Chapter 2: The Guarded Command Language (Part 2)

Skip

- Execution of skip does not have any effect.

$$\{P\}\text{skip}\{Q\} \text{ is equivalent to } [P \Rightarrow Q]$$

- Example

$$\begin{array}{l} |[\\ \textbf{var } x, y : \text{int}; \\ \{x \geq 1\} \\ \text{skip} \\ \{x \geq 0\} \\ ]| \end{array}$$

- Weakest precondition: $wp.\text{skip}.Q \equiv Q$

Assignment

- Any change of state is due to the execution of an assignment statement.

$$x := E$$

replaces the value of x by the value of E.

$$\{P\}x := E\{Q\} \text{ is equivalent to } [P \Rightarrow \mathrm{def}.E \wedge Q(x := E)]$$

Here def.E is defined for which values of its variables in E is defined.

$$\mathrm{def}.(a \ \mathbf{mod} \ b) = b \neq 0$$

- Weakest precondition

$$[wp.(x := E).Q \ \equiv \ \mathbf{def}.E \ \wedge \ Q(x := E)]$$

- Example

$$\{x \geq 3\} x := x + 1 \{x \geq 0\}$$

follows from

$$\begin{array}{ll}
 & \text{def.}(x+1) \wedge (x \geq 0)(x := x + 1) \\
\equiv & \quad \{ \text{ def } \} \\
 & true \wedge (x \geq 0)(x := x + 1) \\
\equiv & \quad \{ \wedge\text{, substitution } \} \\
 & x + 1 \geq 0 \\
\equiv & \quad \{ \text{ arithmetic } \} \\
 & x \geq -1 \\
\Leftarrow & \quad \{ \text{ arithmetic } \} \\
 & x \geq 3
\end{array}$$

Catenation

- Catenation allows us to describe sequence of actions.

$$S;T$$

  S is executed after which T is executed.

$$\{P\}S;T\{Q\} \text{ is equivalent to } \exists R.\{P\}S\{R\} \text{ and } \{R\}T\{Q\}$$

- Weakest precondition

$$[wp.(S;T).Q \;\equiv\; wp.S.(wp.T.Q)]$$

  i.e., semi-colon corresponds to function composition.

- Prove

$$
\begin{array}{l}
|[\\
\textbf{var } a, b : \text{bool}; \\
\{(a \equiv A) \wedge (b \equiv B)\} \\
a := a \equiv b; \\
b := a \equiv b; \\
a := a \equiv b \\
\{(a \equiv B) \wedge (b \equiv A)\} \\
]|
\end{array}
$$

  - Hint: Compute the weakest preconditions backwards.

Selection

$$\mathbf{if}\ B.0 \rightarrow S.0\ [\!]\ \cdots\ [\!]\ B.n \rightarrow S.n\ \mathbf{fi}$$

where

- $B.i$: a boolean expression (a guard)
- $S.i$: a statement
- $B.i \rightarrow S.i$: a guarded command

1. All guards B_i are evaluated.
2. If none of the guards evaluates to true then execution *aborts*, otherwise one of the guards that has the value true is chosen *non-deterministically* and the corresponding statement is executed.

An Example

Derive a statement S that satisfies

$$
\begin{array}{l}
|[\\
\textbf{var } x, y, z : \mathrm{int}; \\
\{\mathrm{true}\} \\
S \\
\{z = x \textbf{ max } y\} \\
]|
\end{array}
$$

where **max** is defined by

$$z = x \textbf{ max } y \;\equiv\; (z = x \vee z = y) \wedge z \geq x \wedge z \geq y$$

We conclude that $z := x$ is a candidate for S. As a precondition we can have

$$
\begin{array}{ll}
& ((z = x \vee z = y) \wedge z \geq x \wedge z \geq y)(z := x) \\
\equiv & \quad \{ \text{ substitution } \} \\
& (x = x \vee x = y) \wedge x \geq x \wedge x \geq y \\
\equiv & \quad \{ \text{ calculus } \} \\
& x \geq y
\end{array}
$$

So

$$x \geq y \rightarrow z := x$$

Symmetrically,

$$y \geq x \rightarrow z := y$$

So, the definition of S is

$$\textbf{if } x \geq y \rightarrow z := x \; [] \; y \geq x \rightarrow z := y \textbf{ fi}$$

Formulation of Selection Statement

$$\{P\}\textbf{if } B_0 \rightarrow S_0 \;[]\; B_1 \rightarrow S_1 \textbf{ fi}\{Q\}$$

is equivalent to

1. $[P \rightarrow B_0 \vee B_1]$ and
2. $\{P \wedge B_0\}S_0\{Q\}$ and $\{P \wedge B_1\}S_1\{Q\}$

- Examples
  - Prove $\{x = 0\}\textbf{if } \mathit{true} \rightarrow x := x + 1 \;[]\; \mathit{true} \rightarrow x := x + 1 \textbf{ fi}\{x = 1\}$.
  - Prove $\{x = 0\}\textbf{if } \mathit{true} \rightarrow x := 1 \;[]\; \mathit{true} \rightarrow x := -1 \textbf{ fi}\{x = 1 \vee x = -1\}$.

Weakest Precondition for Selection

$$
\begin{aligned}
&[wp.(\mathbf{if}\ B_0 \rightarrow S_0\ []\ B_1 \rightarrow S_1\ \mathbf{fi}).Q \\
&\quad \equiv (B_0 \vee B_1) \wedge \\
&\qquad (B_0 \rightarrow wp.S_0.Q) \wedge \\
&\qquad (B_1 \rightarrow wp.S_1.Q) \\
&]
\end{aligned}
$$

Repetition

$$\mathbf{do}\ B.0 \rightarrow S.0\ []\ \cdots\ []\ B.n \rightarrow S.n\ \mathbf{od}$$

1. All guards B_i are evaluated.
2. If none of the guards evaluates to true then execution *skip*, otherwise one of the guards that has the value true is chosen *non-deterministically* and the corresponding statement is executed, after which the repetition is executed again.

Formulation of Repetition Statement

$$\{P\}\mathbf{do}\ B_0 \rightarrow S_0 \ [] \ B_1 \rightarrow S_1 \ \mathbf{od}\{Q\}$$

is equivalent to

$$
\begin{array}{l}
\{P\} \\
\mathbf{if}\ (\neg B_0 \wedge \neg B_1) \rightarrow \text{skip} \\
\ [] \ B_0 \rightarrow S_0;\ \mathbf{do}\ B_0 \rightarrow S_0 \ [] \ B_1 \rightarrow S_1 \ \mathbf{od} \\
\ [] \ B_1 \rightarrow S_1;\ \mathbf{do}\ B_0 \rightarrow S_0 \ [] \ B_1 \rightarrow S_1 \ \mathbf{od} \\
\mathbf{fi} \\
\{Q\}
\end{array}
$$

That is

$$\begin{array}{l}
\{P\} \\
\textbf{if } (\neg B_0 \wedge \neg B_1) \rightarrow \underline{\{P \wedge (\neg B_0 \wedge \neg B_1)\}}\text{skip}\underline{\{Q\}} \\
\ [] \ B_0 \rightarrow \underline{\{P \wedge B_0\}}S_0\underline{\{P\}};\ \underline{\{P\}}\textbf{do } B_0 \rightarrow S_0 \ [] \ B_1 \rightarrow S_1 \textbf{ od}\underline{\{Q\}} \\
\ [] \ B_1 \rightarrow \underline{\{P \wedge B_1\}}S_1\underline{\{P\}};\ \underline{\{P\}}\textbf{do } B_0 \rightarrow S_0 \ [] \ B_1 \rightarrow S_1 \textbf{ od}\underline{\{Q\}} \\
\textbf{fi} \\
\{Q\}
\end{array}$$

So

(i) $[P \wedge (\neg B_0 \wedge \neg B_1) \Rightarrow Q]$ and

(ii) $\{P \wedge B_0\}S_0\{P\}$ and $\{P \wedge B_1\}S_1\{P\}$

implies

$$\{P\}\mathbf{do}\ B_0 \rightarrow S_0\ []\ B_1 \rightarrow S_1\ \mathbf{od}\{Q\}$$

provided that this repetition terminates.

Note: A predicate P that satisfies (ii) is called an invariant of $\mathbf{do}\ B_0 \rightarrow S_0\ []\ B_1 \rightarrow S_1\ \mathbf{od}$.

An Example

Prove that

$$
\begin{array}{l}
|[\\
\mathbf{var}\ x, y : \mathrm{int}; \\
\{x = X \wedge y = Y \wedge x > 0 \wedge y > 0\} \\
\mathbf{do}\ x > y \rightarrow x := x - y\ [\!]\ y > x \rightarrow y := y - x\ \mathbf{od} \\
\{x = X\ \mathbf{gcd}\ Y\} \\
]|
\end{array}
$$

where X **gcd** Y denotes the greatest common divisor of X and Y.

Proof Sketch.

- Define an invariant P as

$$P : \; x > 0 \wedge y > 0 \wedge x \textbf{ gcd } y = X \textbf{ gcd } Y$$

  satisfying $x = X \wedge y = Y \wedge x > 0 \wedge y > 0 \;\Rightarrow P$.

- Prove:
  - $P \wedge \neg(x > y) \wedge \neg(y > x) \;\Rightarrow\; x = X \textbf{ gcd } Y$
  - $\{P \wedge (x > y)\}x := x - y\{P\}$
  - $\{P \wedge (y > x)\}y := y - x\{P\}$

- Show the termination of the repetition.
  - Let $t = x + y$. $t \geq 0$ and t decreases in each step of repetition.

Exercises

Problem 2

The following problem may be used to compute (non-deterministically) natural numbers x and y such that $x * y = N$. Prove:

$$
\begin{array}{l}
|[\\
\textbf{var}\ p, x, y, N : \text{int}; \\
\{N \geq 1\} p, x, y := N - 1, 1, 1 \\
\{N = x * y + p\} \\
;\textbf{do}\ p \neq 0 \\
\quad \rightarrow \textbf{if}\ p\ \textbf{mod}\ x = 0 \rightarrow p, y := p - x, y + 1 \\
\qquad [\,]\ p\ \textbf{mod}\ y = 0 \rightarrow x, p := x + 1, p - y \\
\qquad \textbf{fi} \\
\textbf{od} \\
\{x * y = N\} \\
]|.
\end{array}
$$