq_P x$.

**Satz** Sei $P$ ein algebraischer Präbereich. Eine Menge $X \subseteq P$ ist genau dann eine Lebendigkeitseigenschaft, falls $X$ eine dichte Menge bzgl. der Scott-Topologie $\mathscr{O}_P$ von $P$ ist.

# **IMP/ASSN**: Lebendigkeitseigenschaften

$(A, A') \in \mathrm{Frm} \times \mathrm{Frm}$ total erfüllbar für $I \in \mathit{Val}$

- $\forall \sigma \in \Sigma\,.\ \mathcal{F}[\![A]\!]\, I\, \sigma = \mathit{ff} \quad \vee \quad \exists \sigma' \in \Sigma\,.\ \mathcal{F}[\![A']\!]\, I\, \sigma' \neq \mathit{ff}$

Lemma Seien $A, A' \in \mathrm{Frm}$ und $I \in \mathit{Val}$ und sei $(A, A')$ total erfüllbar für $I$. Seien $f = p_{\mathrm{f}} \circ \mathcal{F}[\![A']\!]\, I$, $F = p_{\mathrm{t}} \circ \mathcal{F}[\![A]\!]\, I$, $g = p_{\mathrm{f}} \circ \mathcal{F}[\![A]\!]\, I$ und $G = p_{\mathrm{t}} \circ \mathcal{F}[\![A']\!]\, I$. Dann ist

$$L = \{h \in [\Sigma \to \Sigma_\perp] \mid F \sqsubseteq_{[\Sigma \to \Sigma_\perp]} G_{\perp\!\!\perp} \circ h\}$$

eine Lebendigkeitseigenschaft des Präbereichs $Z = \{h \in [\Sigma \to \Sigma_\perp] \mid f_{\perp\!\!\perp} \circ h \sqsubseteq_{[\Sigma \to \Sigma_\perp]} g\}$.