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:

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

2.2.2 Die Relation *unless*

- Definition:
  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 gültig ist, dann bleibt es mindestens bis zum Eintreten von q gültig.
- Beispiel: Der Wert der Variablen x ist monoton wachsend
  $x = k \text{ unless } x > k$
- Spezialfälle:
  p is stable $\equiv p$ unless false
  q is invariant $\equiv$ (initial condition $\Rightarrow q) \wedge q$ is stable
- Bemerkung:
  p is stable ist äquivalent zu $\langle \forall s\colon s \text{ in } F :: \{p\}s\{p\}\rangle$,
  p wird deshalb auch als Invariante von F bezeichnet.
- Der Always-Abschnitt eines Programms kann als Definition einer Invarianten angesehen werden.

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 wächst streng monoton
  $x = k \text{ ensures } x > k$

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:

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

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

  (Disjunktivität) $\dfrac{\langle \forall m\colon m \in W :: p(m) \mapsto q\rangle}{\langle \exists m\colon m \in W :: p(m)\rangle \mapsto q}$

2.2.5 Fixpunkt

- Sei R eine zu einer Ausführungsfolge gehörige Zustandsfolge, dann besitzt jedes Element R_i von R die beiden Komponenten
  $R_i.state$, die den Zustand der Variablen darstellt, und
  $R_i.label$, die die Zuweisung charakterisiert, die zu $R_{i+1}.state$ führt.
  R_0,state ist der Anfangszustand.
- Das Fixkpunktprädikat eines Programms G ist folgendermaßen definiert:
  $FP \equiv \langle \forall \text{ statements } s\colon s \text{ in } G \wedge s \text{ is } X := E :: X = E\rangle$

  oder im Zustandsmodell
  $FP[R_i] \equiv \langle \forall j\colon j \geq i :: R_i.state = R_j.state\rangle$.

2.2.6 Die Relationen *detects* und *until*

- Definitionen
  $p \text{ detects } q \equiv (p \Rightarrow q) \wedge (q \mapsto p)$
  $p \text{ until } q \equiv (p \text{ unless } q) \wedge (p \mapsto q)$

2.2.7 Wichtige Theoreme

1. *unless*

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

2. *ensures*

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

3. *leads-to*

- Implikation
  $$\frac{p \Rightarrow q}{p \mapsto q}$$
- Unmöglichkeit
  $$\frac{p \mapsto \text{false}}{\neg p}$$
- Disjunktion
  Für jede Menge W gilt:
  $$\frac{\langle \forall m : m \in W :: p(m) \mapsto q(m) \rangle}{\langle \exists m : m \in W :: p(m) \rangle \mapsto \langle \exists m : m \in W :: q(m) \rangle}$$
- Kürzung
  $$\frac{p \mapsto q \vee b,\; b \mapsto r}{p \mapsto q \vee r}$$
- PSP-Theorem (Progress-Safety-Progress)
  $$p \mapsto q,\; r \text{ unless } b$$
  $$p \wedge r \mapsto (q \wedge r) \vee b$$

- Fertigstellung
  $$\frac{\begin{array}{c} \langle \forall i :: p_i \mapsto q_i \vee r \rangle \\ \langle \forall i :: q_i \text{ unless } r \rangle \end{array}}{\langle \wedge i :: p_i \rangle \mapsto \langle \wedge i :: q_i \rangle \vee r}$$

4. Fixpunkt

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