Das Beweissystem PD

http://www.informatik.uni-bremen.de/theorie/teach/veri

Renate Klempien-Hinrichs

- Beweissystem PD
- Beweis von Korrektheitsformeln
- Korrektheit von PD

Das Bausteine-im-Sack-Spiel

- Bei **Spielanfang** befindet sich eine unbekannte Anzahl roter und schwarzer Bausteine im Sack und ein unbeschränkter Vorrat an schwarzen Bausteinen daneben.
- In einem **Spielzug** werden zwei Bausteine aus dem Sack genommen.
  - Wenn sie dieselbe Farbe haben, werden sie weggelegt und ein schwarzer Baustein aus dem Vorrat kommt in den Sack.
  - Wenn sie unterschiedliche Farben haben, wird der schwarze weggelegt und der rote zurück in den Sack.
- Es werden so viele Spielzüge wie möglich ausgeführt.

---

1. **Frage:** Hört das Spiel irgendwann auf?
2. **Frage:** Wenn das Spiel aufhört, was ist dann im Sack?

Beweissystem PD

(i) $\{p\}\ skip\ \{p\}$ — leere Anweisung

(ii) $\{p[x := t]\}\ x := t\ \{p\}$ — Wertzuweisung

(iii) $$\frac{\{p\}\ S_1\ \{r\},\ \{r\}\ S_2\ \{q\}}{\{p\}\ S_1; S_2\ \{q\}}$$ — sequentielle Komposition

(iv) $$\frac{\{p \wedge B\}\ S_1\ \{q\},\ \{p \wedge \neg B\}\ S_2\ \{q\}}{\{p\}\ \mathbf{if}\ B\ \mathbf{then}\ S_1\ \mathbf{else}\ S_2\ \mathbf{fi}\ \{q\}}$$ — bedingte Anweisung

(v) $$\frac{\{p \wedge B\}\ S\ \{p\}}{\{p\}\ \mathbf{while}\ B\ \mathbf{do}\ S\ \mathbf{od}\ \{p \wedge \neg B\}}$$ — Schleife

(vi) $$\frac{p \to p',\ \{p'\}\ S\ \{q'\},\ q' \to q}{\{p\}\ S\ \{q\}}$$ — Konsequenzregel

Außerdem enthält PD alle gültigen Formeln.

Diese und die Korrektheitsformeln von der Form (i) bzw. (ii) heißen Axiome.

Gültige Formeln

Insbesondere die folgenden Formeln sind für alle Formeln q, r gültig:

(1) $\mathbf{false} \rightarrow q$

(2) $\mathbf{false} \rightarrow \neg q$

(3) $q \rightarrow \mathbf{true}$

(4) $\neg q \rightarrow \mathbf{true}$

(5) $q \rightarrow q$

(6) $q \wedge r \rightarrow q$

(7) $q \wedge r \rightarrow r$

(8) $q \rightarrow q \vee r$

(9) $q \rightarrow r \vee q$

(10) $q \wedge (q \rightarrow r) \rightarrow r$

(11) $(q \rightarrow r) \wedge q \rightarrow r$

Beweis von Korrektheitsformeln

Eine Korrektheitsformel $\{pre\}\ S\ \{post\}$ ist beweisbar mit PD, in Zeichen $\vdash_{\mathsf{PD}} \{pre\}\ S\ \{post\}$, wenn es eine Folge $F_1, \ldots, F_n$ von Formeln und Korrektheitsformeln gibt, so dass gilt:

(1) $F_n = \{pre\}\ S\ \{post\}$ und

(2) für $i = 1, \ldots, n$ ist F_i entweder ein Axiom oder es gibt $F_{i_1}, \ldots, F_{i_k}$ mit $i_1, \ldots, i_k < i$, so dass

$$\frac{F_{i_1}, \ldots, F_{i_k}}{F_i}$$

eine Instanz einer der Regeln (iii)-(vi) ist.

Die Folge $F_1, \ldots, F_n$ heißt Beweis von $\{pre\}\ S\ \{post\}$.

Beispiel: Beweis in PD (1)

Sei DIV $\equiv$ $quo := 0;\ rem := x;\ S_0$ mit $S_0 \equiv$ **while** $rem \geq y$ **do**
$rem := rem - y;$
$quo := quo + 1$
od .

Zeige: $\vdash_{\mathsf{PD}}$ $\{0 \leq x \wedge 0 \leq y\}$ DIV $\{\underbrace{quo \cdot y + rem = x \wedge 0 \leq rem}_{p?}\ \underbrace{rem < y}_{\neg B}\}$.

Vermutung: Schleifeninvariante $p \equiv quo \cdot y + rem = x \wedge 0 \leq rem$

Beispiel: Beweis in PD (2)

2.2 $\{0 \cdot y + x = x \wedge 0 \leq x\}\ quo := 0\ \{quo \cdot y + x = x \wedge 0 \leq x\}$ {(ii)}

2.1 $\{quo \cdot y + x = x \wedge 0 \leq x\}\ rem := x\ \{p\}$ {(ii)}

2.3 $\{0 \cdot y + x = x \wedge 0 \leq x\}\ quo := 0; rem := x\ \{p\}$ {(iii): 2.2–2.1}

2.4 $0 \leq x \wedge 0 \leq y \rightarrow 0 \cdot y + x = x \wedge 0 \leq x$ {gültige Formel}

1.1.2 $\{(quo + 1) \cdot y + rem - y = x \wedge 0 \leq rem - y\}$
$rem := rem - y\ \{(quo + 1) \cdot y + rem = x \wedge 0 \leq rem\}$ {(ii)}

1.1.1 $\{(quo + 1) \cdot y + rem = x \wedge 0 \leq rem\}\ quo := quo + 1\ \{p\}$ {(ii)}

1.1.3 $\{(quo + 1) \cdot y + rem - y = x \wedge 0 \leq rem - y\}$
$rem := rem - y; quo := quo + 1\ \{p\}$ {(iii): 1.1.2–1.1.1}

1.1.4 $p \wedge B \rightarrow (quo + 1) \cdot y + rem - y = x \wedge 0 \leq rem - y$ {gültige Formel}

1.1.5 $p \rightarrow p$ {gültige Formel}

1.1 $\{p \wedge B\}\ rem := rem - y; quo := quo + 1\ \{p\}$ {(vi): 1.1.4–1.1.3–1.1.5}

2 $\{0 \leq x \wedge 0 \leq y\}\ quo := 0; rem := x\ \{p\}$ {(vi): 2.4–2.3–1.1.5}

1 $\{p\}\ S_0\ \{p \wedge \neg B\}$ {(v): 1.1}

$\{0 \leq x \wedge 0 \leq y\}$ DIV $\{p \wedge \neg B\}$ {(iii): 2–1}

Korrektheit von PD

Ein Beweissystem K für eine Klasse C von Programmen ist korrekt für die partielle Korrektheit von Programmen aus C, wenn für alle Korrektheitsformeln $\{p\}\ S\ \{q\}$ mit $S \in C$ gilt:

$$\vdash_K \{p\}\ S\ \{q\} \text{ impliziert } \models \{p\}\ S\ \{q\}\,.$$

Satz (Korrektheit von PD)

PD ist korrekt für die partielle Korrektheit von deterministischen Programmen.