Karlsruher Institut für Technologie

Lehrstuhl für Programmierparadigmen

Andreas Lochbihler
andreas.lochbihler@kit.edu

Joachim Breitner
breitner@kit.edu

# Semantik von Programmiersprachen – SS 2012

http://pp.info.uni-karlsruhe.de/lehre/SS2012/semantik

## Lösungen zu Blatt 1: Mathematische Grundlagen

Besprechung: 24.04.2012

### 1. Äquivalenzrelationen und Ordnungen (H)

Eine **Relation** $R$ zwischen zwei Mengen $A$ und $B$ ist eine Teilmenge von $A \times B$, d.h., eine Menge von Paaren $(a, b)$ mit $a \in A$ und $b \in B$. Statt $(a, b) \in R$ schreibt man oft $a\ R\ b$.

Sei im Folgenden $A = B$. $R$ ist

**reflexiv** falls für alle $a \in A$ gilt: $a\ R\ a$

**symmetrisch** falls für alle $a, b \in A$ gilt: Wenn $a\ R\ b$, dann auch $b\ R\ a$.

**antisymmetrisch** falls für alle $a, b \in A$ gilt: Wenn $a\ R\ b$ und $b\ R\ a$, so gilt $a = b$.

**transitiv** falls für alle $a, b, c \in A$ gilt: Wenn $a\ R\ b$ und $b\ R\ c$, dann auch $a\ R\ c$.

**total** falls für alle $a, b \in A$ gilt: $a\ R\ b$ oder $a = b$ oder $b\ R\ a$.

Eine reflexive, symmetrische und transitive Relation ist eine **Äquivalenzrelation**. Eine reflexive, antisymmetrische und transitive Relation heißt **(Halb-)Ordnung**.

Sei $A = \{a, b, c\}$. Welche der folgenden Relationen sind Äquivalenzrelationen? Welche Ordnungsrelationen? Welche total? Begründen Sie Ihre Antwort!

- $R_1 = \{(a, a), (b, b), (c, c)\}$
- $R_2 = \{(a, a), (a, b), (b, a), (b, b), (c, c)\}$
- $R_3 = \{(a, a), (a, b), (a, c), (b, b), (b, c), (c, c)\}$
- $R_4 = \{(a, a), (a, b), (b, a), (b, b), (b, c), (c, c)\}$

**Lösung:**

- $R_1$ ist die einzige Ordnung und Äquivalenzrelation auf $A$, nicht total.
- $R_2$ ist eine Äquivalenzrelation. Nicht antisymmetrisch wegen $a\ R_2\ b$ und $b\ R_2\ a$.
- $R_3$ ist eine totale Ordnung.
- $R_4$ ist weder antisymmetrisch ($a\ R_4\ b$ und $b\ R_4\ a$) noch symmetrisch ($b\ R_4\ c$, nicht $c\ R_4\ b$).

### 2. Induktive Definitionen (Ü)

Ein Beispiel: *Natürliche Zahlen*. Die Menge der natürlichen Zahlen $\mathbb{N}$ lässt sich als Teilmenge der reellen Zahlen $\mathbb{R}$ wie folgt definieren:

(a) 0 ist eine natürliche Zahl.

(b) Wenn $n$ eine natürliche Zahl ist, so ist auch $n + 1$ eine natürliche Zahl.

(c) Nichts anderes soll eine natürliche Zahl sein.

Solch eine Definition lässt sich kürzer mit Regeln schreiben:

$$0 \in \mathbb{N} \qquad \frac{n \in \mathbb{N}}{n+1 \in \mathbb{N}}$$

Bedingung (c) ist das Charakteristikum für induktive Definitionen und liefert ein Induktionsprinzip: Regelinduktion. Formal:

$$\frac{m \in \mathbb{N} \qquad P(0) \qquad \forall n.\ n \in \mathbb{N} \land P(n) \longrightarrow P(n+1)}{P(m)}$$

Dies ist genau die Regel für Induktion über natürliche Zahlen: Um eine Aussage für eine beliebige natürliche Zahl zu zeigen, genügt es, sie für 0 zu zeigen, und für $n+1$ unter der Annahme, dass sie für $n$ gilt.
*Ein Beispielbeweis:* Die Summe der ersten n Zahlen ist gleich $\frac{n(n+1)}{2}$.
Formal: $P(n) \equiv \left(\sum\limits_{i=0}^{n} i = \frac{n(n+1)}{2}\right)$

- Induktionsanfang: Zu zeigen $P(0)$, d.h., $\sum\limits_{i=0}^{0} i = \frac{0(0+1)}{2}$ Beweis: Ausrechnen!
- Induktionsschritt: Zu zeigen: $\forall n.\ n \in \mathbb{N} \land P(n) \longrightarrow P(n+1)$. Sei $n \in \mathbb{N}$ beliebig.
  Induktionannahme: Es gilt $P(n)$, d.h. $\sum\limits_{i=0}^{n} i = \frac{n(n+1)}{2}$.
  Zu zeigen: $P(n+1)$, d.h. $\sum\limits_{i=0}^{n+1} i = \frac{(n+1)((n+1)+1)}{2}$.
  Beweis:

$$\sum_{i=0}^{n+1} i = \left(\sum_{i=0}^{n} i\right) + (n+1) = \text{(nach Induktionsannahme)}$$
$$\frac{n(n+1)}{2} + (n+1) = \frac{(n+1)((n+1)+1)}{2} \qquad \square$$

Sei $\rightarrow$ nun wieder eine Relation auf einer Menge $A$. Die reflexive, transitive Hülle $\rightarrow^*$ von $\rightarrow$ sei durch folgende Regeln definiert:

$$\textsc{refl}: a \rightarrow^* a \qquad \textsc{step}: \frac{a \rightarrow^* b \qquad b \rightarrow c}{a \rightarrow^* c}$$

(a) Bestimmen Sie für folgende Mengen die reflexive, transitive Hülle. Hierbei sei $A = \{a, b, c, d\}$.
   i. $\rightarrow_1 = \{(a,b), (b,d), (c,d)\}$
   ii. $\rightarrow_2 = \{(a,b), (b,c), (d,a)\}$
   iii. $\rightarrow_3 = \{(a,b), (b,c), (c,d), (d,a)\}$

**Lösung:**

| $\rightarrow_1^*$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | x | x | | x |
| $b$ | | x | | x |
| $c$ | | | x | x |
| $d$ | | | | x |

| $\rightarrow_2^*$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | x | x | x | |
| $b$ | | x | x | |
| $c$ | | | x | |
| $d$ | x | x | x | x |

| $\rightarrow_3^*$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | x | x | x | x |
| $b$ | x | x | x | x |
| $c$ | x | x | x | x |
| $d$ | x | x | x | x |

(b) Schreiben Sie die Induktionsregel für $\rightarrow^*$ auf.
**Lösung:**

$$\frac{x \rightarrow^* y \qquad \forall a.\ P(a,a) \qquad \forall a,b,c.\ a \rightarrow^* b \land P(a,b) \land b \rightarrow c \longrightarrow P(a,c)}{P(x,y)}$$

(c) Zeigen Sie, dass $\rightarrow^*$ reflexiv ist.

**Lösung:** Zu zeigen: Für alle $a \in A$ gilt: $a \rightarrow^* a$. Dies folgt direkt aus der Regel REFL.

(d) Zeigen Sie mittels Induktion, dass auch folgende Regel gilt:

$$\frac{x \rightarrow y \qquad y \rightarrow^* z}{x \rightarrow^* z}$$

**Lösung:**

Annahmen: $x \rightarrow y$ und $y \rightarrow^* z$.

Zu zeigen: $x \rightarrow^* z$. Induktion nach $y \rightarrow^* z$.

Damit $P(y, z) \equiv x \rightarrow y \longrightarrow x \rightarrow^* z$.

1. Fall: Zu zeigen: $\forall a.\ P(a, a)$, d.h.: $\forall a.\ x \rightarrow a \longrightarrow x \rightarrow^* a$. Beweis mittels eines Ableitungsbaums.

Sei $a$ beliebig mit $x \rightarrow a$. Dann gilt:

$$\dfrac{\dfrac{}{x \rightarrow^* x}\,\textsc{refl} \qquad \dfrac{}{x \rightarrow a}}{x \rightarrow^* a}\,\textsc{step}$$

2. Fall: Zu zeigen: $\forall a, b, c.\ a \rightarrow^* b \wedge P(a, b) \wedge b \rightarrow c \longrightarrow P(a, c)$.

Beweis: Seien $a$, $b$, $c$ beliebig mit $a \rightarrow^* b$ und $b \rightarrow c$.

Induktionsannahme $P(a, b)$, d.h. $x \rightarrow a \longrightarrow x \rightarrow^* b$.

Zu zeigen: $P(a, c)$, d.h., $x \rightarrow a \longrightarrow x \rightarrow^* c$.

Beweis: Gelte $x \rightarrow a$. Nach Induktionsannahme gilt dann auch $x \rightarrow^* b$. Zusammen mit $b \rightarrow c$ folgt $x \rightarrow^* c$ nach der Regel STEP.

(e) Zeigen Sie, dass $\rightarrow^*$ transitiv ist.

**Lösung:**

Seien $x \rightarrow^* y$ und $y \rightarrow^* z$. Zu zeigen: $x \rightarrow^* z$. Induktion über $y \rightarrow^* z$. Damit $P(y, z) \equiv (x \rightarrow^* y \longrightarrow x \rightarrow^* z)$.

1. Fall: Zu zeigen: $\forall a.\ P(a, a)$, d.h.: $x \rightarrow^* a \longrightarrow x \rightarrow^* a$. Trivial.

2. Fall: Zu zeigen: $\forall a, b, c.\ a \rightarrow^* b \wedge P(a, b) \wedge b \rightarrow c \longrightarrow P(a, c)$.

Beweis: Seien $a$, $b$, $c$ beliebig mit $a \rightarrow^* b$ und $b \rightarrow c$.

Induktionannahme: $P(a, b)$, d.h. $x \rightarrow^* a \longrightarrow x \rightarrow^* b$.

Zu zeigen: $P(a, c)$, d.h. $x \rightarrow^* a \longrightarrow x \rightarrow^* c$.

Beweis: Angenommen, $x \rightarrow^* a$. Nach Induktionsannahme folgt $x \rightarrow^* b$. Zusammen mit $b \rightarrow c$ folgt $x \rightarrow^* c$ nach der Regel STEP.

*Alternativer Beweis mit Induktion über $x \rightarrow^* y$:*

Damit $P(x, y) \equiv (y \rightarrow^* z \longrightarrow x \rightarrow^* z)$.

1. Fall: Zu zeigen: $\forall a.\ P(a, a)$, d.h.: $a \rightarrow^* z \longrightarrow a \rightarrow^* z$. Trivial.

2. Fall: Zu zeigen: $\forall a, b, c.\ a \rightarrow^* b \wedge P(a, b) \wedge b \rightarrow c \longrightarrow P(a, c)$.

Beweis: Seien $a$, $b$, $c$ beliebig mit $a \rightarrow^* b$ und $b \rightarrow c$.

Induktionannahme: $P(a, b)$, d.h. $b \rightarrow^* z \longrightarrow a \rightarrow^* z$.

Zu zeigen: $P(a, c)$, d.h. $c \rightarrow^* z \longrightarrow a \rightarrow^* z$.

Beweis: Sei $c \rightarrow^* z$. Mit $b \rightarrow c$ folgt $b \rightarrow^* z$ nach vorheriger Aufgabe. Nach Induktionsannahme folgt $a \rightarrow^* z$.

(f) Regelsysteme lassen sich direkt in Prolog-Prädikate übersetzen. Implementieren Sie entsprechend obiger Regeln ein Prolog-Prädikat `rtrancl(R,X,Y)`, das erfüllt ist, wenn `X` `R`$^*$ `Y` für das Prolog-Prädikat `R` gilt.

**Lösung:**

```
rtrancl(_,A,A).
rtrancl(R,A,C) :- call(R,B,C),rtrancl(R,A,B).
```

**3. Falsche Induktionsbeweise (H)**

Finden Sie die Fehler in folgenden Induktionsbeweisen!

(a) Alle Pferde einer endlichen Menge $M$ von Pferden haben die gleiche Farbe.

Sei $n$ die Anzahl der Pferde in $M$. Beweis durch Induktion über $n$.

Induktionsanfang: $n = 0$. Dann ist $M$ leer und die Aussage trivial. Induktionsschritt: Angenommen, für alle Pferdemengen $M'$ der Größe $n$ gilt die Aussage. Sei $M$ eine Pferdemenge der Größe $n + 1$, also $M = \{p_0, p_1, \ldots, p_n\}$. Dann ist $M_1 = \{p_0, p_1, \ldots, p_{n-1}\}$ eine Pferdemenge der Größe $n$, somit haben $p_0, \ldots, p_{n-1}$ alle die gleiche Farbe. Wähle nun $M_2 = \{p_1, p_2, \ldots, p_n\}$. Dies ist wieder eine Pferdemenge der Größe $n$, somit haben auch $p_1, \ldots, p_n$ alle die gleiche Farbe. Damit hat $p_0$ also die gleiche Farbe wie $p_1$ und $p_1$ die gleiche Farbe wie $p_2$ bis $p_n$, somit haben alle Pferde aus $M$ die gleiche Farbe.

**Lösung:** Für $n = 1$ im Induktionsschritt überlappen sich die Mengen $M_1$ und $M_2$ nicht, damit haben die beiden Pferde $p_0$ und $p_1$ also nicht notwendigerweise die gleiche Farbe.

(b) Sei $\to$ eine beliebige binäre Relation auf der Menge $\{\text{grün}, \text{gelb}, \text{rot}\}$. Dann gilt, dass in der transitiven Hülle von $\to$ nur rot von rot aus erreichbar ist.

Formal: Für alle $b$ gilt, wenn rot $\to^* b$, dann rot $= b$.

Beweis per (Regel-)Induktion über rot $\to^* b$:

- Fall REFL: Zu zeigen: rot = rot. Trivial.
- Fall STEP: Induktionsannahmen: rot $\to^* b$, $b \to c$ und $b =$ rot.
  Zu zeigen: rot $= b$. Folgt aus der Annahme.

**Lösung:** Das zu Zeigende in Fall STEP ist falsch, es müsste rot $= c$ heißen.

Grundsätzlich ist bei Induktionen über induktiv definierte Relationen Vorsicht angebracht, wenn einzelne Parameter bereits fixiert sind (im Beispiel rot) und diese Fixierung durch die Induktion geschleift werden soll. Die Allquantoren der Induktionsregel heben eine solche Fixierung auf, so dass man formal die Fixierung in die Eigenschaft $P$ packen müsste: Wenn $a \to^* b$ und $a = rot$, dann $rot = b$. Somit wäre $P(a, b) = (a = rot \longrightarrow rot = b)$.