

---

# Axiomatische Semantik von WHILE

**Insbesondere:** ...Korrektheit und Vollständigkeit der axiomatischen Semantik

## Erinnerung:

- *Hoare-Tripel* (syntaktische Sicht) bzw. *Korrektheitsformeln* (semantische Sicht) der Form

$$\{p\} \pi \{q\} \quad \text{bzw.} \quad [p] \pi [q]$$

- Gültigkeit einer Korrektheitsformel im Sinne
  - *partieller* Korrektheit
  - *totaler* Korrektheit

---

# 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  $\sigma$  gilt: ist die Vorbedingung  $p$  in  $\sigma$  erfüllt **und** terminiert die zugehörige Berechnung von  $\pi$  angesetzt auf  $\sigma$  regulär in einem Endzustand  $\sigma'$ , **dann** ist auch die Nachbedingung  $q$  in  $\sigma'$  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  $\sigma$  gilt: ist die Vorbedingung  $p$  in  $\sigma$  erfüllt, **dann** terminiert die zugehörige Berechnung von  $\pi$  angesetzt auf  $\sigma$  regulär mit einem Endzustand  $\sigma'$  **und** die Nachbedingung  $q$  ist in  $\sigma'$  erfüllt.

---

# Intuitiv

“Totale Korrektheit = Partielle Korrektheit + Terminierung”

---

# Partielle und totale Korrektheit

- Die Zustandsmenge

$$Ch(p) =_{df} \{ \sigma \in \Sigma \mid \llbracket p \rrbracket_B(\sigma) = \text{tt} \}$$

heißt *Charakterisierung* von  $p \in \mathbf{Bexp}$ .

- *Semantik von Korrektheitsformeln:*

Eine Korrektheitsformel  $\{p\} \pi \{q\}$  heißt

- *partiell korrekt* (in Zeichen:  $\models_{pk} \{p\} \pi \{q\}$ ), falls  $\llbracket \pi \rrbracket(Ch(p)) \subseteq Ch(q)$
- *total korrekt* (in Zeichen:  $\models_{tk} \{p\} \pi \{q\}$ ), falls  $\{p\} \pi \{q\}$  partiell korrekt ist und  $Def(\llbracket \pi \rrbracket) \supseteq Ch(p)$  gilt. Dabei bezeichnet  $Def(\llbracket \pi \rrbracket)$  die Menge aller Zustände, für die  $\pi$  regulär terminiert.

*Konvention:*  $\llbracket \pi \rrbracket(Ch(p)) =_{df} \{ \llbracket \pi \rrbracket(\sigma) \mid \sigma \in Ch(p) \}$

---

# Erinnerung

...an einige Sprechweisen:

Ein (deterministisches) Programm  $\pi$

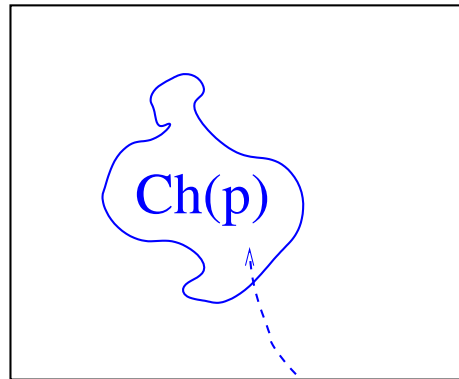
- angesetzt auf einen Anfangszustand  $\sigma$  *terminiert regulär* gdw.  $\pi$  nach endlich vielen Schritten in einem Zustand  $\sigma' \in \Sigma$  endet.
- angesetzt auf einen Anfangszustand  $\sigma$  *terminiert irregulär* gdw.  $\pi$  nach endlich vielen Schritten zur Konfiguration *undef* führt.
- Ein Programm  $\pi$  heißt *divergent* gdw.  $\pi$  terminiert für keinen Anfangszustand regulär.

---

# Veranschaulichung (1)

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

Menge aller Zustände  $\Sigma$



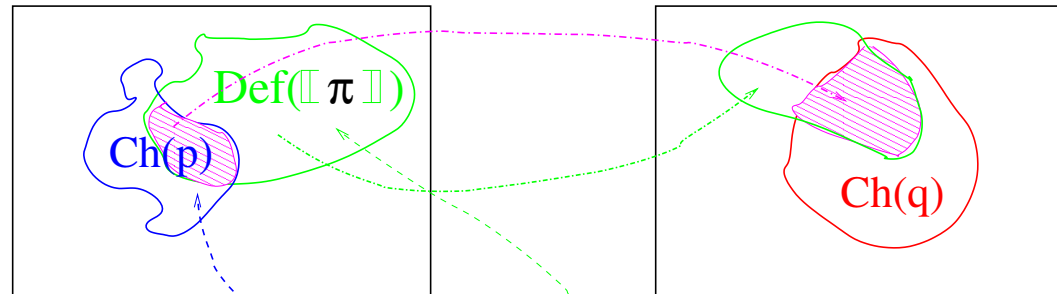
Charakterisierung von  $p$ :  $Ch(p) \subseteq \Sigma$

---

# Veranschaulichung (2)

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

Menge aller Zustände  $\Sigma$



Charakterisierung von  $p$ :  $\text{Ch}(p) \subseteq \Sigma$

Definitionsbereich von  $\pi$  :  $\text{Def}(\llbracket \pi \rrbracket) \subseteq \Sigma$

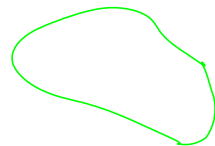


Bild von  $\llbracket \pi \rrbracket$  für  $\text{Def}(\llbracket \pi \rrbracket)$

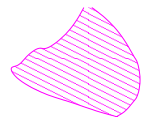


Bild von  $\llbracket \pi \rrbracket$  für  $\text{Def}(\llbracket \pi \rrbracket) \cap \text{Ch}(p)$

---

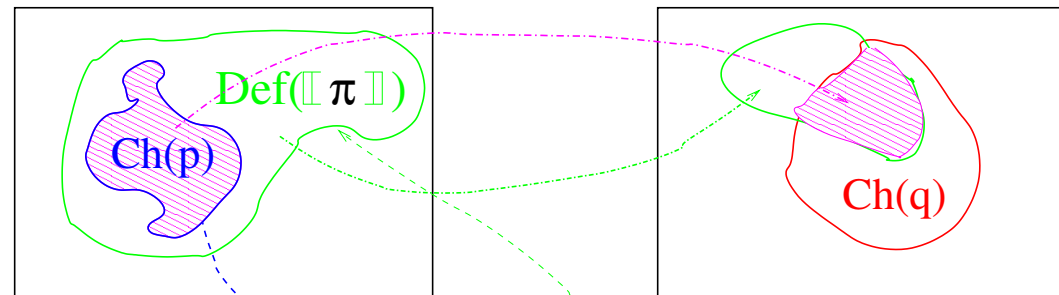


---

# Veranschaulichung (3)

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

Menge aller Zustände  $\Sigma$



Charakterisierung von  $p$ :  $Ch(p) \subseteq \Sigma$

Definitionsbereich von  $\pi$ :  $Def(\llbracket \pi \rrbracket) \subseteq \Sigma$

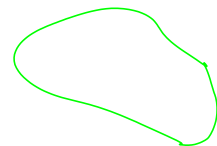


Bild von  $\llbracket \pi \rrbracket$  für  $Def(\llbracket \pi \rrbracket)$

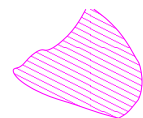


Bild von  $\llbracket \pi \rrbracket$  für  $Def(\llbracket \pi \rrbracket) \cap Ch(p)$

---

---

# Hoare-Kalkül $HK_{PK}$ für partielle Korrektheit

$$[\text{skip}] \frac{}{\{p\} \text{skip} \{p\}}$$

$$[\text{abort}] \frac{}{\{p\} \text{abort} \{q\}}$$

$$[\text{ass}] \frac{}{\{p[t \setminus x]\} x := t \{p\}}$$

$$[\text{comp}] \frac{\{p\} \pi_1 \{r\}, \{r\} \pi_2 \{q\}}{\{p\} \pi_1; \pi_2 \{q\}}$$

$$[\text{ite}] \frac{\{p \wedge b\} \pi_1 \{q\}, \{p \wedge \neg b\} \pi_2 \{q\}}{\{p\} \text{if } b \text{ then } \pi_1 \text{ else } \pi_2 \text{ fi } \{q\}}$$

$$[\text{while}] \frac{\{I \wedge b\} \pi \{I\}}{\{I\} \text{while } b \text{ do } \pi \text{ od } \{I \wedge \neg b\}}$$

$$[\text{cons}] \frac{p \Rightarrow p_1, \{p_1\} \pi \{q_1\}, q_1 \Rightarrow q}{\{p\} \pi \{q\}}$$

---

# Hoare-Kalkül $HK_{TK}$ für totale Korrektheit

...identisch mit  $HK_{PK}$ , wobei aber Regel [while] ersetzt ist durch:

$$[\text{while}_{TK}] \frac{I \wedge b \Rightarrow u[t/v], \{I \wedge b \wedge t=w\} \pi \{I \wedge t < w\}}{\{I\} \text{ while } b \text{ do } \pi \text{ od } \{I \wedge \neg b\}}$$

wobei

- $u$  Boolescher Ausdruck über der Variablen  $v$ ,
- $t$  Term,
- $w$  Variable, die in  $I$ ,  $b$ ,  $\pi$  und  $t$  nicht frei vorkommt,
- $M =_{df} \{\sigma(v) \mid \sigma \in \Sigma \wedge \llbracket u \rrbracket_B(\sigma) = \text{tt}\}$  noethersch geordnete Menge (sog. noethersche Halbordnung).

---

# Korrektheit und Vollständigkeit von $HK_{PK}$ und $HK_{TK}$

Sei  $K$  ein Kalkül für partielle bzw. totale Korrektheit

Zentral sind dann die Fragen der...

- *Korrektheit*: ...ist jede mithilfe von  $K$  ableitbare Korrektheitsformel partiell bzw. total korrekt?
- *Vollständigkeit*: ...ist jede partiell bzw. total korrekte Korrektheitsformel mithilfe von  $K$  ableitbar?

## Speziell:

- Sind  $HK_{PK}$  und  $HK_{TK}$  korrekt und vollständig?

---

# Hauptresultate

**Zur Korrektheit:**

**Theorem [Korrektheit von  $HK_{PK}$  und  $HK_{TK}$ ]**

1.  $HK_{PK}$  ist korrekt, d.h. jede mit  $HK_{PK}$  ableitbare Korrektheitsformel ist gültig im Sinne partieller Korrektheit.
2.  $HK_{TK}$  ist korrekt, d.h. jede mit  $HK_{TK}$  ableitbare Korrektheitsformel ist gültig im Sinne totaler Korrektheit.

**Beweis** ...durch Induktion über die Anzahl der Regelanwendungen im Beweisbaum zur Ableitung der Korrektheitsformel.

**Zur Vollständigkeit:**

Für Korrektheitskalküle ist i.a. nur sog. *relative* Vollständigkeit beweisbar. Das gilt auch für  $HK_{PK}$  und  $HK_{TK}$ . Details dazu später.

---

---

## Beispiele 1(2)

...Beweis partieller Korrektheit von Hoareschen Zusicherungen anhand zweier Programme zur Berechnung

- der Fakultät und
- der ganzzahligen Division mit Rest

---

## Beispiele 2(2)

Im Detail:

*Beweise, dass die beiden Hoareschen Zusicherungen*

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

und

$$\begin{array}{c} \{x \geq 0 \wedge y > 0\} \\ q := 0; r := x; \text{ while } r \geq y \text{ do } q := q + 1; r := r - y \text{ od} \\ \{x = q * y + r \wedge 0 \leq r < y\} \end{array}$$

*gültig sind im Sinne partieller Korrektheit.*

In der Folge geben wir die Beweise dafür in baumartiger Notation an...

# Bew. part. Korrektheit: Fakultät (1)

Erster Beweis

$$\begin{array}{c}
 \frac{}{} \\
 \frac{}{} \text{Ass} \quad \frac{}{} \text{Ass} \\
 \frac{\{(y*x)^{(x-1)}!=a! \ \& \ (x-1)>0\} \ y:=y*x \ \{(y^{(x-1)}!=a! \ \& \ (x-1)>0\}}{\{(y*x)^{(x-1)}!=a! \ \& \ (x-1)>0\}} \text{Comp} \\
 \frac{y*x!=a! \ \& \ x>0 \ \& \ x>1 \implies (y*x)^{(x-1)}!=a! \ \& \ (x-1)>0 \quad \{(y*x)^{(x-1)}!=a! \ \& \ (x-1)>0\} \ y:=y*x; \ x:=x-1 \ \{y*x!=a! \ \& \ x>0\}}{y*x!=a! \ \& \ x>0 \ \& \ x>1} \text{Cons} \\
 \frac{\{(y*x!=a! \ \& \ x>0 \ \& \ x>1\} \ y:=y*x; \ x:=x-1 \ \{y*x!=a! \ \& \ x>0\}}{\{(y*x!=a! \ \& \ x>0\} \ \text{WHILE } x>1 \ \text{DO } y:=y*x; \ x:=x-1 \ \text{OD } \{y*x!=a! \ \& \ x>0 \ \& \ \sim(x>1)\}} \text{While} \\
 \frac{\{(y*x!=a! \ \& \ x>0\} \ \text{WHILE } x>1 \ \text{DO } y:=y*x; \ x:=x-1 \ \text{OD } \{y*a!\}}{\{(y*x!=a! \ \& \ x>0\} \ \text{WHILE } x>1 \ \text{DO } y:=y*x; \ x:=x-1 \ \text{OD } \{y*a!\}} \text{Comp} \\
 \frac{\{a>0\} \ x:=a; \ y:=1 \ \{y*x!=a! \ \& \ x>0\}}{\{a>0\} \ x:=a; \ y:=1; \ \text{WHILE } x>1 \ \text{DO } y:=y*x; \ x:=x-1 \ \text{OD } \{y*a!\}} \text{Comp}
 \end{array}$$

wobei

$$\mathbf{T} \equiv \left\{ \frac{\frac{\{1*a!=a! \ \& \ a>0 \ \& \ a=a\} \ x:=a \ \{1*x!=a! \ \& \ a>0 \ \& \ x=a\}}{\{1*a!=a! \ \& \ a>0 \ \& \ a=a\} \ x:=a; \ y:=1 \ \{y*x!=a! \ \& \ a>0 \ \& \ x=a\}} \text{Ass} \quad \frac{\{1*x!=a! \ \& \ a>0 \ \& \ x=a\} \ y:=1 \ \{y*x!=a! \ \& \ a>0 \ \& \ x=a\}}{\{1*x!=a! \ \& \ a>0 \ \& \ x=a\}} \text{Ass} \\
 \frac{a>0 \implies 1*a!=a! \ \& \ a>0 \ \& \ a=a \quad \{1*a!=a! \ \& \ a>0 \ \& \ a=a\} \ x:=a; \ y:=1 \ \{y*x!=a! \ \& \ a>0 \ \& \ x=a\} \quad y*x!=a! \ \& \ a>0 \ \& \ x=a \implies y*x!=a! \ \& \ x>0}{\{a>0\} \ x:=a; \ y:=1 \ \{y*x!=a! \ \& \ x>0\}} \text{Comp} \\
 \text{Cons}
 \end{array}$$

& : Logisches und  
 ~ : Logisches nicht



# Bew. part. Korrektheit: Fakultät (2)

Zweiter Beweis

$$\begin{array}{c}
 \frac{}{} \\
 \frac{}{} \text{Ass} \quad \frac{}{} \text{Ass} \\
 \frac{\{(y*x)^*(x-1)!=a! \ \& \ (x-1)>0\} \ y:=y*x \ \{y*(x-1)!=a! \ \& \ (x-1)>0\}}{\{y*(x-1)!=a! \ \& \ (x-1)>0\} \ x:=x-1 \ \{y*x!=a! \ \& \ x>0\}} \text{Ass} \\
 \frac{y*x!=a! \ \& \ x>0 \ \& \ x>1 \implies (y*x)^*(x-1)!=a! \ \& \ (x-1)>0 \quad \{(y*x)^*(x-1)!=a! \ \& \ (x-1)>0\} \ y:=y*x; \ x:=x-1 \ \{y*x!=a! \ \& \ x>0\}}{y*x!=a! \ \& \ x>0 \ \& \ x>1} \text{Comp} \\
 \frac{\{y*x!=a! \ \& \ x>0 \ \& \ x>1\} \ y:=y*x; \ x:=x-1 \ \{y*x!=a! \ \& \ x>0\}}{\{y*x!=a! \ \& \ x>0\} \ \text{WHILE } x>1 \ \text{DO } y:=y*x; \ x:=x-1 \ \text{OD } \{y*x!=a! \ \& \ x>0 \ \& \ \sim(x>1)\}} \text{While} \\
 \frac{\{a>0\} \ x:=a; \ y:=1 \ \{y*x!=a! \ \& \ x>0\}}{\{y*x!=a! \ \& \ x>0\} \ \text{WHILE } x>1 \ \text{DO } y:=y*x; \ x:=x-1 \ \text{OD } \{y=a!\}} \text{Cons} \\
 \frac{\{a>0\} \ x:=a; \ y:=1 \ \{y*x!=a! \ \& \ x>0\}}{\{a>0\} \ x:=a; \ y:=1; \ \text{WHILE } x>1 \ \text{DO } y:=y*x; \ x:=x-1 \ \text{OD } \{y=a!\}} \text{Comp}
 \end{array}$$

wobei

$$\mathbf{T}^I \equiv \left\{ \begin{array}{c}
 \frac{}{} \text{Ass} \quad \frac{}{} \text{Ass} \\
 \frac{\{1*a!=a! \ \& \ a>0\} \ x:=a \ \{1*x!=a! \ \& \ x>0\}}{\{1*x!=a! \ \& \ x>0\} \ y:=1 \ \{y*x!=a! \ \& \ x>0\}} \text{Ass} \\
 \frac{a>0 \implies 1*a!=a! \ \& \ a>0 \quad \{1*a!=a! \ \& \ a>0\} \ x:=a; \ y:=1 \ \{y*x!=a! \ \& \ x>0\}}{\{a>0\} \ x:=a; \ y:=1 \ \{y*x!=a! \ \& \ x>0\}} \text{Comp} \\
 \text{Cons}
 \end{array} \right.$$

& : Logisches und  
 ~ : Logisches nicht

# Bew. partieller Korrektheit: Division

	Ass		Ass
	$\{x=(q+1)*y+r-y \ \& \ r-y \geq 0\} \ q:=q+1 \ \{x=q*y+r-y \ \& \ r-y \geq 0\} \ \{x=q*y+r-y \ \& \ r-y \geq 0\} \ r:=r-y \ \{x=q*y+r \ \& \ r \geq 0\}$		
<b>Comp</b>			
	$(x=q*y+r \ \& \ r \geq 0 \ \& \ r > y) \Rightarrow (x=(q+1)*y+r-y \ \& \ r-y \geq 0) \ \{x=(q+1)*y+r-y \ \& \ r-y \geq 0\} \ q:=q+1; \ r:=r-y \ \{x=q*y+r \ \& \ r \geq 0\}$		
<b>Cons</b>			
	$\{x=q*y+r \ \& \ r \geq 0 \ \& \ r > y\} \ q:=q+1; \ r:=r-y \ \{x=q*y+r \ \& \ r \geq 0\}$		
<b>While</b>			
	$\{x=q*y+r \ \& \ r \geq 0\} \ \text{WHILE } r > y \ \text{DO } q:=q+1; \ r:=r-y \ \text{OD } \{x=q*y+r \ \& \ r \geq 0 \ \& \ \sim(r > y)\} \ (x=q*y+r \ \& \ r \geq 0 \ \& \ \sim(r > y)) \Rightarrow (x=q*y+r \ \& \ r \geq 0 \ \& \ r < y)$		
<b>Cons</b>			

	Ass		Ass
	$\{x=0*y+x \ \& \ x > 0\} \ q:=0 \ \{x=q*y+x \ \& \ x > 0\} \ \{x=q*y+x \ \& \ x > 0\} \ r:=x \ \{x=q*y+r \ \& \ r \geq 0\}$		
	$(x > 0 \ \& \ y > 0) \Rightarrow (x=0*y+x \ \& \ x > 0) \ \{x=0*y+x \ \& \ x > 0\} \ q:=0; \ r:=x \ \{x=q*y+r \ \& \ r \geq 0\}$		
	<b>Comp</b>		
	<b>Cons</b>		
	$\{x > 0 \ \& \ y > 0\} \ q:=0; \ r:=x \ \{x=q*y+r \ \& \ r \geq 0\}$	$\{x=q*y+r \ \& \ r \geq 0\} \ \text{WHILE } r > y \ \text{DO } q:=q+1; \ r:=r-y \ \text{OD } \{x=q*y+r \ \& \ r \geq 0 \ \& \ r < y\}$	
	$\{x > 0 \ \& \ y > 0\} \ q:=0; \ r:=x; \ \text{WHILE } r > y \ \text{DO } q:=q+1; \ r:=r-y \ \text{OD } \{x=q*y+r \ \& \ r \geq 0 \ \& \ r < y\}$		
		<b>Comp</b>	

& : Logisches und  
 ~ : Logisches nicht

---

# 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* bzw. *linearen Beweisskizze*.

---

## 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...

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

...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

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

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

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

---

## 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 *Rückwärtszuweisungsregel* 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:

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

↓ [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:

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

---

# Bew. part. Korrektheit: Fakultät (10)

## Schritt 3

Zur gewünschten Nachbedingung verbleibt offenbar ebenfalls eine Beweislücke:

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

---

# Bew. part. Korrektheit: Fakultät (11)

Schluss der Beweislücke in der zugrundeliegenden Theorie:

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

---

## Bew. part. Korrektheit: Fakultät (12)

Aus Platzgründen etwas verkürzt dargestellt:

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

---

# Bew. part. Korrektheit: Fakultät (13)

## Schritt 4

Es verbleibt, die Beweislücke zur gewünschten Vorbedingung zu schließen:

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

---

# Bew. part. Korrektheit: Fakultät (14)

Einmalige Anwendung der [ass]-Regel liefert:

$$\{a > 0\}$$

$$x := a;$$

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

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

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

while  $x > 1$  do

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

↓ [cons]

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

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

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

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

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

od [while]

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

↓ [cons]

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



---

# Bew. part. Korrektheit: Fakultät (15)

Abermalige Anwendung der [ass]-Regel liefert:

$$\{a > 0\}$$

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

$x := a$ ; [ass]

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

$y := 1$ ; [ass]

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

while  $x > 1$  do

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

↓ [cons]

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

$y := y * x$ ; [ass]

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

$x := x - 1$ ; [ass]

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

od [while]

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

↓ [cons]

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

---

## Bew. part. Korrektheit: Fakultät (16)

Schluss der letzten Beweislücke in der zugrundeliegenden Theorie:

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

---

# Überblick (17)

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

---

## Bew. part. Korrektheit: Fakultät (18)

Damit haben wir insgesamt wie gewünscht gezeigt:

Das Hoaresche Tripel

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

ist gültig im Sinne partieller Korrektheit.

---

# Linearer vs. baumartiger Beweisstil

Vorteil linearen gegenüber baumartigen Beweisnotationsstils:

- wenig Redundanz
- daher insgesamt knappere Beweise

---

# 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
- $\pi$  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:

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

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

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

*...zum Ausdruck totaler Korrektheit von  $\pi$  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 *Korrektivformel*

betont jeweils die

- syntaktische bzw.
- semantische Sicht

auf

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