2.2 Basisrelationen zur Beschreibung des Programmverhaltens

2.2.1 Zusicherungstechnik nach Floyd-Hoare

$\{p\}s\{q\}$ besagt, daß die Ausführung der Anweisung s in einem Zustand, der das Prädikat p erfüllt, zu einem Zustand führt, der das Prädikat q erfüllt.

Einige wichtige Aussagen:

- $\{p\}s\{true\}$
- $\{false\}s\{q\}$
- $\dfrac{\{p\}s\{false\}}{\neg p}$
- $\dfrac{\{p\}s\{q\},\ \{p'\}s\{q'\}}{\{p \vee p'\}s\{q \vee q'\},\ \{p \wedge p'\}s\{q \vee q'\}}$
- $\left\{(b_0 \Rightarrow q^x_{e_0}) \wedge \ \ldots \wedge (b_n \Rightarrow q^x_{e_n}) \wedge ((\neg b_0 \wedge \ldots \wedge \neg b_n) \Rightarrow q)\right\}$

  $x := e_0 \ \text{ if } \ b_0 \sim \ldots \sim e_n \ \text{ if } \ b_n \quad \{q\}$

Reproduktion jeder Art oder Verwendung dieser Unterlage zu Lehrzwecken außerhalb der Universität Erlangen-Nürnberg ist ohne Genehmigung des Autors unzulässig

2.2.2 Die Relation *unless*

❑ Definition:

◆ Quantifizierung:

F sei ein Programm

- $\langle \forall s(s \text{ in } F \Rightarrow \{p\}s\{q\})\rangle$ soll zum Ausdruck bringen, daß für alle Anweisung s des Programms F die Aussage $\{p\}s\{q\}$ zutrifft,
- $\langle \exists s(s \text{ in } F \Rightarrow \{p\}s\{q\})\rangle$ soll zum Ausdruck brinngen, daß auf wenigstens eine Anweisung des Programms F die Aussage $\{p\}s\{q\}$ zutrifft.

◆ F sei ein Programm, s eine Anweisung

$$p \text{ unless } q \equiv \langle \forall s\colon s \text{ in } F :: \{p \wedge \neg q\}s\{p \vee q\}\rangle \ ,$$

informell: Wenn p erst einmal gültig ist, dann bleibt es mindestens bis zum Eintreten von q gültig.

Reproduktion jeder Art oder Verwendung dieser Unterlage zu Lehrzwecken außerhalb der Universität Erlangen-Nürnberg ist ohne Genehmigung des Autors unzulässig

❑ Beispiel: Der Wert der Variablen x ist monoton wachsend

$$x = k \ \text{ unless } \ x > k$$

◆ Spezialfälle:

$$p \ \text{ is stable } \ \equiv p \text{ unless false}$$

$$q \ \text{ is invariant } \ \equiv (\text{initial condition } \Rightarrow q) \wedge q \ \text{ is stable}$$

◆ Bemerkung:

p is stable ist äquivalent zu $\forall s(s \text{ in } F \Rightarrow \{p\}s\{p\})$,
p wird deshalb auch als Invariante von F bezeichnet.

◆ Der Always-Abschnitt eines Programms kann als Definition einer Invarianten angesehen werden.

Reproduktion jeder Art oder Verwendung dieser Unterlage zu Lehrzwecken außerhalb der Universität Erlangen-Nürnberg ist ohne Genehmigung des Autors unzulässig

2.2.3 Die Relation *ensures*

❑ Definition:

$$p \ \text{ ensures } \ q \equiv (p \text{ unless } q \wedge \langle \exists s\colon s \text{ in } F :: \{p \wedge \neg q\}s\{q\}\rangle)$$

❑ Beispiel: Der Wert der Variablen x ist monoton wachsend

$$x = k \ \text{ ensures } \ x > k$$

2.2.4 Die Relation *leads-to* ($\mapsto$)

❑ Definition:

Es gilt $p \mapsto q$ genau dann, wenn es auf Grund des folgenden Regelsystems ableitbar ist:

$$\frac{p \ \text{ ensures } \ q}{p \mapsto q}$$

(Transitivität)
$$\frac{p \mapsto q,\ q \mapsto r}{p \mapsto r}$$

(Disjunktivität)
$$\frac{\forall m(m \in W \Rightarrow p(m) \mapsto q \ )}{\langle \exists m(m \in W \wedge p(m))\rangle \mapsto q}$$

Reproduktion jeder Art oder Verwendung dieser Unterlage zu Lehrzwecken außerhalb der Universität Erlangen-Nürnberg ist ohne Genehmigung des Autors unzulässig

2.2.5 Fixpunkt

❑ Sei R eine zu einer Ausführungsfolge gehörige Zustandsfolge,
dann besitzt jedes Element R_i von R eine Komponente

R_i.state, die den Zustand der Variablen darstellt, und eine Komponente

R_i.label, die die Zuweisung charakterisiert, die zu R_{i+1}.state führt.

R_0.state ist der Anfangszustand.

❑ Das *Fixpunktprädikat FP* eines Programms G ist folgendermaßen definiert:

$$\forall s(s \text{ in } G \wedge s \text{ is } X{:=}E \Rightarrow (X = E))$$

oder im Zustandsmodell

$$FP[R_i] \equiv \langle \forall j(j \geq i \Rightarrow R_i.\text{state} = R_j.\text{state}) \rangle .$$

2.2.6 Die Relationen *detects* und *until*

◆ Definitionen

$$p \text{ detects } q \equiv (p \Rightarrow q) \wedge (q \mapsto p)$$

$$p \text{ until } q \equiv (p \text{ unless } q) \wedge (p \mapsto q)$$

Reproduktion jeder Art oder Verwendung dieser Unterlage zu Lehrzwecken außerhalb der Universität Erlangen-Nürnberg ist ohne Genehmigung des Autors unzulässig

2.2.7 Wichtige Theoreme

❑ unless

- Reflexivität
  p unless p
  Antireflexivität
  p unless $\neg$p
- Abschwächung der Nachbedingung

$$\frac{p \text{ unless } q,\ q \Rightarrow r}{p \text{ unless } r}$$

- Konjunktion und Disjunktion

$$\frac{\begin{array}{c}p \text{ unless } q,\\ p' \text{ unless } q'\end{array}}{\begin{array}{c}(p \wedge p') \text{ unless } (p \wedge q') \vee (p' \wedge q) \vee (q \wedge q')\\ (p \vee p) \text{ unless } (\neg p \wedge q') \vee (\neg p' \wedge q) \vee (q \wedge q')\end{array}}$$

- Kürzung

$$\frac{\begin{array}{c}p \text{ unless } q,\\ q \text{ unless } r\end{array}}{p \vee q \text{ unless } r}$$

Reproduktion jeder Art oder Verwendung dieser Unterlage zu Lehrzwecken außerhalb der Universität Erlangen-Nürnberg ist ohne Genehmigung des Autors unzulässig

❑ ensures

- Reflexivität
  p ensures p
- Abschwächung der Nachbedingung

$$\frac{p \text{ ensures } q,\ q \Rightarrow r}{p \text{ ensures } r}$$

- Unmöglichkeit

$$\frac{p \text{ ensures false}}{\neg p}$$

- Konjunktion

$$\frac{\begin{array}{c}p \text{ unless } q,\\ p' \text{ ensures } q'\end{array}}{p \wedge p' \text{ ensures } (p \wedge q') \vee (p' \wedge q) \vee (q \wedge q')}$$

- Disjunktion

$$\frac{p \text{ ensures } q}{p \vee r \text{ ensures } q \vee r}$$

Reproduktion jeder Art oder Verwendung dieser Unterlage zu Lehrzwecken außerhalb der Universität Erlangen-Nürnberg ist ohne Genehmigung des Autors unzulässig

❑ leads-to

- Implikation

$$\frac{p \Rightarrow q}{p \mapsto q}$$

- Unmöglichkeit

$$\frac{p \mapsto \text{false}}{\neg p}$$

- Disjunktion
  Für jede Menge W gilt:

$$\frac{\langle \forall m(m \in W \Rightarrow p(m) \mapsto q(m)) \rangle}{\langle \exists m(m \in W \wedge p(m)) \rangle \mapsto \langle \exists m(m \in W \wedge q(m)) \rangle}$$

- Kürzung

$$\frac{p \mapsto q \vee b,\ b \mapsto r}{p \mapsto q \vee r}$$

Reproduktion jeder Art oder Verwendung dieser Unterlage zu Lehrzwecken außerhalb der Universität Erlangen-Nürnberg ist ohne Genehmigung des Autors unzulässig

- PSP-Theorem (Progress-Safety-Progress)

$$\frac{p \mapsto q,\ r \text{ unless } b}{p \wedge r \mapsto (q \wedge r) \vee b}$$

- Fertigstellung

$$\frac{\langle \forall i (p_i \mapsto q_i \vee r) \rangle \quad \langle \forall i (q_i \text{ unless } r) \rangle}{\langle \wedge i (p_i) \rangle \mapsto \langle \wedge i (q_i) \rangle \vee r}$$

❑ Fixpunkt

- Stabilität im Fixpunkt
  Für jedes Prädikat p ist $(FP \wedge p)$ stabil (stable).
- Korollar: $\dfrac{p \mapsto q}{FP \Rightarrow (p \Rightarrow q)}$

Reproduktion jeder Art oder Verwendung dieser Unterlage zu Lehrzwecken außerhalb der Universität Erlangen-Nürnberg ist ohne Genehmigung des Autors unzulässig