CS 512, Spring 2018, Handout 19

Hoare Logic (Continued)

Assaf Kfoury

March 20, 2018

using proof rules for PCA's (example from Handout 18)

- show $\vdash_{\text{par}} \{\top\}\, z := x;\ z := z + y;\ u := z;\ \{u = x + y\}$

using proof rules for PCA's (example from Handout 18)

- show $\vdash_{\text{par}}$ $\{\, \top \,\}\ z := x;\ z := z + y;\ u := z;\ \{\, u = x + y \,\}$

$z := x;$

$z := z + y;$

$u := z;$

using proof rules for PCA's (example from Handout 18)

- show $\vdash_{\text{par}} \; \{\, \top \,\}\; z := x;\; z := z + y;\; u := z;\; \{\, u = x + y \,\}$

$z := x;$

$z := z + y;$

$u := z;$

$$\{u = x + y\}$$

using proof rules for PCA's (example from Handout 18)

- show $\vdash_{\text{par}} \{ \top \}\ z := x;\ z := z + y;\ u := z;\ \{ u = x + y \}$

$z := x;$

$z := z + y;$

$\{z = x + y\}$ (assignment)

$u := z;$

$\{u = x + y\}$

using proof rules for PCA's (example from Handout 18)

- show $\vdash_{\text{par}} \{\top\}\ z := x;\ z := z + y;\ u := z;\ \{u = x + y\}$

$z := x;$

$\qquad \{z + y = x + y\}$ (assignment)

$z := z + y;$

$\qquad \{z = x + y\}$ (assignment)

$u := z;$

$\qquad \{u = x + y\}$

using proof rules for PCA's (example from Handout 18)

- show $\vdash_{\text{par}} \{ \top \}\ z := x;\ z := z + y;\ u := z;\ \{ u = x + y \}$

$\quad\{x + y = x + y\}$	(assignment)
$z := x;$	
$\quad\{z + y = x + y\}$	(assignment)
$z := z + y;$	
$\quad\{z = x + y\}$	(assignment)
$u := z;$	
$\quad\{u = x + y\}$	

using proof rules for PCA's (example from Handout 18)

- show $\vdash_{\text{par}} \{ \top \}\ z := x;\ z := z + y;\ u := z;\ \{ u = x + y \}$

$$
\begin{array}{ll}
\quad \{\top\} & \text{(implied)} \\
\quad \{x + y = x + y\} & \text{(assignment)} \\
z := x; & \\
\quad \{z + y = x + y\} & \text{(assignment)} \\
z := z + y; & \\
\quad \{z = x + y\} & \text{(assignment)} \\
u := z; & \\
\quad \{u = x + y\} &
\end{array}
$$

using proof rules for PCA's (continued)

- show
  $\vdash_{\text{par}} \{ x = m \wedge y = n \}\, z := x;\; x := y;\; y := z;\; \{ y = m \wedge x = n \}$

using proof rules for PCA's (continued)

- show
  $\vdash_{\text{par}} \{ x = m \wedge y = n \}\, z := x;\ x := y;\ y := z;\ \{ y = m \wedge x = n \}$

$z := x;$

$x := y;$

$y := z;$

using proof rules for PCA's (continued)

- show
  $\vdash_{\text{par}} \{ x = m \wedge y = n \} \, z := x; \; x := y; \; y := z; \; \{ y = m \wedge x = n \}$

$z := x;$

$x := y;$

$y := z;$

$\{y = m \wedge x = n\}$

using proof rules for PCA's (continued)

- show
  $\vdash_{\text{par}} \ \{ x = m \wedge y = n \} \ z := x; \ x := y; \ y := z; \ \{ y = m \wedge x = n \}$

$z := x;$

$x := y;$

$\qquad \{z = m \wedge x = n\}$ (assignment)

$y := z;$

$\qquad \{y = m \wedge x = n\}$

using proof rules for PCA's (continued)

- show
  $\vdash_{\text{par}} \{ x = m \land y = n \}\ z := x;\ x := y;\ y := z;\ \{ y = m \land x = n \}$

$z := x;$

$\{z = m \land y = n\}$ (assignment)

$x := y;$

$\{z = m \land x = n\}$ (assignment)

$y := z;$

$\{y = m \land x = n\}$

using proof rules for PCA's (continued)

- show
  $\vdash_{\text{par}} \{ x = m \wedge y = n \}\ z := x;\ x := y;\ y := z;\ \{ y = m \wedge x = n \}$

$\quad\{x = m \wedge y = n\}$	(assignment)
$z := x;$	
$\quad\{z = m \wedge y = n\}$	(assignment)
$x := y;$	
$\quad\{z = m \wedge x = n\}$	(assignment)
$y := z;$	
$\quad\{y = m \wedge x = n\}$	

modified if-statement rule

$$\frac{\{\ \varphi_1\ \}\ C_1\ \{\ \psi\ \} \qquad \{\ \varphi_2\ \}\ C_2\ \{\ \psi\ \}}{\{\ (B \to \varphi_1) \wedge (\neg B \to \varphi_2)\ \}\ \textbf{if}\ B\ \textbf{then}\ C_1\ \textbf{else}\ C_2\ \textbf{fi}\ \{\ \psi\ \}}\ \text{if-statement}$$

using proof rules for PCA's (continued)

- show $\vdash_{\text{par}} \{ \top \} \text{ Succ } \{ y = x + 1 \}$

  where Succ is the following program:

  $a := x + 1;$

  if $a = 1$ **then** $y := 1$ **else** $y := a$ **fi**

using proof rules for PCA's (continued)

$a := x + 1;$

if $a = 1$

then $y := 1$

else $y := a$

fi

using proof rules for PCA's (continued)

$a := x + 1;$

if $a = 1$

then $y := 1$

else $y := a$

fi

$\{y = x + 1\}$

using proof rules for PCA's (continued)

$a := x + 1;$

if $a = 1$

$\{1 = x + 1\}$ (assignment)

then $y := 1$

$\{a = x + 1\}$ (assignment)

else $y := a$

fi

$\{y = x + 1\}$

using proof rules for PCA's (continued)

$a := x + 1;$

$\{a = 1 \to (1 = x + 1) \wedge a \neq 1 \to (a = x + 1)\}$ (if-statement)

if $a = 1$

$\{1 = x + 1\}$ (assignment)

then $y := 1$

$\{a = x + 1\}$ (assignment)

else $y := a$

fi

$\{y = x + 1\}$

using proof rules for PCA's (continued)

$\{x+1=1 \to (1=x+1) \land x+1 \neq 1 \to (x+1=x+1)\}$ (assignment)

$a := x+1;$

$\{a=1 \to (1=x+1) \land a \neq 1 \to (a=x+1)\}$ (if-statement)

if $a=1$

$\{1=x+1\}$ (assignment)

then $y := 1$

$\{a=x+1\}$ (assignment)

else $y := a$

fi

$\{y=x+1\}$

using proof rules for PCA's (continued)

$\{\top\}$ (implied)

$\{x+1=1 \rightarrow (1=x+1) \wedge x+1 \neq 1 \rightarrow (x+1=x+1)\}$ (assignment)

$a := x+1;$

$\quad \{a=1 \rightarrow (1=x+1) \wedge a \neq 1 \rightarrow (a=x+1)\}$ (if-statement)

if $a=1$

$\quad \{1=x+1\}$ (assignment)

then $y := 1$

$\quad \{a=x+1\}$ (assignment)

else $y := a$

fi

$\{y=x+1\}$

reminder: (partial-while) rule once more

$$\frac{\{\ \psi \wedge B\ \}\ C\ \{\ \psi\ \}}{\{\ \psi\ \}\ \textbf{while}\ B\ \textbf{do}\ C\ \textbf{od}\ \{\ \psi \wedge \neg B\ \}} \qquad \text{partial-while}$$

ψ is the **invariant** of the while-loop

reminder: (partial-while) rule once more

$$\frac{\{\ \psi \wedge B\ \}\ C\ \{\ \psi\ \}}{\{\ \psi\ \}\ \textbf{while}\ B\ \textbf{do}\ C\ \textbf{od}\ \{\ \psi \wedge \neg B\ \}} \quad \text{partial-while}$$

ψ is the **invariant** of the while-loop

can you show $\vdash_{\text{par}}\ \{\ \top\ \}\ \text{P}\ \{\ \top \wedge \neg\top\ \}$ where P is
"**while** $(x = x)$ **do** $x := 0$ **od**" ??

reminder: (partial-while) rule once more

$$\frac{\{\ \psi \land B\ \}\ C\ \{\ \psi\ \}}{\{\ \psi\ \}\ \textbf{while}\ B\ \textbf{do}\ C\ \textbf{od}\ \{\ \psi \land \neg B\ \}} \quad \text{partial-while}$$

ψ is the **invariant** of the while-loop

can you show $\vdash_{\text{par}}\ \{\ \top\ \}\ \text{P}\ \{\ \top \land \neg\top\ \}$ where P is
"**while** $(x = x)$ **do** $x := 0$ **od**" ??

YES!

using proof rules for PCA's (continued)

show $\vdash_{\text{par}} \{ \top \}$ Fact $\{ y = x! \}$ where Fact is

$$y := 1;$$
$$z := 0;$$
$$\textbf{while } z \neq x \textbf{ do } z := z + 1;\ y := y * z \textbf{ od}$$

using proof rules for PCA's (continued)

$y := 1;$

$z := 0;$

while $z \neq x$

do $z := z + 1$

$y := y * z$ **od**

using proof rules for PCA's (continued)

$y := 1;$

$z := 0;$

while $z \neq x$

do $z := z + 1$

$y := y * z$ **od**

$\{y = x!\}$

using proof rules for PCA's (continued)

$y := 1;$

$z := 0;$

while $z \neq x$

do $z := z + 1$

$y := y * z$ **od**

$\{y = z! \wedge z = x\}$ (implied)

$\{y = x!\}$

using proof rules for PCA's (continued)

$y := 1;$

$z := 0;$

while $z \neq x$

do $z := z + 1$

$y := y * z$ **od**

$\{y = z!\}$

$\{y = z! \wedge z = x\}$ (implied)

$\{y = x!\}$

using proof rules for PCA's (continued)

$y := 1;$

$z := 0;$

while $z \neq x$

do $z := z + 1$

$\{y \cdot z = z!\}$ (assignment)

$y := y * z$ **od**

$\{y = z!\}$

$\{y = z! \land z = x\}$ (implied)

$\{y = x!\}$

using proof rules for PCA's (continued)

$y := 1;$

$z := 0;$

while $z \neq x$

$\{y \cdot (z+1) = (z+1)!\}$ (assignment)

do $z := z + 1$

$\{y \cdot z = z!\}$ (assignment)

$y := y * z$ **od**

$\{y = z!\}$

$\{y = z! \wedge z = x\}$ (implied)

$\{y = x!\}$

using proof rules for PCA's (continued)

$y := 1;$

$z := 0;$

$\textbf{while } z \neq x$

$\{y = z! \wedge z \neq x\}$ (implied)

$\{y \cdot (z+1) = (z+1)!\}$ (assignment)

$\textbf{do } \; z := z + 1$

$\{y \cdot z = z!\}$ (assignment)

$y := y * z \quad \textbf{od}$

$\{y = z!\}$

$\{y = z! \wedge z = x\}$ (implied)

$\{y = x!\}$

using proof rules for PCA's (continued)

$y := 1;$

$z := 0;$

$\{y = z!\}$ (partial-while)

$\textbf{while } z \neq x$

$\{y = z! \wedge z \neq x\}$ (implied)

$\{y \cdot (z+1) = (z+1)!\}$ (assignment)

$\textbf{do} \quad z := z + 1$

$\{y \cdot z = z!\}$ (assignment)

$y := y * z \quad \textbf{od}$

$\{y = z!\}$

$\{y = z! \wedge z = x\}$ (implied)

$\{y = x!\}$

using proof rules for PCA's (continued)

$y := 1;$

$\{y = 0!\}$ (assignment)

$z := 0;$

$\{y = z!\}$ (partial-while)

while $z \neq x$

$\{y = z! \wedge z \neq x\}$ (implied)

$\{y \cdot (z+1) = (z+1)!\}$ (assignment)

do $z := z + 1$

$\{y \cdot z = z!\}$ (assignment)

$y := y * z$ **od**

$\{y = z!\}$

$\{y = z! \wedge z = x\}$ (implied)

$\{y = x!\}$

using proof rules for PCA's (continued)

$\{1 = 0!\}$ (assignment)

$y := 1;$

$\{y = 0!\}$ (assignment)

$z := 0;$

$\{y = z!\}$ (partial-while)

while $z \neq x$

$\{y = z! \wedge z \neq x\}$ (implied)

$\{y \cdot (z + 1) = (z + 1)!\}$ (assignment)

do $z := z + 1$

$\{y \cdot z = z!\}$ (assignment)

$y := y * z$ **od**

$\{y = z!\}$

$\{y = z! \wedge z = x\}$ (implied)

$\{y = x!\}$

using proof rules for PCA's (continued)

$\{\top\}$ (implied)

$\{1 = 0!\}$ (assignment)

$y := 1;$

$\{y = 0!\}$ (assignment)

$z := 0;$

$\{y = z!\}$ (partial-while)

while $z \neq x$

$\{y = z! \wedge z \neq x\}$ (implied)

$\{y \cdot (z + 1) = (z + 1)!\}$ (assignment)

do $z := z + 1$

$\{y \cdot z = z!\}$ (assignment)

$y := y * z$ **od**

$\{y = z!\}$

$\{y = z! \wedge z = x\}$ (implied)

$\{y = x!\}$

(THIS PAGE INTENTIONALLY LEFT BLANK)