5.5 Induktive Prädikate

Ziel: Als wir zu Beginn des Kapitels über Listen gesprochen haben, hatten wir Prädikate

$$\text{list } \Sigma \,, \quad \text{list } a.\alpha \,, \quad \text{readable } n.$$

Diese Prädikate haben wir noch nicht definiert.

Ansatz:
- Definiere induktiv eine Menge abstrakter Terme t (die Listen, Bäume oder Zahlen repräsentieren werden).
- Definiere Prädikate pred t, die von diesen Termen abhängen.
- Mache dazu Induktion über die Struktur der Terme.

Definition:

Sei (Σ, rk) ein ranked Alphabet, also eine endliche Menge an Buchstaben Σ, die mit Stelligkeiten $rk: \Sigma \to \mathbb{N}$ ausgestattet wird.

Die Menge Σ-Term ist induktiv definiert:

$$t ::= f(t_1, \ldots, t_n), \quad \text{wobei } n = rk(f).$$

Beachte, dass Buchstaben a mit $rk(a) = 0$ den Basisfall bilden.

Definition:

- Ein induktives Prädikat mit Bezeichner pred, Stelligkeit n und gebildet über Σ-Term ist gegeben als die Menge an Prädikatssymbolen

$$(\text{pred } t)/n$$

mit $t \in \Sigma$-Term.

• Wir erweitern die Syntax von Separation-Logik-Assertions:

$$A ::= \underbrace{\ldots}_{\text{wie bisher}} \mid [\mathrm{pred}\ t](\tilde{a}) \mid t_1 = t_2$$

mit $\tilde{a} = a_1, \ldots, a_n$.

• Ein induktives Prädikat kommt mit einer Menge an <u>definierenden Gleichungen</u>

$$[\mathrm{pred}\ f(t_1, \ldots, t_n)](\tilde{x}) := A,$$

wobei A höchstens die Prädikatssymbole $\mathrm{pred}\ t_i$ verwendet und auf die Variablen $\tilde{x} = x_1, \ldots, x_n$ Bezug nehmen darf.
Es gibt eine definierende Gleichung für jeden Buchstaben in Σ.

• Die Semantik der neuen Assertion ist

$$[\![[\mathrm{pred}\ t](\tilde{a})]\!]\, s\, h := [\![A[\tilde{x}/\tilde{a}]]\!]\, s\, h,$$

wobei A die rechte Seite der definierenden Gleichung von t ist.

Ferner:
$$[\![t_1 = t_2]\!]\, s\, h := t_1 = t_2.$$

<u>Beispiel</u>:

Für einfach verkettete Listen mit Einträgen u, v wählen wir

$$\Sigma := \{ u/0, v/0, \varepsilon/0, \cdot/2 \}$$

Die definierenden Gleichungen sind

Basisfälle
$$\begin{cases} [\mathrm{lseg}\ \varepsilon](i, j) := \mathrm{emp} \wedge i = j \\ [\mathrm{lseg}\ {}^{u}_{v}](i, j) := i \mapsto {}^{u}_{v}, j \end{cases}$$

Induktionsschritt
$$\{ [\mathrm{lseg}\ \alpha.\beta](i, j) := \exists k.\ [\mathrm{lseg}\ \alpha](i, k) \wedge [\mathrm{lseg}\ \beta](k, j)$$

Verglichen mit der Definition zu Anfang des Kapitels können wir nun mehr:

- Die Liste beginnt nicht nur bei i, wir haben ein Listensegment von i zu j.
- Wir haben die Separating-Conjunction benutzt und damit $[\mathrm{list}\ a_1 \ldots a_n](i_0, i_n)$ äquivalent zu

$$\exists i_1, \ldots, i_{n-1} .\ i_0 \mapsto a_1, i_1 * \ldots * i_{n-1} \mapsto a_n, i_n .$$

Per Definition von $*$ sind $i_0, \ldots, i_{n-1}$ alle verschieden. Das hat uns zu Anfang viel Mühe gemacht und reachable n eingebracht.

- Beachte, dass $i_0 = i_n$ sein kann,

$$[\mathrm{lseg}\ a_1 \ldots a_n](i, i) \quad \text{mag also gelten.}$$

Es gilt also

$$[\mathrm{lseg}\ \alpha](i, j) * (j \hookrightarrow \_) \rightarrow (i = j \Leftrightarrow \alpha = \varepsilon).$$