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

$$
\begin{aligned}
& z:=x ; \\
& z:=z+y ; \\
& u:=z
\end{aligned}
$$

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

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

$$
\begin{aligned}
& z:=x ; \\
& z:=z+y ; \\
& u:=z ; \\
& \quad\{u=x+y\}
\end{aligned}
$$

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

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

$$
\begin{aligned}
z:= & x ; \\
z:= & z+y ; \\
& \{z=x+y\} \\
u:= & z ; \\
& \{u=x+y\}
\end{aligned}
$$

(assignment)

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

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

$$
\begin{aligned}
z:= & x ; \\
& \{z+y=x+y\} \\
z:= & z+y ; \\
& \{z=x+y\} \\
u:= & z \\
& \{u=x+y\}
\end{aligned}
$$

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

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

$$
\begin{equation*}
\{x+y=x+y\} \tag{assignment}
\end{equation*}
$$

$$
z:=x
$$

$$
\begin{equation*}
\{z+y=x+y\} \tag{assignment}
\end{equation*}
$$

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

$$
u:=z ;
$$

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

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

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

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

## 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

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

$$
z:=x
$$

$$
x:=y
$$

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

(assignment)

$$
\begin{aligned}
y:= & z ; \\
& \{y=m \wedge x=n\}
\end{aligned}
$$

(assignment)

## using proof rules for PCA's (continued)

- show

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

$$
z:=x
$$

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

(assignment)

$$
x:=y
$$

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

(assignment)

$$
\begin{aligned}
y:= & z \\
& \{y=m \wedge x=n\}
\end{aligned}
$$

## using proof rules for PCA's (continued)

- show

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

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

(assignment)
$z:=x ;$

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

(assignment)

$$
x:=y
$$

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

(assignment)

$$
\begin{aligned}
y:= & z ; \\
& \quad\{y=m \wedge x=n\}
\end{aligned}
$$

## modified if-statement rule

$$
\frac{\left\{\varphi_{1}\right\} C_{1}\{\psi\} \quad\left\{\varphi_{2}\right\} C_{2}\{\psi\}}{\left\{\left(B \rightarrow \varphi_{1}\right) \wedge\left(\neg B \rightarrow \varphi_{2}\right)\right\} \text { if } B \text { then } C_{1} \text { else } C_{2} \text { fi }\{\psi\}}
$$

## using proof rules for PCA's (continued)

- show $\vdash_{\text {par }}\{\top\} \operatorname{Succ}\{y=x+1\}$
where Succ is the following program:
$a:=x+1 ;$
if $a=1$ then $y:=1$ else $y:=a \mathbf{f i}$


## using proof rules for PCA's (continued)

$$
\begin{aligned}
& a:=x+1 \\
& \text { if } a=1 \\
& \text { then } y:=1 \\
& \text { else } y:=a \\
& \text { fi }
\end{aligned}
$$

## using proof rules for PCA's (continued)

$$
\begin{aligned}
& a:=x+1 ; \\
& \text { if } a=1 \\
& \text { then } y:=1 \\
& \text { else } y:=a \\
& \text { fi } \\
& \{y=x+1\}
\end{aligned}
$$

## using proof rules for PCA's (continued)

$$
\begin{aligned}
& a:=x+1 \\
& \text { if } a=1 \\
& \quad\{1=x+1\} \\
& \text { then } y:=1 \\
& \quad\{a=x+1\} \\
& \text { else } y:=a \\
& \text { fi } \\
& \{y=x+1\}
\end{aligned}
$$

## using proof rules for PCA's (continued)

$$
\begin{aligned}
& a:=x+1 \\
& \quad\{a=1 \rightarrow(1=x+1) \wedge a \neq 1 \rightarrow(a=x+1)\} \\
& \text { if } a=1 \\
& \quad\{1=x+1\} \\
& \text { then } y:=1 \\
& \quad\{a=x+1\} \\
& \text { else } y:=a \\
& \text { (if-statement) } \\
& \text { fi } \\
& \{y=x+1\}
\end{aligned}
$$

## using proof rules for PCA's (continued)

$$
\begin{aligned}
& \{x+1=1 \rightarrow(1=x+1) \wedge x+1 \neq 1 \rightarrow(x+1=x+1)\} \text { (assignment) } \\
& a:=x+1 \\
& \quad\{a=1 \rightarrow(1=x+1) \wedge a \neq 1 \rightarrow(a=x+1)\} \quad \text { (if-statement) } \\
& \text { if } a=1 \\
& \quad\{1=x+1\} \\
& \text { then } y:=1 \\
& \quad\{a=x+1\} \\
& \text { else } y:=a \\
& \text { fi } \\
& \{y=x+1\}
\end{aligned}
$$

## using proof rules for PCA's (continued)

$$
\begin{align*}
& \left\{\begin{array}{l}
\text { T }\} \\
\{x+1=1 \rightarrow(1=x+1) \wedge x+1 \neq 1 \rightarrow(x+1=x+1)\} \text { (assignment) } \\
a:=x+1 ; \\
\quad\{a=1 \rightarrow(1=x+1) \wedge a \neq 1 \rightarrow(a=x+1)\} \quad \text { (if-statement) } \\
\text { if } a=1 \\
\quad\{1=x+1\} \\
\text { then } y:=1 \\
\quad\{a=x+1\} \\
\text { else } y:=a \\
\text { fi } \\
\{y=x+1\}
\end{array}\right. \\
& \text { (assignment) } \\
& \text { (assignment) } \\
&
\end{align*}
$$

## reminder: (partial-while) rule once more

$$
\frac{\{\psi \wedge B\} C\{\psi\}}{\{\psi\} \text { while } B \text { do } C \text { od }\{\psi \wedge \neg B\}}
$$

partial-while
$\psi$ is the invariant of the while-loop

## reminder: (partial-while) rule once more

$$
\{\psi \wedge B\} C\{\psi\}
$$

partial-while
$\psi$ is the invariant of the while-loop
can you show $\vdash_{\text {par }}\{\top\} P\{\top \wedge \neg \top\}$ where P is "while $(x=x)$ do $x:=0$ od" ??

## reminder: (partial-while) rule once more

$$
\{\psi \wedge B\} C\{\psi\}
$$

partial-while
$\psi$ is the invariant of the while-loop
can you show $\vdash_{\text {par }}\{\top\} P\{\top \wedge \neg \top\}$ 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

$$
\begin{aligned}
& y:=1 \\
& z:=0 \\
& \text { while } z \neq x \text { do } z:=z+1 ; y:=y * z \text { od }
\end{aligned}
$$

## using proof rules for PCA's (continued)

$$
\begin{aligned}
& y:=1 \\
& z:=0
\end{aligned}
$$

while $z \neq x$

$$
\begin{aligned}
\text { do } z & :=z+1 \\
y & :=y * z \text { od }
\end{aligned}
$$

## using proof rules for PCA's (continued)

$$
\begin{aligned}
& y:=1 \\
& z:=0
\end{aligned}
$$

while $z \neq x$

$$
\text { do } z:=z+1
$$

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

$$
\{y=x!\}
$$

## using proof rules for PCA's (continued)

$$
\begin{align*}
& y:=1 ; \\
& z:=0 ; \\
& \text { while } z \neq x \\
& \\
& \qquad \begin{aligned}
\text { do } \quad z:=z+1 \\
\qquad \\
\\
\{y:=y * z \quad \text { od } \\
\{y=z!\wedge z=x\} \\
\{y=x!\}
\end{aligned}
\end{align*}
$$

## using proof rules for PCA's (continued)

$$
\begin{aligned}
& y:=1 \\
& z:=0
\end{aligned}
$$

while $z \neq x$

$$
\begin{align*}
& \text { do } z:=z+1 \\
& y:=y * z \quad \text { od } \\
& \{y=z!\} \\
& \{y=z!\wedge z=x\}  \tag{implied}\\
& \{y=x!\}
\end{align*}
$$

## using proof rules for PCA's (continued)

$$
\begin{aligned}
& y:=1 \\
& z:=0
\end{aligned}
$$

while $z \neq x$

$$
\begin{aligned}
& \text { do } z:=z+1 \\
& \{y \cdot z=z!\} \\
& y:=y * z \quad \text { od } \\
& \{y=z!\} \\
& \{y=z!\wedge z=x\} \\
& \{y=x!\}
\end{aligned}
$$

(assignment)
(implied)

## using proof rules for PCA's (continued)

$$
\begin{aligned}
& y:=1 \\
& z:=0
\end{aligned}
$$

while $z \neq x$

$$
\begin{aligned}
&\{y \cdot(z+1)=(z+1)!\} \\
& \text { do } z:=z+1 \\
&\{y \cdot z=z!\} \\
& y:=y * z \text { od } \\
&\{y=z!\} \\
&\{y=z!\wedge z=x\} \\
&\{y=x!\}
\end{aligned}
$$

## using proof rules for PCA's (continued)

$$
\begin{aligned}
& y:=1 \\
& z:=0
\end{aligned}
$$

while $z \neq x$

$$
\begin{aligned}
& \{y=z!\wedge z \neq x\} \\
& \{y \cdot(z+1)=(z+1)!\}
\end{aligned}
$$

$$
\text { do } z:=z+1
$$

$$
\{y \cdot z=z!\}
$$

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

$$
\{y=z!\}
$$

$$
\{y=z!\wedge z=x\}
$$

(assignment)
(implied)

$$
\{y=x!\}
$$

## using proof rules for PCA's (continued)

$$
\begin{aligned}
& y:=1 ; \\
& z:=0 ; \\
& \{y=z!\} \\
& \text { (partial-while) } \\
& \text { while } z \neq x \\
& \{y=z!\wedge z \neq x\} \\
& \{y \cdot(z+1)=(z+1)!\} \\
& \text { do } z:=z+1 \\
& \{y \cdot z=z!\} \\
& y:=y * z \quad \text { od } \\
& \{y=z!\} \\
& \{y=z!\wedge z=x\} \\
& \{y=x!\} \\
& \text { (implied) } \\
& \text { (assignment) } \\
& \text { (assignment) } \\
& \text { (implied) }
\end{aligned}
$$

## using proof rules for PCA's (continued)

$$
\begin{aligned}
& y:=1 ; \\
& \{y=0!\} \\
& z:=0 ; \\
& \{y=z!\} \\
& \text { (assignment) } \\
& \text { (partial-while) } \\
& \text { while } z \neq x
\end{aligned}
$$

## using proof rules for PCA's (continued)

$$
\begin{align*}
& \{1=0!\} \\
& y:=1 ; \\
& \{y=0!\} \\
& z:=0 ; \\
& \{y=z!\} \\
& \text { (assignment) } \\
& \text { (assignment) } \\
& \text { (partial-while) } \\
& \text { while } z \neq x \\
& \{y=z!\wedge z \neq x\} \\
& \{y \cdot(z+1)=(z+1)!\} \\
& \text { do } z:=z+1 \\
& \{y \cdot z=z!\} \\
& y:=y * z \quad \text { od } \\
& \{y=z!\} \\
& \{y=z!\wedge z=x\}  \tag{implied}\\
& \{y=x!\}
\end{align*}
$$

## using proof rules for PCA's (continued)

| \{T\} | (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) |
| $y:=y * z \quad$ od |  |
| $\{y=z!\}$ |  |
| $\{y=z!\wedge z=x\}$ | (implied) |
| $\{y=x!\}$ |  |

## (THIS PAGE INTENTIONALLY LEFT BLANK)

