Auch Separation-Logik-Assertions erfüllen
das Substitutionslemma der Prädikatenlogik.

Lemma (Substitutionslemma, Weakest Pre)

$$[\![A[x/a]]\!]\, s\, h = [\![A]\!]\, s[x/[\![a]\!]s]\, h$$

Ersetze die Belegung von x, falls existent,
sonst füge sie hinzu.

5.3 Inferenz

Ziel: Gib ein Beweissystem (Axiome und Beweisregeln)
für Assertions an.
Beweisregeln haben die Form

$$\frac{A_1 \qquad A_n}{A}$$

Wie in der Logik üblich handelt es sich um Regelschemata,
die mit konkreten Assertions instantiiert werden müssen.

Definition:
Ein Regelschema heißt gültig (oder sound),
falls für alle Instantiierungen gilt:
sofern die Prämissen (alle) allgemeingültig sind,
ist auch die Konklusion allgemeingültig.

Bemerkung:
(1) $\frac{A}{B}$ und (2) $\overline{A \to B}$ sind nicht äquivalent.
Bei (1) gilt: sofern A auf allen Zuständen gilt,
gilt auch B auf allen Zuständen.

Bei (2) gilt: Für jeden Zustand, auf dem A gilt, muss auch B gelten.

Illustration:

Folgende Generalisierungsregel

$$\frac{A}{\forall x. A}$$

ist gültig.

- Betrachte die Instanz

$$\frac{x+y = y+x}{\forall x.\ x+y = y+x}.$$

Sie gilt, da die Konklusion allgemeingültig ist.

- Betrachte die Instanz

$$\frac{x=0}{\forall x.\ x=0}.$$

Sie gilt, da die Prämisse nicht allgemeingültig ist.

- Die Implikation

$$x=0 \to \forall x.\ x=0$$

hingegen ist nicht allgemeingültig, und daher das entsprechende Axiom nicht gültig.

Im Folgenden werden Axiome ohne $\forall$ geschrieben.

Satz (Kleene '52, Reynolds)

Folgendes Beweissystem ist sound und complete für Prädikatenlogik und auch gültig für Separation-Logik-Assertions:

- $A \to (B \to A)$
- $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
- $A \wedge B \to A$
- $A \wedge B \to B$
- $A \to (B \to (A \wedge B))$
- $\neg\neg A \to A$

- $A \to A \vee B$
- $B \to A \vee B$
- $(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$
- $(A \to B) \to ((A \to \neg B) \to \neg A)$
- $(A \leftrightarrow B) \to ((A \to B) \wedge (B \to A))$
- $((A \to B) \wedge (B \to A)) \to (A \leftrightarrow B)$

- $\forall x. A \to A[x/a]$
- $A[x/a] \to \exists x. A$

(Modus Ponens) $\dfrac{A \qquad A \to B}{B}$

$\dfrac{A \to B}{A \to \forall x. B}$, falls $x \notin fv(A)$

$\dfrac{A \to B}{(\exists x. A) \to B}$, falls $x \notin fv(B)$

Wir sind eher an Axiomen und Beweisregeln interessiert, die sich auf die neuen Operatoren beziehen.

Lemma:

Folgende Axiome sind gültig: (Assoc, $*$, emp) bilden ein kommutatives Monoid.

(1) $A * B \leftrightarrow B * A$

$A * (B * C) \leftrightarrow (A * B) * C$

$A * emp \leftrightarrow A$

(2) $(A \vee B) * C \leftrightarrow (A * C) \vee (B * C)$ (Distributivität)

$(A \wedge B) * C \to (A * C) \wedge (B * C)$

(3) $(\exists x. A) * B \leftrightarrow \exists x. (A * B)$, $x \notin fv(B)$ (Scope-Erweiterung)

$(\forall x. A) * B \to \forall x. (A * B)$, $x \notin fv(B)$

Lemma:

Folgende Beweisregeln sind gültig.

(1) $$\frac{A \to B \qquad C \to D}{A * C \to B * D}$$ (Monotonie)

(2) $$\frac{A * B \to C}{A \to (B \multimap C)}$$ (Deduktionstheorem / Currying)

(3) $$\frac{A \to (B \multimap C)}{A * B \to C}$$ (Deduktionstheorem / Decurrying).

Korollar:

Folgende Axiome und Regeln sind gültig:

(1) $A * (A \multimap B) \to B$ (Modus Ponens)

(2) $$\frac{A' \to A \qquad B \to B'}{(A \multimap B) \to (A' \multimap B')}$$ (Strengthening / Weakening bei $\multimap$)

(3) $B \to (A \multimap (A * B))$

(4) $(A * B) \to A * (C \multimap (C * B))$

(5) $$\frac{A_0 \to (B \multimap C) \qquad A_1 \to (C \multimap D)}{A_0 * A_1 \to (B \multimap D)}$$ (Transitivität von $\multimap$)

Beweis:

Um das Korollar abzuleiten führen wir formale Beweise (Kalkülbeweise).

Betrachte nur Axiom (1):

(1) $\underbrace{A * (A \mathrel{-\!\!*} B)}_{X} \leftrightarrow \underbrace{(A \mathrel{-\!\!*} B) * A}_{Y}$ // Kommutativität

(2) $(X \leftrightarrow Y) \to [(X \to Y) \wedge (Y \to X)]$ // Äquivalenz

(3) $(X \to Y) \wedge (Y \to X)$ // Modus Ponens (1) + (2)

(4) $[(X \to Y) \wedge (Y \to X)] \to (X \to Y)$ // Konjunktion

(5) $[A * (A \mathrel{-\!\!*} B)] \to [(A \mathrel{-\!\!*} B) * A]$ // Modus Ponens (3) + (4)

(6) $(A \mathrel{-\!\!*} B) \to (A \mathrel{-\!\!*} B)$ // $A \to A$, kann man herleiten

(7) $[(A \mathrel{-\!\!*} B) * A] \to B$ // Decurrying (6)

(8) $A * (A \mathrel{-\!\!*} B) \to B$ // Transitivität → (5) + (7) kann man herleiten. □

Bemerkung:

$A \to A * A$ und $A * B \to A$ gelten nicht.

Betrachte als Instanzen $A \equiv x \mapsto 1$ und $B \equiv y \mapsto 2$.

Dann gilt A auf (manchen) Heaps mit einer Zelle,

aber $A * A$ ist unerfüllbar.

Analog gilt $A * B$ auf geeigneten Heaps mit zwei Zellen,

während A auf keinem Heap mit zwei Zellen gilt.

Wir betrachten weitere Axiome für points-to.

Die Axiomenmenge ist nicht vollständig.

Lemma: Folgende Axiome sind gültig.

- $a_0 \mapsto a_0' \wedge a_1 \mapsto a_1' \leftrightarrow a_0 \mapsto a_0' \wedge a_0 = a_1 \wedge a_0' = a_1'$

- $a_0 \hookrightarrow a_0' * a_1 \hookrightarrow a_1' \rightarrow a_0 \neq a_1$
- $emp \leftrightarrow \forall x. \neg(x \hookrightarrow \_)$
- $(a \hookrightarrow a') \wedge A \rightarrow (a \mapsto a') * [(a \mapsto a') \mathrel{-\!\!*} A]$

5.4 Teilklassen von Assertions

Ziel: Teilklassen von Assertions erlauben zweckmäßige Beweisregeln.

Ansatz: Definiere Teilklassen semantisch. Finde hinreichende syntaktische Bedingungen.

5.4.1 Pure Assertions

Idee: Assertions, die unabhängig vom Heap sind.

Definition:
Assertion A ist pure, falls

$$\forall s, h, h'. \quad [\![A]\!]\, s\, h = [\![A]\!]\, s\, h'.$$

Lemma:
Falls A weder emp noch $\mapsto$ enthält, ist A pure.

Falls Assertions pure sind, wird aus $*$ normales $\wedge$ und aus $\mathrel{-\!\!*}$ normales $\rightarrow$.

Genauer:

Lemma:
Folgende Axiome gelten:

(1) $A \wedge B \rightarrow A * B$, falls A oder B pure

(2) $A * B \rightarrow A \wedge B$, falls A und B pure

(3) $(A \wedge B) * C \iff (A * C) \wedge B$, falls B pure

// Wichtig

(4) $(A \mathrel{-\!\!*} B) \to (A \to B)$, falls A pure

(5) $(A \to B) \to (A \mathrel{-\!\!*} B)$, falls A und B pure.

5.4.2 Precise Assertions

Idee: Wenn eine Assertion auf einem Teilheap gilt, dann ist dieser Teilheap eindeutig bestimmt.

Definition:
Assertion A ist precise, falls

$$\forall s, h.\ \exists \text{ at most one } h' \subseteq h.\ [\![A]\!]_{s h'} = 1.$$

Lemma:
Folgende Grammatik liefert precise Assertions:

$$\begin{aligned} A ::= {} & emp \mid a_1 \mapsto a_2 \mid A * B \\ & \mid A \wedge B, \text{ falls } A \text{ oder } B \text{ precise} \\ & \mid A, \text{ falls } A \to B \text{ gültig und } B \text{ precise.} \end{aligned}$$

Beispiel:
Folgende Assertions sind nicht precise:

true $emp \vee x \mapsto 10$ $x \mapsto 10 \vee y \mapsto 10$ $\exists x.\ x \mapsto 10$

Precisenen gibt uns die fehlenden Distributivitäten:

Lemma: Folgende Axiome gelten.

(1) $(A * C) \wedge (B * C) \to (A \wedge B) * C$, falls C precise.

(2) $\forall x.\ (A * B) \to (\forall x.\ A) * B$, falls $x \notin fv(B)$ und B precise.

5.4.3 Intuitionistische Assertions

Ziel: Man möchte Assertions A in $A * B$ droppen.

Aktuelle Separation-Logiken, insbesondere IRIS, arbeiten nur mit intuitionistischen Assertions.

Idee: Fordere Monotonie bzgl. Heap-Erweiterung.

Definition:

Eine Assertion I heißt intuitionistisch, falls

$$\forall s, h, h' : \quad [\![I]\!]\, s\, h = 1 \;\wedge\; h \subseteq h' \;\Rightarrow\; [\![I]\!]\, s\, h' = 1.$$

Lemma:

Folgende Grammatik liefert intuitionistische Assertions (mit A eine beliebige Assertion):

$$\begin{aligned} I ::= {} & \text{jede pure Assertion} \mid a_1 \mapsto a_2 \\ & \mid A * I \mid I_1 \wedge I_2 \mid I_1 \vee I_2 \\ & \mid A \mathrel{-\!\!*} I \mid I \mathrel{-\!\!*} A \mid \forall x.\, I \mid \exists x.\, I. \end{aligned}$$

Beispiele:

$A * \mathrm{true}$, $\mathrm{true} \mathrel{-\!\!*} A$ sind intuitionistisch, da true pure ist.

Lemma:

Folgende Axiome und Regeln gelten:

(1) $I_1 * I_2 \;\to\; I_1 \wedge I_2$

(2) $I * A \;\to\; I$

(3) $I \;\to\; (A \mathrel{-\!\!*} I)$

(4) $$\frac{A \to I}{(A * \mathrm{true}) \to I}$$

(5) $$\frac{I \to A}{I \to (\mathrm{true} \mathrel{-\!\!*} A)}$$

Lemma:

Für jede Aussage A ist

(i) $A * \text{true}$ die stärkste intuitionistische Aussage schwächer als A

(ii) $\text{true} \twoheadrightarrow A$ ist die schwächste intuitionistische Aussage stärker als A.

Beweis:

Zeige (i). Sei dazu I eine intuitionistische Aussage schwächer als A, also $A \to I$.

Dann folgt mit (4) aus obigem Lemma

$$(A * \text{true}) \to I.$$ □

Bemerkung:

Man kann auch rein intuitionistische SL-Aussagen definieren:

$A ::=$ pure Aussagen $\mid a_1 \hookrightarrow a_2$

$\mid A_1 \wedge A_2 \mid A_1 \vee A_2 \mid \exists x.\, A \mid \forall x.\, A$

$\mid A_1 * A_2 \mid A_1 \twoheadrightarrow A_2$

$\mid \dot{\neg} A \mid A_1 \dot{\to} A_2 \mid A_1 \dot{\leftrightarrow} A_2$.

Anstatt die Semantik der intuitionistischen Junktoren anzugeben, zeigen wir gleich eine Übersetzung in gewöhnliche SL-Aussagen:

$\dot{\neg} A \rightsquigarrow \text{true} \twoheadrightarrow (\neg A)$ Ishtiaq & O'Hearn '01.

$A_1 \dot{\to} A_2 \rightsquigarrow \text{true} \twoheadrightarrow (A_1 \to A_2)$

$A_1 \dot{\leftrightarrow} A_2 \rightsquigarrow \text{true} \twoheadrightarrow (A_1 \leftrightarrow A_2)$

Egal, welchen Heap man hinzufügt, die Negation / Implikation / Äquivalenz gilt.

Die Modelle sind also upward-closed bzgl. Heap-Erweiterung.