Sprechweisen im Zshg. mit Hoare-Tripeln (1)

Hoaresche Zusicherungen sind von einer der zwei Formen

- $\{p\}\ \pi\ \{q\}$ und
- $[p]\ \pi\ [q]$

wobei

- p, q logische Formeln sind (meist prädikatenlogische Formeln 1. Stufe) und
- π ein Programm ist.

Sprechweisen im Zshg. mit Hoare-Tripeln (2)

In einer Hoareschen Zusicherung von einer der Formen

- $\{p\}\ \pi\ \{q\}$ und
- $[p]\ \pi\ [q]$

heißen

- p und q *Vor-* bzw. *Nachbedingung*.

Sprechweisen im Zshg. mit Hoare-Tripeln (3)

In einer Hoareschen Zusicherung werden üblicherweise

- geschweifte Klammern wie in

  $$\{p\}\ \pi\ \{q\}$$

  für Tripel im Sinne *partieller Korrektheit* und

- eckige Klammern wie in

  $$[p]\ \pi\ [q]$$

  für Tripel im Sinne *totaler Korrektheit*

benutzt.

Sprechweisen im Zshg. mit Hoare-Tripeln (4)

Zwei Beispiele Hoarescher Zusicherungen:

$$\{a > 0\}$$
$$x := a;\ \ y := 1;\ \ \text{while } x > 1 \text{ do } y := y * x; x := x - 1 \text{ od}$$
$$\{y = a!\}$$

...zum Ausdruck partieller Korrektheit von π *bzgl. der Vorbedingung* $a > 0$ *und der Nachbedingung* $y = a!$

$$[a > 0]$$
$$x := a;\ \ y := 1;\ \ \text{while } x > 1 \text{ do } y := y * x; x := x - 1 \text{ od}$$
$$[y = a!]$$

...zum Ausdruck totaler Korrektheit von π *bzgl. der Vorbedingung* $a > 0$ *und der Nachbedingung* $y = a!$

Sprechweisen im Zshg. mit Hoare-Tripeln (5)

Die Wortwahl

- *Hoaresches Tripel* oder kurz *Hoare-Tripel* bzw.
- *Hoaresche Zusicherung* oder kurz *Korrektsheitsformel*

betont jeweils die

- syntaktische bzw.
- semantische Sicht

auf

- $\{p\}\ \pi\ \{q\}$ bzw. $[p]\ \pi\ [q]$

Weitere Sprechweisen

Ein (deterministisches) Programm π

- angesetzt auf einen Anfangszustand σ *terminiert regulär* gdw. π nach endlich vielen Schritten in einem Zustand $\sigma' \in \Sigma$ endet.

  Mit $Def(\llbracket \pi \rrbracket)$ bezeichnen wir die Menge aller Zustände, für die π regulär terminiert.

- angesetzt auf einen Anfangszustand σ *terminiert irregulär* gdw. π nach endlich vielen Schritten zur Konfiguration $undef$ führt.

- Ein Programm π heißt *divergent* gdw. π terminiert für keinen Anfangszustand regulär.

Erinnerung: WHILE-Programme sind deterministisch!

Definition partieller Korrektheit

Sei $\pi \in \mathbf{Prg}$ ein WHILE-Programm:

Ein Hoaresche Zusicherung $\{p\}\ \pi\ \{q\}$ heißt

- *gültig* (*im Sinne der partiellen Korrektheit*) oder kurz (*partiell*) *korrekt* gdw. für jeden Anfangszustand σ gilt: ist die Vorbedingung p in σ erfüllt **und** terminiert die zugehörige Berechnung von π angesetzt auf σ regulär in einem Endzustand σ', **dann** ist auch die Nachbedingung q in σ' erfüllt.

Definition totaler Korrektheit

Sei $\pi \in \mathbf{Prg}$ ein WHILE-Programm:

Ein Hoaresche Zusicherung $[p]\ \pi\ [q]$ heißt

- *gültig* (*im Sinne der totalen Korrektheit*) oder kurz (*total*) *korrekt* gdw. für jeden Anfangszustand σ gilt: ist die Vorbedingung p in σ erfüllt, **dann** terminiert die zugehörige Berechnung von π angesetzt auf σ regulär mit einem Endzustand σ' **und** die Nachbedingung q ist in σ' erfüllt.

Partielle und totale Korrektheit

Erinnerung:

- Die Zustandsmenge

  $$Ch(p) =_{df} \{\sigma \in \Sigma \mid [\![\, p \,]\!]_B(\sigma) = true\}$$

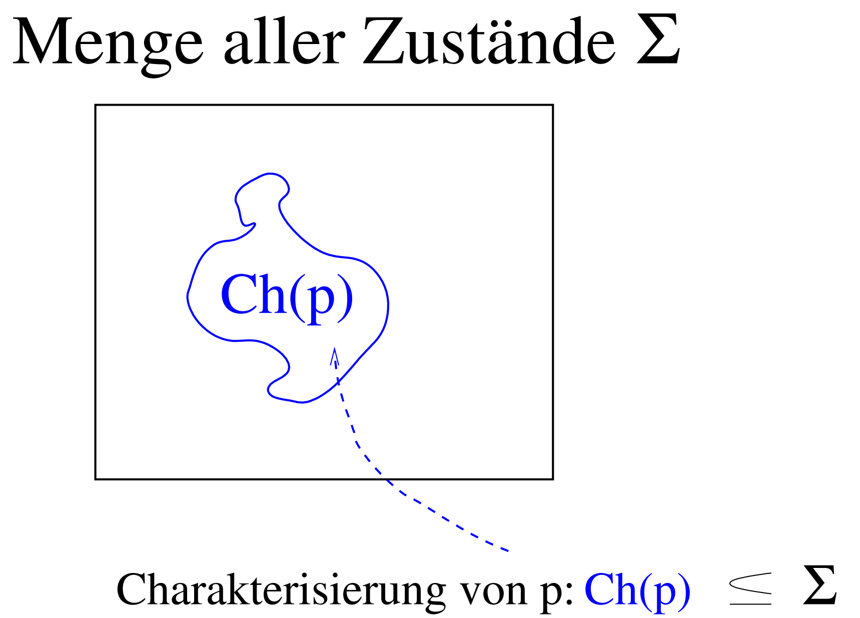
  heißt *Charakterisierung von* $p \in$ **Bexp**.

- *Semantik von Korrektheitsformeln:*
  Eine Korrektheitsformel $\{p\}\ \pi\ \{q\}$ heißt
  - *partiell korrekt*, falls $[\![\, \pi \,]\!](Ch(p)) \subseteq Ch(q)$
  - *total korrekt*, falls $\{p\}\ \pi\ \{q\}$ partiell korrekt ist und $Def([\![\, \pi \,]\!]) \supseteq Ch(p)$ gilt.

  Konvention: $[\![\, \pi \,]\!](Ch(p)) =_{df} \{[\![\, \pi \,]\!](\sigma) \mid \sigma \in Ch(p)\}$

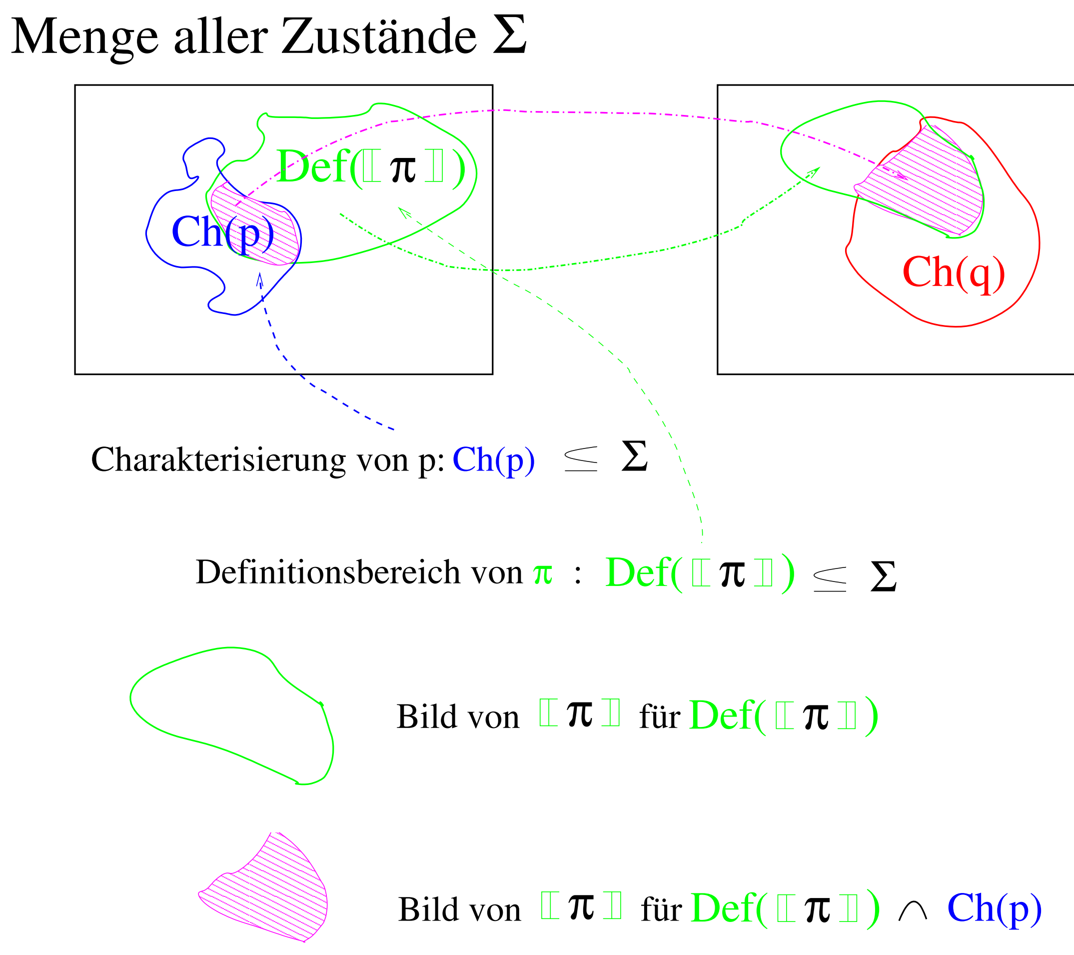
Veranschaulichung (1)

...der Charakterisierung $Ch(p)$ einer logischen Formel p:



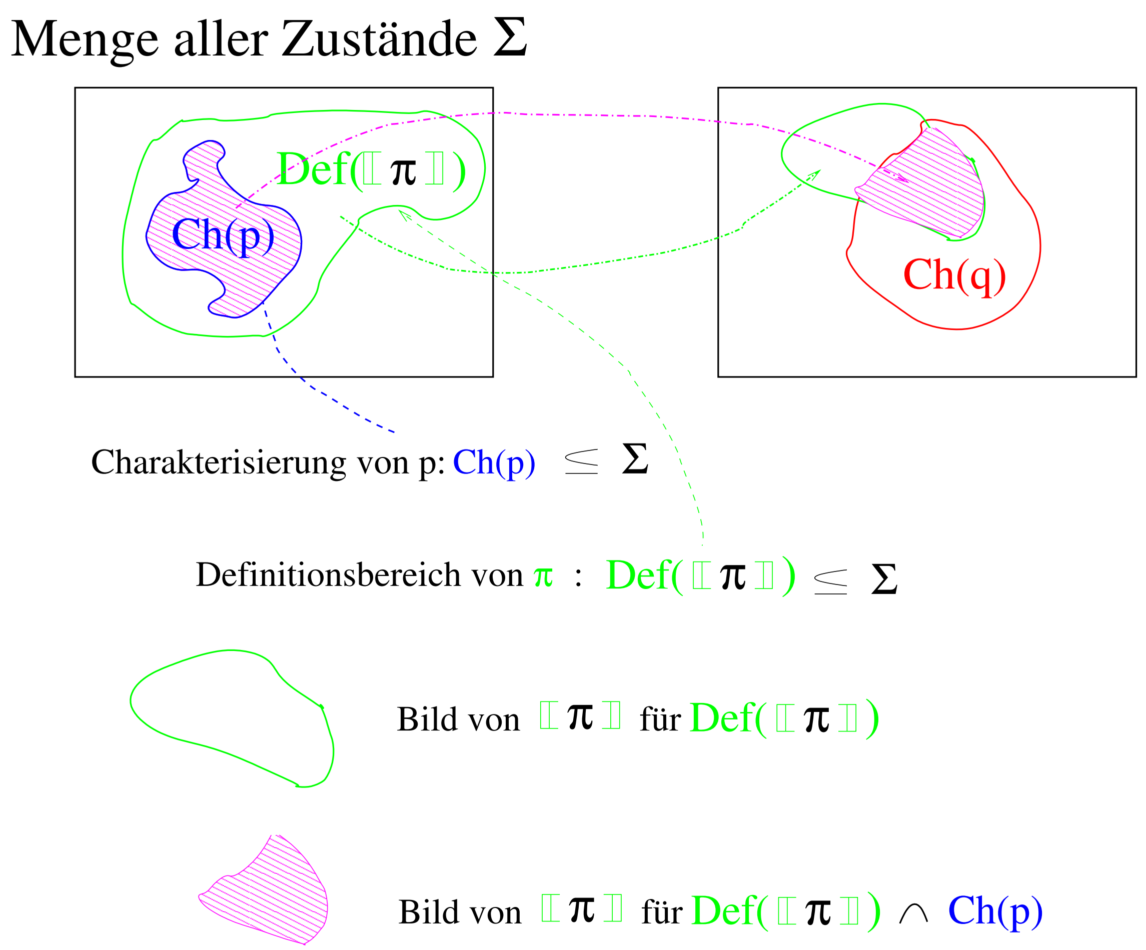
Veranschaulichung (2)

...der Gültigkeit eine Hoareschen Zusicherung $\{p\}\ \pi\ \{q\}$ im Sinne partieller Korrektheit:



Veranschaulichung (3)

...der Gültigkeit eine Hoareschen Zusicherung $[p]\ \pi\ [q]$ im Sinne totaler Korrektheit:



Stärkste Nach- und schwächste Vorbedingungen (1)

In der Situation der vorigen Abbildungen gilt:

- $[\![\,\pi\,]\!](Ch(p))$ heißt *stärkste Nachbedingung* von π bezüglich p.
- $[\![\,\pi\,]\!]^{-1}(Ch(q))$ heißt *schwächste Vorbedingung* von π bezüglich q, wobei $[\![\,\pi\,]\!]^{-1}(\Sigma')=_{df}\{\sigma \in \Sigma | [\![\,\pi\,]\!](\sigma) \in \Sigma'\}$
- $[\![\,\pi\,]\!]^{-1}(Ch(q)) \cup C(Def([\![\,\pi\,]\!]))$ heißt *schwächste liberale Vorbedingung* von π bezüglich q, wobei C den Mengenkomplementsoperator (bzgl. der Grundmenge Σ) bezeichnet.

Stärkste Nach- und schwächste Vorbedingungen (2)

Lemma

Ist $[\![\, \pi \,]\!]$ total definiert, d.h. gilt $Def([\![\, \pi \,]\!]) = \Sigma$, dann gilt für alle Formeln p und q:

$$[\![\, \pi \,]\!](Ch(p)) \subseteq Ch(q) \iff [\![\, \pi \,]\!]^{-1}(Ch(q)) \supseteq Ch(p)$$

Beweis: Übungsaufgabe

Partielle vs. totale Korrektheit

Lemma

Für deterministische Programme π gilt:

- $[p]\ \pi\ [q] \quad \Rightarrow \quad \{p\}\ \pi\ \{q\}$

d.h. für deterministische Programme impliziert totale Korrektheit bzgl. eines Paars aus Vor- und Nachbedingung auch partielle Korrektheit bzgl. dieses Paars aus Vor- und Nachbedingung.

Bew. part. Korrektheit: Fakultät (1)

- Die unmittelbare baumartige Notation von Hoareschen Korrektheitsbeweisen ist i.a. unhandlich.
- Alternativ hat sich deshalb eine Notationsvariante eingebürgert, bei der in den Programmtext Zusicherungen als Annotationen eingestreut werden.
- In der Folge demonstrieren wir diesen Notationsstil am Beispiel des Nachweises der partiellen Korrektheit unseres Fakultätsprogramms bezüglich der angegebenen Vor- und Nachbedingung. Man spricht auch von einem sog. *linearen Beweis*.

Bew. part. Korrektheit: Fakultät (2)

Beweise, dass das Hoare-Tripel

$$\{a > 0\}$$
$$x := a;\ \ y := 1;\ \ \text{while } x > 1 \text{ do } y := y * x; x := x - 1 \text{ od}$$
$$\{y = a!\}$$

gültig ist im Sinne partieller Korrektheit.

Wir entwickeln den Beweis in der Folge Schritt für Schritt!

Bew. part. Korrektheit: Fakultät (3)

Schritt 1

“*Träumen*” der Invariante...

- $\{y * x! = a! \land x > 0\}$

...um die [while]-Regel anwenden zu können.

Bew. part. Korrektheit: Fakultät (4)

Schritt 2

Behandlung des Rumpfs der while-Schleife...

Der Nachweis der Gültigkeit von

$$\begin{gathered}\{y * x! = a! \wedge x > 0 \wedge x > 1\} \\ y := y * x; \\ x := x - 1; \\ \{y * x! = a! \wedge x > 0\}\end{gathered}$$

erlaubte mithilfe der [while]-Regel den Übergang zu:

$$\begin{gathered}\{y * x! = a! \wedge x > 0\} \\ \text{while } x > 1 \text{ do} \\ \{y * x! = a! \wedge x > 0 \wedge x > 1\} \\ y := y * x; \\ x := x - 1; \\ \{y * x! = a! \wedge x > 0\} \\ \text{od [while]} \\ \{y * x! = a! \wedge x > 0 \wedge \neg(x > 1)\}\end{gathered}$$

Bew. part. Korrektheit: Fakultät (5)

Behandlung des Rumpfs der while-Schleife im Detail:

$$\{y * x! = a! \wedge x > 0 \wedge x > 1\}$$

$$y := y * x;$$
$$x := x - 1;$$
$$\{y * x! = a! \wedge x > 0\}$$

Bew. part. Korrektheit: Fakultät (6)

Wegen *Rückwärts*zuweisungsregel wird der Rumpf der while-Schleife von hinten nach vorne bearbeitet:

$$\{y * x! = a! \wedge x > 0 \wedge x > 1\}$$

$$y := y * x;$$

$$\{y * (x-1)! = a! \wedge x - 1 > 0\}$$

$$x := x - 1; \text{ [ass]}$$

$$\{y * x! = a! \wedge x > 0\}$$

Bew. part. Korrektheit: Fakultät (7)

Nach abermaliger Anwendung der [ass]-Regel erhalten wir...

$$\{y * x! = a! \wedge x > 0 \wedge x > 1\}$$

$$\{(y * x) * (x - 1)! = a! \wedge x - 1 > 0\}$$

$$y := y * x; \text{ [ass]}$$

$$\{y * (x - 1)! = a! \wedge x - 1 > 0\}$$

$$x := x - 1; \text{ [ass]}$$

$$\{y * x! = a! \wedge x > 0\}$$

...wobei noch eine "Beweislücke" verbleibt!

Bew. part. Korrektheit: Fakultät (8)

Schluss der “Beweislücke” in der zugrundeliegenden Theorie:

$$\{y * x! = a! \wedge x > 0 \wedge x > 1\}$$

$$\Downarrow \text{[cons]}$$

$$\{(y * x) * (x - 1)! = a! \wedge x - 1 > 0\}$$

$$y := y * x; \text{ [ass]}$$

$$\{y * (x - 1)! = a! \wedge x - 1 > 0\}$$

$$x := x - 1; \text{ [ass]}$$

$$\{y * x! = a! \wedge x > 0\}$$

Bew. part. Korrektheit: Fakultät (9)

Anwendung der [while]-Regel liefert nun wie gewünscht:

$$
\begin{gathered}
\{y * x! = a! \wedge x > 0\} \\
\text{while } x > 1 \text{ do} \\
\{y * x! = a! \wedge x > 0 \wedge x > 1\} \\
\Downarrow \text{[cons]} \\
\{(y * x) * (x-1)! = a! \wedge x - 1 > 0\} \\
y := y * x; \text{ [ass]} \\
\{y * (x-1)! = a! \wedge x - 1 > 0\} \\
x := x - 1; \text{ [ass]} \\
\{y * x! = a! \wedge x > 0\} \\
\text{od [while]} \\
\{y * x! = a! \wedge x > 0 \wedge \neg(x > 1)\}
\end{gathered}
$$

Bew. part. Korrektheit: Fakultät (10)

Schritt 3

Zur gewünschten Nachbedingung verbleibt offenbar ebenfalls eine Beweislücke:

$$\{y * x! = a! \land x > 0\}$$
$$\text{while } x > 1 \text{ do}$$
$$\{y * x! = a! \land x > 0 \land x > 1\}$$
$$\Downarrow \text{[cons]}$$
$$\{(y * x) * (x - 1)! = a! \land x - 1 > 0\}$$
$$y := y * x; \text{ [ass]}$$
$$\{y * (x - 1)! = a! \land x - 1 > 0\}$$
$$x := x - 1; \text{ [ass]}$$
$$\{y * x! = a! \land x > 0\}$$
$$\text{od [while]}$$
$$\{y * x! = a! \land x > 0 \land \neg(x > 1)\}$$

$$\{y = a!\}$$

Bew. part. Korrektheit: Fakultät (11)

Schluss der Beweislücke in der zugrundeliegenden Theorie:

$$\{y * x! = a! \wedge x > 0\}$$
$$\text{while } x > 1 \text{ do}$$
$$\{y * x! = a! \wedge x > 0 \wedge x > 1\}$$
$$\Downarrow \text{[cons]}$$
$$\{(y * x) * (x - 1)! = a! \wedge x - 1 > 0\}$$
$$y := y * x; \text{ [ass]}$$
$$\{y * (x - 1)! = a! \wedge x - 1 > 0\}$$
$$x := x - 1; \text{ [ass]}$$
$$\{y * x! = a! \wedge x > 0\}$$
$$\text{od [while]}$$
$$\{y * x! = a! \wedge x > 0 \wedge \neg(x > 1)\}$$
$$\Downarrow \text{[cons]}$$
$$\{y * x! = a! \wedge x > 0 \wedge x \leq 1\}$$
$$\Downarrow \text{[cons]}$$
$$\{y * x! = a! \wedge x = 1\}$$
$$\Downarrow \text{[cons]}$$
$$\{y = a!\}$$

Bew. part. Korrektheit: Fakultät (12)

Aus Platzgründen etwas verkürzt dargestellt:

$$\{y * x! = a! \wedge x > 0\}$$
$$\text{while } x > 1 \text{ do}$$
$$\{y * x! = a! \wedge x > 0 \wedge x > 1\}$$
$$\Downarrow \text{[cons]}$$
$$\{(y * x) * (x - 1)! = a! \wedge x - 1 > 0\}$$
$$y := y * x; \text{ [ass]}$$
$$\{y * (x - 1)! = a! \wedge x - 1 > 0\}$$
$$x := x - 1; \text{ [ass]}$$
$$\{y * x! = a! \wedge x > 0\}$$
$$\text{od [while]}$$
$$\{y * x! = a! \wedge x > 0 \wedge \neg(x > 1)\}$$
$$\Downarrow \text{[cons]}$$
$$\{y = a!\}$$

Bew. part. Korrektheit: Fakultät (13)

Schritt 4

Es verbleibt, die Beweislücke zur gewünschten Vorbedingung zu schließen:

$$\{a > 0\}$$

$$
\begin{gathered}
x := a; \\
y := 1; \\
\{y * x! = a! \wedge x > 0\} \\
\text{while } x > 1 \text{ do} \\
\{y * x! = a! \wedge x > 0 \wedge x > 1\} \\
\Downarrow \text{[cons]} \\
\{(y * x) * (x-1)! = a! \wedge x - 1 > 0\} \\
y := y * x; \text{ [ass]} \\
\{y * (x-1)! = a! \wedge x - 1 > 0\} \\
x := x - 1; \text{ [ass]} \\
\{y * x! = a! \wedge x > 0\} \\
\text{od [while]} \\
\{y * x! = a! \wedge x > 0 \wedge \neg(x > 1)\} \\
\Downarrow \text{[cons]} \\
\{y = a!\}
\end{gathered}
$$

Bew. part. Korrektheit: Fakultät (14)

Einmalige Anwendung der [ass]-Regel liefert:

$$\{a > 0\}$$

$$x := a;$$
$$\{1 * x! = a! \land x > 0\}$$
$$y := 1; \text{ [ass]}$$
$$\{y * x! = a! \land x > 0\}$$
$$\text{while } x > 1 \text{ do}$$
$$\{y * x! = a! \land x > 0 \land x > 1\}$$
$$\Downarrow \text{ [cons]}$$
$$\{(y * x) * (x - 1)! = a! \land x - 1 > 0\}$$
$$y := y * x; \text{ [ass]}$$
$$\{y * (x - 1)! = a! \land x - 1 > 0\}$$
$$x := x - 1; \text{ [ass]}$$
$$\{y * x! = a! \land x > 0\}$$
$$\text{od [while]}$$
$$\{y * x! = a! \land x > 0 \land \neg(x > 1)\}$$
$$\Downarrow \text{ [cons]}$$
$$\{y = a!\}$$

Bew. part. Korrektheit: Fakultät (15)

Abermalige Anwendung der [ass]-Regel liefert:

$$\{a > 0\}$$

$$\{1 * a! = a! \wedge a > 0\}$$
$$x := a;\ \text{[ass]}$$
$$\{1 * x! = a! \wedge x > 0\}$$
$$y := 1;\ \text{[ass]}$$
$$\{y * x! = a! \wedge x > 0\}$$
$$\text{while } x > 1 \text{ do}$$
$$\{y * x! = a! \wedge x > 0 \wedge x > 1\}$$
$$\Downarrow \text{[cons]}$$
$$\{(y * x) * (x - 1)! = a! \wedge x - 1 > 0\}$$
$$y := y * x;\ \text{[ass]}$$
$$\{y * (x - 1)! = a! \wedge x - 1 > 0\}$$
$$x := x - 1;\ \text{[ass]}$$
$$\{y * x! = a! \wedge x > 0\}$$
$$\text{od [while]}$$
$$\{y * x! = a! \wedge x > 0 \wedge \neg(x > 1)\}$$
$$\Downarrow \text{[cons]}$$
$$\{y = a!\}$$

Bew. part. Korrektheit: Fakultät (16)

Schluss der letzten Beweislücke in der zugrundeliegenden Theorie:

$$
\begin{array}{c}
\{a > 0\} \\
\Downarrow \text{[cons]} \\
\{1 * a! = a! \wedge a > 0\} \\
x := a;\ \text{[ass]} \\
\{1 * x! = a! \wedge x > 0\} \\
y := 1;\ \text{[ass]} \\
\{y * x! = a! \wedge x > 0\} \\
\text{while } x > 1 \text{ do} \\
\{y * x! = a! \wedge x > 0 \wedge x > 1\} \\
\Downarrow \text{[cons]} \\
\{(y * x) * (x-1)! = a! \wedge x - 1 > 0\} \\
y := y * x;\ \text{[ass]} \\
\{y * (x-1)! = a! \wedge x - 1 > 0\} \\
x := x - 1;\ \text{[ass]} \\
\{y * x! = a! \wedge x > 0\} \\
\text{od [while]} \\
\{y * x! = a! \wedge x > 0 \wedge \neg(x > 1)\} \\
\Downarrow \text{[cons]} \\
\{y = a!\}
\end{array}
$$

Überblick (17)

$$\{a > 0\}$$
$$\Downarrow \text{[cons]}$$
$$\{1 * a! = a! \wedge a > 0\}$$
$$x := a; \text{ [ass]}$$
$$\{1 * x! = a! \wedge x > 0\}$$
$$y := 1; \text{ [ass]}$$
$$\{y * x! = a! \wedge x > 0\}$$
$$\text{while } x > 1 \text{ do}$$
$$\{y * x! = a! \wedge x > 0 \wedge x > 1\}$$
$$\Downarrow \text{[cons]}$$
$$\{(y * x) * (x - 1)! = a! \wedge x - 1 > 0\}$$
$$y := y * x; \text{ [ass]}$$
$$\{y * (x - 1)! = a! \wedge x - 1 > 0\}$$
$$x := x - 1; \text{ [ass]}$$
$$\{y * x! = a! \wedge x > 0\}$$
$$\text{od [while]}$$
$$\{y * x! = a! \wedge x > 0 \wedge \neg(x > 1)\}$$
$$\Downarrow \text{[cons]}$$
$$\{y * x! = a! \wedge x > 0 \wedge x \leq 1\}$$
$$\Downarrow \text{[cons]}$$
$$\{y * x! = a! \wedge x = 1\}$$
$$\Downarrow \text{[cons]}$$
$$\{y = a!\}$$

Bew. part. Korrektheit: Fakultät (18)

Damit haben wir insgesamt wie gewünscht gezeigt:

Das Hoaresche Tripel

$$\{a > 0\}$$
$$x := a;\ \ y := 1;\ \ \text{while } x > 1 \text{ do } y := y * x; x := x - 1 \text{ od}$$
$$\{y = a!\}$$

ist gültig im Sinne partieller Korrektheit.

Linearer vs. baumartiger Beweis

Vorteil linearer gegenüber baumartigen Beweisnotationsstils:

- wenig Redundanz
- daher insgesamt knappere Beweise

Schwächste Vor- und stärkste Nachbedingungen

...noch einmal anders betrachtet:

Definition

Seien A, B, A_1, A_2, ... (logische) Formeln

- A heißt *schwächer* als B, wenn gilt: $B \Rightarrow A$
- A_i heißt *schwächste* Formel in $\{A_1, A_2, \ldots\}$, wenn gilt: $A_j \Rightarrow A_i$ für alle j.

Schwächste Vorbedingungen

Definition

Sei π ein Programm und q eine Formel.

Dann heißt

- $wp(\pi, q)$ *schwächste Vorbedingung* für totale Korrektheit von π bezüglich (der Nachbedingung) q, wenn

  $$[wp(\pi, q)]\ \pi\ [q]$$

  total korrekt ist und $wp(\pi, q)$ die schwächste Formel mit dieser Eigenschaft ist.

- $wlp(\pi, q)$ *schwächste liberale Vorbedingung* für partielle Korrektheit von π bezüglich (der Nachbedingung) q, wenn

  $$\{wlp(\pi, q)\}\ \pi\ \{q\}$$

  partiell korrekt ist und $wlp(\pi, q)$ die schwächste Formel mit dieser Eigenschaft ist.

Stärkste Nachbedingungen (1)

Analog zu A ist *schwächer* als B lässt sich definieren:

- A heißt *stärker* als B, wenn gilt: B ist schwächer als A, d.h. wenn gilt: $A \Rightarrow B$
- A_i heißt *stärkste* Formel in $\{A_1, A_2, \ldots\}$, wenn gilt: $A_i \Rightarrow A_j$ für alle j.

Zum Überlegen:

Ist es sinnvoll, analog zum Begriff der schwächsten (liberalen) Vorbedingung $wp(\pi, q)$ bzw. $wlp(\pi, q)$ auch den Begriff der stärksten (liberalen) Nachbedingung $spo(p, \pi)$ bzw. $slpo(p, \pi)$ zu gegebenem Programm π und Vorbedingung p zu betrachten?

Stärkste Nachbedingungen (2)

Betrachte...

Definition

Sei π ein Programm und p eine Formel.

Dann heißt

- $spo(p, \pi)$ *stärkste Nachbedingung* für totale Korrektheit von π bezüglich (der Vorbedingung) p, wenn
$$[p]\ \pi\ [spo(p, \pi)]$$
total korrekt ist und $spo(p, \pi)$ die stärkste Formel mit dieser Eigenschaft ist.

- $slpo(p, \pi)$ *stärkste liberale Nachbedingung* für partielle Korrektheit von π bezüglich (der Vorbedingung) p, wenn
$$\{p\}\ \pi\ \{slpo(p, \pi)\}$$
partiell korrekt ist und $slpo(p, \pi)$ die stärkste Formel mit dieser Eigenschaft ist.

Stärkste Nachbedingungen (3)

Fragen

- Gibt es Programme π und Formeln p derart, dass
  - $spo(p, \pi)$
  - $slpo(p, \pi)$

  unterscheidbar, d.h. logisch nicht äquivalent sind?

- Wie passen die hier betrachteten Begriffe von schwächsten Vor- und stärksten Nachbedingungen mit denen auf Folie 13 von diesem Vorlesungsteil betrachteten zusammen?

Vorschau auf die nächsten Vorlesungstermine...

- *Mo, 07.11.2005: Keine Vorlesung!*
- Mo, 14.11.2005, Vorlesung von 16:15 Uhr bis 17:45 Uhr im Eckert-Hörsaal
- Mo, 21.11.2005, Vorlesung von 16:15 Uhr bis 17:45 Uhr im Eckert-Hörsaal
- Mo, 28.11.2005, Vorlesung von 16:15 Uhr bis 17:45 Uhr im Eckert-Hörsaal