# CS 512, Spring 2018, Handout 20 Hoare Logic (Continued) 

Assaf Kfoury

## March 21, 2018

## using proof rules for PCA's (program computes $r=x \bmod y$ and $q=x$ div $y$ )

$$
\begin{aligned}
& r:=x \\
& q:=0 \\
& \text { while } y \leqslant r
\end{aligned}
$$

$$
\text { do } \begin{aligned}
r & :=r-y \\
& q:=q+1 \quad \text { od }
\end{aligned}
$$

## using proof rules for PCA's (program computes $r=x \bmod y$ and $q=x$ div $y$ )

$$
\begin{aligned}
& r:=x \\
& q:=0 \\
& \text { while } y \leqslant r
\end{aligned}
$$

$$
\text { do } r:=r-y
$$

$$
q:=q+1 \quad \text { od }
$$

$$
\{x=r+y \cdot q \wedge r<y\}
$$

## using proof rules for PCA's (program computes $r=x \bmod y$ and $q=x$ div $y$ )

$$
\begin{aligned}
& r:=x \\
& q:=0
\end{aligned}
$$

$$
\text { while } y \leqslant r
$$

$$
\begin{array}{r}
\text { do } \quad r:=r-y \\
q:=q+1 \quad \text { od } \\
\{x=r+y \cdot q\} \\
\{x=r+y \cdot q \wedge r<y\}
\end{array}
$$

## using proof rules for PCA's

$$
\begin{aligned}
& r:=x \\
& q:=0
\end{aligned}
$$

```
while }y\leqslant
```

$$
\begin{aligned}
& \text { do } r:=r-y \\
&\{x=r+y \cdot(q+1)\} \\
& q:=q+1 \quad \text { od } \\
&\{x=r+y \cdot q\} \\
&\{x=r+y \cdot q \wedge r<y\}
\end{aligned}
$$

## using proof rules for PCA's

$$
\begin{aligned}
& r:=x \\
& q:=0
\end{aligned}
$$

```
while }y\leqslant
```

$$
\begin{aligned}
&\{x=r-y+y \cdot(q+1)\} \\
& \text { do } \quad r:=r-y \\
&\{x=r+y \cdot(q+1)\} \\
& q:=q+1 \quad \text { od } \\
&\{x=r+y \cdot q\} \\
&\{x=r+y \cdot q \wedge r<y\}
\end{aligned}
$$

## using proof rules for PCA's

$$
\begin{aligned}
& r:=x \\
& q:=0
\end{aligned}
$$

while $y \leqslant r$

$$
\begin{aligned}
&\{x=r+y \cdot q\} \\
&\{x=r-y+y \cdot(q+1)\} \\
& \text { do } \quad r:=r-y \\
&\{x=r+y \cdot(q+1)\} \\
& q:=q+1 \quad \text { od } \\
&\{x=r+y \cdot q\} \\
&\{x=r+y \cdot q \wedge r<y\}
\end{aligned}
$$

(implied)
(assignment)
(assignment)

## using proof rules for PCA's

$$
\begin{aligned}
& r:=x \\
& q:=0
\end{aligned}
$$

while $y \leqslant r$

$$
\begin{aligned}
&\{x=r+y \cdot q \wedge y \leqslant r\} \\
&\{x=r+y \cdot q\} \\
&\{x=r-y+y \cdot(q+1)\} \\
& \text { do } \quad r:=r-y \\
&\{x=r+y \cdot(q+1)\} \\
& q:=q+1 \quad \text { od } \\
&\{x=r+y \cdot q\} \\
&\{x=r+y \cdot q \wedge r<y\}
\end{aligned}
$$

(implied)
(implied)
(assignment)
(assignment)

## using proof rules for PCA's

$$
\begin{aligned}
& r:=x ; \\
& q:=0 ; \\
& \{x=r+y \cdot q\} \\
& \text { (partial-while) } \\
& \text { while } y \leqslant r \\
& \{x=r+y \cdot q \wedge y \leqslant r\} \\
& \{x=r+y \cdot q\} \\
& \{x=r-y+y \cdot(q+1)\} \\
& \text { do } r:=r-y \\
& \{x=r+y \cdot(q+1)\} \\
& q:=q+1 \quad \text { od } \\
& \{x=r+y \cdot q\} \\
& \{x=r+y \cdot q \wedge r<y\} \\
& \text { (implied) } \\
& \text { (assignment) } \\
& \text { (assignment) }
\end{aligned}
$$

## using proof rules for PCA's

$$
\begin{aligned}
& r:=x ; \\
& \{x=r\} \\
& q:=0 \text {; } \\
& \{x=r+y \cdot q\} \\
& \text { (assignment) } \\
& \text { (partial-while) } \\
& \text { while } y \leqslant r \\
& \{x=r+y \cdot q \wedge y \leqslant r\} \\
& \{x=r+y \cdot q\} \\
& \{x=r-y+y \cdot(q+1)\} \\
& \text { do } r:=r-y \\
& \{x=r+y \cdot(q+1)\} \\
& q:=q+1 \quad \text { od } \\
& \{x=r+y \cdot q\} \\
& \{x=r+y \cdot q \wedge r<y\} \\
& \text { (partial-while) } \\
& \text { (implied) } \\
& \text { (implied) } \\
& \text { (assignment) } \\
& \text { (assignment) }
\end{aligned}
$$

## using proof rules for PCA's

(assignment)
(assignment)
(partial-while)
(implied)
(implied)
(assignment)
(assignment)

$$
\begin{aligned}
& \{x=x\} \\
& r:=x \text {; } \\
& \{x=r\} \\
& q:=0 \text {; } \\
& \{x=r+y \cdot q\} \\
& \text { while } y \leqslant r \\
& \{x=r+y \cdot q \wedge y \leqslant r\} \\
& \{x=r+y \cdot q\} \\
& \{x=r-y+y \cdot(q+1)\} \\
& \text { do } r:=r-y \\
& \{x=r+y \cdot(q+1)\} \\
& q:=q+1 \quad \text { od } \\
& \{x=r+y \cdot q\} \\
& \{x=r+y \cdot q \wedge r<y\}
\end{aligned}
$$

## using proof rules for PCA's

(program computes $r=x \bmod y$ and $q=x \operatorname{div} y$ )

## \{T\}

$$
\{x=x\}
$$

$$
r:=x
$$

$$
\{x=r\}
$$

$$
q:=0
$$

$$
\{x=r+y \cdot q\}
$$

while $y \leqslant r$

$$
\begin{aligned}
&\{x=r+y \cdot q \wedge y \leqslant r\} \\
&\{x=r+y \cdot q\} \\
&\{x=r-y+y \cdot(q+1)\} \\
& \text { do } \quad r:=r-y \\
&\{x=r+y \cdot(q+1)\} \\
& q:=q+1 \quad \text { od } \\
&\{x=r+y \cdot q\} \\
&\{x=r+y \cdot q \wedge r<y\}
\end{aligned}
$$

## (implied)

(assignment)
(assignment)
(partial-while)
(implied)
(implied)
(assignment)
(assignment)

## using proof rules for PCA's (from last page of Handout 19)

| $\{T\}$ | (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) |
| $\{y=x!\}$ |  |

## using proof rules for TCA's

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

while $z \neq x$

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

## using proof rules for TCA's

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

## using proof rules for TCA's

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

while $z \neq x$

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

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

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

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

## using proof rules for TCA's

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

while $z \neq x$

$$
\begin{aligned}
& \text { do } z:=z+1 \\
& \qquad \begin{array}{l}
y:=y * z \text { od } \\
\qquad\{y=z!\wedge 0 \leqslant x-z<v\} \\
\{y=z!\wedge z=x\} \\
\{y=x!\}
\end{array}
\end{aligned}
$$

## using proof rules for TCA's

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

while $z \neq x$

$$
\begin{aligned}
& \text { do } \quad z:=z+1 \\
& \\
& \quad\{y \cdot z=z!\wedge 0 \leqslant x-z<v\} \\
& \\
& \quad y:=y * z \text { od } \\
& \\
& \quad\{y=z!\wedge 0 \leqslant x-z<v\} \\
& \{y=z!\wedge z=x\} \\
& \{y=x!\}
\end{aligned}
$$

## using proof rules for TCA's

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

while $z \neq x$

$$
\begin{aligned}
& \quad\{y \cdot(z+1)=(z+1)!\wedge 0 \leqslant x-(z+1)<v\} \\
& \text { do } \quad z:=z+1 \\
& \\
& \{y \cdot z=z!\wedge 0 \leqslant x-z<v\} \\
& \\
& \\
& \\
& \\
& \\
& \{y:=y * z \text { od } \\
& \{y=z!\wedge z=x\} \\
& \{y=x!\}
\end{aligned}
$$

## using proof rules for TCA's

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

while $z \neq x$

$$
\begin{aligned}
& \{y=z!\wedge z \neq x \wedge 0 \leqslant x-z=v\} \\
& \{y \cdot(z+1)=(z+1)!\wedge 0 \leqslant x-(z+1)<v\} \\
\text { do } & z:=z+1 \\
& \{y \cdot z=z!\wedge 0 \leqslant x-z<v\} \\
& y:=y * z \text { od } \\
& \{y=z!\wedge 0 \leqslant x-z<v\} \\
\{y=z!\wedge & \text { (assignment) } \\
\{y=x\} & \text { (assignment) } \\
& x\}
\end{aligned}
$$

## using proof rules for TCA's

$$
\begin{aligned}
& y:=1 \\
& z:=0 \\
& \{y=z!\wedge 0 \leqslant x-z\}
\end{aligned}
$$

(total-while)
while $z \neq x$

$$
\begin{aligned}
& \{y=z!\wedge z \neq x \wedge 0 \leqslant x-z=v\} \\
& \{y \cdot(z+1)=(z+1)!\wedge 0 \leqslant x-(z+1)<v\} \\
\text { do } & z:=z+1 \\
& \{y \cdot z=z!\wedge 0 \leqslant x-z<v\} \\
& y:=y * z \text { od } \\
& \{y=z!\wedge 0 \leqslant x-z<v\} \\
\{y=z!\wedge z=x\} & \text { (assignment) } \\
\{y=x!\} & \text { (assignment) } \\
&
\end{aligned}
$$

## using proof rules for TCA's

$$
\begin{array}{ll}
\begin{array}{l}
y:=1 ; \\
\\
\{y=0! \\
z:=0 ; \\
\\
\{y=z!\wedge 0 \leqslant x-0\} \\
\text { while } z \neq x
\end{array} & \text { (assignment) } \\
& \{y=z!\wedge z \neq x \wedge 0 \leqslant x-z=v\} \\
& \{y \cdot(z+1)=(z+1)!\wedge 0 \leqslant x-(z+1)<v\} \\
& \text { (total-while) } \\
& \quad z:=z+1 \\
& \{y \cdot z=z!\wedge 0 \leqslant x-z<v\} \\
& y:=y * z \quad \text { od } \\
& \{y=z!\wedge 0 \leqslant x-z<v\} \\
\text { (implied) } \\
\{y=z!\wedge z=x\} & \text { (assignment) } \\
\{y=x!\} &
\end{array}
$$

## using proof rules for TCA's

$$
\begin{array}{ll}
\{1=0!\wedge 0 \leqslant x-0\} \\
y:=1 ; & \\
\{y=0!\wedge 0 \leqslant x-0\} & \text { (assignment) } \\
z:=0 ; & \text { (assignment) } \\
\{y=z!\wedge 0 \leqslant x-z\} \\
\text { while } z \neq x & \text { (total-while) } \\
& \{y=z!\wedge z \neq x \wedge 0 \leqslant x-z=v\} \\
& \{y \cdot(z+1)=(z+1)!\wedge 0 \leqslant x-(z+1)<v\} \\
& \text { do } \quad z:=z+1 \\
& \{y \cdot z=z!\wedge 0 \leqslant x-z<v\} \\
& y:=y * z \quad \text { od } \\
& \{y=z!\wedge 0 \leqslant x-z<v\} \\
\text { (implied) } \\
\{y=z!\wedge z=x\} & \text { (assignment) } \\
\{y=x!\} & \text { (assignment) } \\
\{y=x
\end{array}
$$

## using proof rules for TCA's

$$
\begin{aligned}
& \{x \geqslant 0\} \\
& \{1=0!\wedge 0 \leqslant x-0\} \\
& y:=1 ; \\
& \{y=0!\wedge 0 \leqslant x-0\} \\
& z:=0 \\
& \{y=z!\wedge 0 \leqslant x-z\}
\end{aligned}
$$

(implied)
(assignment)
(assignment)
(total-while)
while $z \neq x$

$$
\begin{aligned}
&\{y=z!\wedge z \neq x \wedge 0 \leqslant x-z=v\} \\
&\{y \cdot(z+1)=(z+1)!\wedge 0 \leqslant x-(z+1)<v\} \\
& \text { do } z:=z+1 \\
&\{y \cdot z=z!\wedge 0 \leqslant x-z<v\} \\
& y:=y * z \text { od } \\
&\{y=z!\wedge 0 \leqslant x-z<v\} \\
&\{y=z!\wedge z=x\} \\
&\{y=x!\} \text { (assignment) } \\
& \text { (assignment) } \\
&
\end{aligned}
$$

## (THIS PAGE INTENTIONALLY LEFT BLANK)

