Axiomatic Semantics

- Based on techniques from predicate logic.
- More abstract than denotational semantics.
- There is no concept of “state of the machine”.
- Semantic meaning of a program is based on assertions about relationships that remain the same each time the program executes.
- Application: Proving programs to be correct.

Limitations

- Side effects disallowed in expressions.
- goto command difficult to specify.
- Aliasing not allowed.
- Scope rules difficult to describe ⇒ require all identifier names to be unique.

Concentrate on commands in Wren.

Assertion

A logical formula, say \((m \neq 0 \text{ and } (\sqrt{m})^2 = m)\), that is true when a point in the program is reached.

Precondition: Assertion before a command.
Postcondition: Assertion after a command.

\{ PRE \} C \{ POST \}

Partial Correctness

If the initial assertion (the precondition) is true and if the program terminates, then the final assertion (the postcondition) must be true.

Precondition + Termination ⇒ Postcondition

Total Correctness

Given that the precondition for the program is true, the program must terminate and the postcondition must be true.

Total Correctness = Partial Correctness + Termination

Assignment Command

1) \{ true \} m := 13 \{ m = 13 \}
2) \{ n = 3 \text{ and } c = 2 \} n := c*n \{ n = 6 \text{ and } c = 2 \}
3) \{ k \geq 0 \} k := k + 1 \{ k > 0 \}

Notation

\{ Precondition \} command \{ Postcondition \}

P[V\rightarrow E] denotes substitution of E for V in P

Axiom for assignment command

\{ P[V\rightarrow E] \} V := E \{ P \}

Work backwards:

Postcondition: \( P = (n = 6 \text{ and } c = 2) \)
Command: \( n := c*n \)
Precondition: \( P[V\rightarrow E] = (c*n = 6 \text{ and } c = 2) \)

Read and Write Commands

Notation

Use “IN = [1,2,3]” and “OUT = [4,5]” to represent input and output files.

\([M]\)L denotes list whose head is M and tail is L.
Use small caps, \(K, M, N, \ldots\), to represent arbitrary numerals.

Axiom for Read Command

\{ IN = [K]\}L \text{ and } P[V\rightarrow K] \} \text{ read } V \{ IN = L \text{ and } P \}

Axiom for Write Command

\{ OUT=L \text{ and } E=K \text{ and } P \}
write E
\{ OUT=L[K] \text{ and } E=K \text{ and } P \}

Note: \(L[K]\) means \text{affix}(L,K).
Rules of Inference

\[
\frac{H_1, H_2, \ldots, H_n}{H}
\]
Compare with structural operational semantics.

Axiom for Command Sequencing

\[
\frac{(P) C_1 \{Q\}, (Q) C_2 \{R\}}{(P) \ C_1 ; C_2 \{R\}}
\]

Axioms for If Commands

\[
\frac{(P \text{ and } B) C_1 \{Q\}, (P \text{ and not } B) C_2 \{Q\}}{(P) \text{ if } B \text{ then } C_1 \text{ else } C_2 \text{ end if } \{Q\}}
\]

\[
\frac{(P \text{ and } B) \ C \{Q\}, (P \text{ and not } B) \supset Q}{(P) \text{ if } B \text{ then } C \text{ end if } \{Q\}}
\]

Weaken Postcondition

\[
\frac{(P) C(Q), Q \supset R}{(P) \ C \{R\}}
\]

Strengthen Precondition

\[
\frac{P \supset Q, (Q) C\{R\}}{(P) \ C \{R\}}
\]

And and Or Rules

\[
\frac{(P) C(Q), (P') C\{Q'\}}{(P \text{ and } P') \ C \{Q \text{ and } Q'\}}
\]

\[
\frac{(P) C\{Q\}, (P') \ C\{Q'\}}{(P \text{ or } P') \ C \{Q \text{ or } Q'\}}
\]

Observation

\[
\{ \text{false} \} \text{ any-command } \{ \text{any-postcondition} \}
\]

Example

\[
\{ \text{IN} = [4,9,16] \text{ and OUT} = [0,1,2] \}
\]

read m; read n;
if m\geq n then
a := 2 * m
else
a := 2 * n
end if;
write a
\{ \text{IN} = [16] \text{ and OUT} = [0,1,2,18] \}

\[
\{ \text{IN} = [4,9,16] \text{ and OUT} = [0,1,2] \}
\]

\[
\{ \text{IN} = [4,9,16] \text{ and OUT} = [0,1,2] \text{ and } 4=4 \}
\]

read m;
\{ \text{IN} = [9,16] \text{ and OUT} = [0,1,2] \text{ and } m=4 \}
\{ \text{IN} = [9,16] \text{ and OUT} = [0,1,2] \text{ and } m=4 \text{ and } 9=9 \}

read n;
\{ \text{IN} = [16] \text{ and OUT} = [0,1,2] \text{ and } m=4 \text{ and } n=9 \}

Let S = \{ \text{IN} = [16] \text{ and OUT} = [0,1,2] \}
and B = m\geq n

Then
\( (S \text{ and } B) \supset \text{false}, \)
and
\( S \supset \text{not } B \)

So
\{ S \text{ and } B \}, which is equivalent to false
\( a := 2 \times m \)
\{ \text{IN} = [16] \text{ and OUT} = [0,1,2] \text{ and } m=4 \text{ and } n=9 \text{ and } a=18 \},
and
\{ S \text{ and not } B \}
\{ \text{IN} = [16] \text{ and OUT} = [0,1,2] \text{ and } m=4 \text{ and } n=9 \text{ and } 2\times n=18 \}
\( a := 2 \times n \)
\{ \text{IN} = [16] \text{ and OUT} = [0,1,2] \text{ and } m=4 \text{ and } n=9 \text{ and } a=18 \}
Therefore by one of the If axioms,
\{ S \}
if \( m \geq n \) then
  \[ a := 2 \cdot m \]
else
  \[ a := 2 \cdot n \]
end if;
\{ \text{IN} = [16] \text{ and OUT} = [0,1,2] \text{ and } m=4 \text{ and } n=9 \text{ and } a=18 \}
and
\{ \text{IN} = [16] \text{ and OUT} = [0,1,2] \text{ and } m=4 \text{ and } n=9 \text{ and } a=18 \}
write a
\{ \text{IN} = [16] \text{ and OUT} = [0,1,2] \text{ and } m=4 \text{ and } n=9 \text{ and } a=18 \}
which implies
\{ \text{IN} = [16] \text{ and OUT} = [0,1,2] \text{ and } m=4 \text{ and } n=9 \text{ and } a=18 \}

\section*{Loop Invariant}

- A relationship among the variables that does not change as the loop is executed.
- Look for some expression that can be combined with not B to produce part of the postcondition.
- Construct a table of values to see what stays constant.
- Combine what has already been computed at some stage in the loop with what has yet to be computed to yield a constant of some sort.

Look at the factorial example carefully.

\section*{Example: Exponent}
\{ N \geq 0 \text{ and } A \geq 0 \}
\begin{align*}
k &:= N; \quad s := 1; \\
\text{while } k > 0 \text{ do} \\
  &\quad s := A \cdot s; \\
  &\quad k := k - 1 \\
\text{end while} \\
\{ s = A^N \}
\end{align*}

Trace algorithm with small numbers \( A=2, N=5 \).

Build a table of values to find loop invariant.

\begin{tabular}{|c|c|c|c|}
\hline
\( k \) & \( s \) & \( 2^k \) & \( s \cdot 2^k \) \\
\hline
5 & 1 & 32 & 32 \\
4 & 2 & 16 & 32 \\
3 & 4 & 8 & 32 \\
2 & 8 & 4 & 32 \\
1 & 16 & 2 & 32 \\
0 & 32 & 1 & 32 \\
\hline
\end{tabular}
Example: Nested While Loops

\{ \text{IN} = [A] \text{ and } \text{OUT} = [] \text{ and } A \geq 0 \}\)

\hspace{1cm} \begin{align*}
\text{(1)} \quad & \text{read } x; \\
& m := 0; \ n := 0; \ s := 0; \\
\text{(2)} \quad & \text{while } x > 0 \text{ do } \text{ (outer loop invariant: C) } \\
& \hspace{1cm} \text{x := x–1; } \ n := m+2; \ m := m+1; \\
\text{(4)} \quad & \text{while } m > 0 \text{ do } \text{ (inner loop invariant: D) } \\
& \hspace{2cm} \text{m := m–1; } \ s := s+1 \\
& \hspace{2cm} \text{end while; } \\
& m := n \\
& \text{end while; } \\
\text{(5)} \quad & \text{write } s
\end{align*}

\{ \text{OUT} = [A^2] \}\)

Verification of Program

Initialization:
\{ n \geq 0 \text{ and } A \geq 0 \} \supset
\{ N \geq n \geq 0 \text{ and } A \geq 0 \text{ and } 1=1 \} \\
\hspace{1cm} \begin{align*}
& k := N; \ s := 1; \\
& \{ k \geq N \geq 0 \text{ and } A \geq 0 \text{ and } s=1 \} \supset \\
& \{ k \geq 0 \text{ and } s \cdot A^k = A^N \}
\end{align*}

Preservation:
\{ k \geq 0 \text{ and } s \cdot A^k = A^N \text{ and } k > 0 \} \supset
\{ k > 0 \text{ and } s \cdot A^k = A^N \} \supset \\
\hspace{1cm} \begin{align*}
& \{ k > 0 \text{ and } A \cdot s \cdot A^k = A^N \} \\
& s := A \cdot s; \\
& \{ k > 0 \text{ and } s \cdot A^k = A^N \} \supset \\
& \{ k-1 \geq 0 \text{ and } s \cdot A^k = A^N \} \\
& k := k-1 \\
& \{ k \geq 0 \text{ and } s \cdot A^k = A^N \}
\end{align*}

Completion:
\{ k \geq 0 \text{ and } s \cdot 2^k = A^N \text{ and } k \leq 0 \} \supset
\{ k=0 \text{ and } s \cdot 2^k = A^N \} \supset \{ s = A^N \}

Introduce boolean valued terms, called predicates, to refer to the invariants.

The outer invariant \( C(x, m, n, s) = \)
\hspace{1cm} \begin{align*}
& ( x \geq 0 \text{ and } m=2(A–x) \text{ and } m=n \geq 0 \\
& \text{ and } s=(A–x)^2 \text{ and } \text{OUT}=[ ] )
\end{align*}

First prove this invariant is true initially by pushing it back through the initialization code.

\hspace{1cm} \begin{align*}
\text{(1) } \rightarrow \text{ (2) } \\
\{ \text{IN} = [A] \text{ and } \text{OUT} = [] \text{ and } A \geq 0 \}\supset \\
\{ A \geq 0 \text{ and } 0=2(A–A) \text{ and } 0=(A–A)^2 \\
\text{ and IN} = [A][ ] \text{ and } \text{OUT}=[ ] \} \\
\text{read } x; \\
\{ x \geq 0 \text{ and } 0=2(A–x) \text{ and } 0=(A–x)^2 \\
\text{ and IN} = [ ] \text{ and } \text{OUT}=[ ] \} \supset \\
\{ x \geq 0 \text{ and } 0=2(A–x) \text{ and } 0=0 \text{ and } 0=(A–x)^2 \\
\text{ and } \text{OUT}=[ ] \} \}
m := 0;
{ x≥0 and m=2(A–x) and m=0 and 0=(A–x)^2 and OUT=[] } ⊃
{ x≥0 and m=2(A–x) and m=0 and 0≥0 and 0=(A–x)^2 and OUT=[] }

n := 0;
{ x≥0 and m=2(A–x) and m=n and n≥0 and 0=(A–x)^2 and OUT=[] }
s := 0
{ x≥0 and m=2(A–x) and m=n≥0 and s=(A–x)^2 and OUT=[] }

Next show that the outer loop invariant and the exit condition, followed by the write command, produce the desired final assertion.

First show the inner loop invariant is initially true by starting with the outer loop invariant, combined with the loop entry condition, and pushing it through the assignment commands before the inner loop.

{ C(x,m,n,s) and x>0 }
= \{ x≥0 and m=2(A–x) and m=n≥0 and s=(A–x)^2 and OUT=[] and x>0 \ }
\supset \{ x–1≥0 and m+2=2(A–x+1) and m+1≥0 and m+2≥0 and m+1+m+2=(A–x+1)^2 and OUT=[] \ }

= \{ D(x–1,m+1,m+2,s) \ }
since \( s=(A–x)^2 \) and \( m+2=(A–x+1) \) \supset m+1+m+2=(A–x+1)^2.
Therefore, by the assignment rule, we have:

{ C(x,m,n,s) and x>0 } \supset \{ D(x–1,m+1,m+2,s) \ }
x := x–1; n := m+2; m := m+1

Next we need to show that the inner loop invariant is preserved

{ D(x,m,n,s) and m>0 }
= \{ m := m–1; s := s+1 \ }
{ D(x,m,n,s) \ }

It suffices to show

{ D(x,m,n,s) and m>0 }
\supset \{ x≥0 and n=2(A–x) and m≥0 and n≥0 and m+s=(A–x)^2 and OUT=[] \ }
\supset \{ (m–1)+s+1=(A–x)^2 and OUT=[] \ }

To complete the proof, show that the inner loop invariant, combined with the inner loop exit condition, pushed through the assignment \( m := n \), results in the outer loop invariant.

Showing preservation of the outer loop invariant \( (3 \rightarrow 6 \rightarrow 3) \) involves executing the outer loop, so introduce the inner loop invariant D.

\( D(x,m,n,s) = \)

( x≥0 and n=2(A–x) and m≥0 and n≥0 and m+s=(A–x)^2 and OUT=[] )
Discovering a Loop Invariant

Make a table of values for a simple case and trace values for the relevant variables.

Let $A = 3$ in the previous example.

<table>
<thead>
<tr>
<th>$x$</th>
<th>$m$</th>
<th>$n$</th>
<th>$s$</th>
<th>$A-x$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>4</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>5</td>
<td>6</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>6</td>
<td>9</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Positions where the invariant $C(x,m,n,s)$ for the outer loop should hold are marked by arrows.

Note how the variable $s$ takes the values of the perfect squares, $0$, $1$, $4$, and $9$, at these locations.

The difficulty is to determine what $s$ is the square of as its values increase.

Observe that $x$ decreases as the program executes.

Since $A$ is constant, this means the value $A-x$ increases: $0$, $1$, $2$, and $3$.

This gives the relationship $s = (A-x)^2$.

Also note that $m$ is always even and increases: $0$, $2$, $4$, $6$.

This produces the relation $m = 2(A-x)$ in the outer invariant.

For the inner loop invariant, $s$ is not always a perfect square, but $m+s$ is.

Also, in the inner loop, $n$ preserves the final value for $m$ as the loop executes.

So $n$ also obeys the relationship $n = 2(A-x)$.

Finally, the loop entry conditions are combined with the value that causes loop exit.

For the outer loop, $x > 0$ is combined with $x=0$ to add the condition $x \geq 0$ to the outer loop invariant. Combined with $x \leq 0$, this gives $x=0$ at a crucial point.

In a similar way, $m > 0$ is combined with $m=0$ to add $m \geq 0$ to the inner loop invariant. Combined with $m \leq 0$, this gives $m=0$ at the appropriate point.

The condition $n \geq 0$ is added to $D$ to enable the proof to work.
Constructing Invariants

a) PRE: \( \{ N \geq 0 \} \)
   \( k := 1; \ s := 0; \)
   while \( k \leq N \) do
   \( s := s + k; \ k := k + 1 \) end while
POSt: \( \{ s = N(N+1)/2 \} \)
Loop Invariant: __________________________

b) PRE: \( \{ A > 0 \text{ and } B > 0 \} \)
   \( x := A; \ y := B; \)
   while \( x < y \) do
   if \( x > y \) then
   \( x := x - y \)
   else \( y := y - x \) end if
   end while
POST: \( \{ x = \gcd(A,B) \} \)
Loop Invariant: __________________________

c) PRE: \( \{ \text{true} \} \)
   \( k := 1; \ c := 0; \ s := 0; \)
   while \( s \leq 1000 \) do
   \( s := s + k \ast k; \ c := c + 1; \ k := k + 1 \)
   end while
POST:
\( \{ \text{"c is the smallest number of consecutive squares starting at 1 whose sum is > 1000"} \} \)
Loop Invariant: __________________________

Axiomatic Semantics for Pelican

- Assume programs have been checked for syntactic correctness.
- Transform programs so that all identifiers have unique names.

New Kind of Inference Rule

\[ H_1, H_2, \ldots, H_n \vdash H_{n+1} \]

Meaning: If \( H_{n+1} \) can be proved from \( H_1, H_2, \ldots, H_n \), then conclude that \( H \) is true.

Note: \( H_1, H_2, \ldots, H_n, H_{n+1} \) and \( H \) are generally either of the form \( \{ P \} C \{ Q \} \) or are just simple assertions.
Premises to rules may hold important information gleaned from procedure definitions.

Given declarations

\[
\begin{align*}
\text{procedure } & p_1 \text{ is } b_1; \\
\text{procedure } & p_2 \text{ (} n : \text{integer} \text{) is } b_2;
\end{align*}
\]

Form assertions (premises)

\[
\begin{align*}
\text{body}(p_1) = b_1, \\
\text{parameter}(p_2) = n, \text{ body}(p_2) = b_2
\end{align*}
\]

The information in constant declarations is added to the precondition.

Given declarations

\[
\begin{align*}
\text{const } & k=5; \\
\text{const } & f=\text{false};
\end{align*}
\]

Add these assertions to the precondition for the command that constitutes the body of the block:

\[
\begin{align*}
k=5 \text{ and } f=\text{false}
\end{align*}
\]

Note: An empty collection of assertions is equivalent to true.

In rules of inference, let “Procs” and “Const” stand for the collections of assertions that result from the declarations D in a block B.

**Rule for Blocks (Block):**

\[
\begin{align*}
\text{Procs} & \vdash \{ P \text{ and Const } \} C \{ Q \} \\
\{ P \} & \text{ D begin } C \text{ end } \{ Q \}
\end{align*}
\]

Consider an anonymous block, declare Blk:

\[
\begin{align*}
\text{declare} & \\
& \text{const } a=2; \\
& \text{const } c=-1; \\
& \text{var } m,n : \text{integer}; \\
\text{begin} & \\
& m := 99; \\
& n := a \times m + c; \\
& \text{write } n
\end{align*}
\]

Want to prove that:

\[
\begin{align*}
\{ \text{OUT} = [ ] \} & \text{ Blk } \{ \text{OUT} = [197] \}
\end{align*}
\]

Procs is empty (equivalent to true).
Const contains the assertion \( a = 2 \) and \( c = -1 \).

Proof Proceeds:

\[
\begin{align*}
\{ \text{OUT} = [ ] \text{ and } a=2 \text{ and } c=-1 \} \supset \\
\{ \text{OUT} = [ ] \text{ and } a=2 \text{ and } c=-1 \text{ and } 99=99 \} \\
\text{m := 99; } \\
\{ \text{OUT} = [ ] \text{ and } a=2 \text{ and } c=-1 \text{ and } m=99 \} \supset \\
\{ \text{OUT} = [ ] \text{ and } a=2 \text{ and } c=-1 \text{ and } a \times m+c=197 \} \\
\text{n := a} \times m+c; \\
\{ \text{OUT} = [ ] \text{ and } a=2 \text{ and } c=-1 \text{ and } n = 197 \} \\
\text{write } n \\
\{ \text{OUT} = [197] \text{ and } a=2 \text{ and } c=-1 \text{ and } n = 197 \} \supset \\
\{ \text{OUT} = [197] \}
\end{align*}
\]

**Nonrecursive Procedures**

No parameter (Call0):

\[
\begin{align*}
\{ P \} & \text{ B } \{ Q \}, \text{ body(proc) = B } \\
\{ P \} & \text{ proc } \{ Q \}
\end{align*}
\]

One parameter (Call1):

\[
\begin{align*}
\{ P \} \text{ B } \{ Q \}, \text{ body(proc)=B, parameter(proc)=F } \\
\{ P[F\rightarrow E] \} \text{ proc(E) } \{ Q[F\rightarrow E] \}
\end{align*}
\]
Example: declare Blk

\begin{verbatim}
declare
procedure addup(num : integer) is
var k : integer;
begin
  k := 1;
  while k<=num do
    sum := sum+k;
    k := k+1
  end while
end begin
  addup(A) end
\end{verbatim}

Prove

\[ \{ A \geq 0 \text{ and } sum = 0 \} \text{ Blk } \{ sum = A\cdot(A+1)/2 \} \]

For this block,

sum is nonlocal,

Procs contains the assertions

body(addup) = Bod

parameter(addup) = num,

and Const is the empty (true) assertion.

\[\text{Want to show:}\]

\[\text{body(addup) = Bod,}\]
\[\text{parameter(addup) = num}\]
\[\text{\quad \text{\small{\#}} } \{ A \geq 0 \text{ and } sum = 0 \text{ and true } \}\]
\[\text{\quad addup(A)}\]

\[\text{\quad \text{\small{\#}} } \{ sum = A\cdot(A+1)/2 \}\]

Let \( P = \{ num \geq 0 \text{ and } sum = 0 \} \)
and \( Q = \{ sum = num\cdot(num+1)/2 \} \)

Then \( P[num\to A] = \{ A \geq 0 \text{ and } sum = 0 \} \)
and \( Q[num\to A] = \{ sum = A\cdot(A+1)/2 \} \)

Using rule for a procedure invocation with a parameter, we need to show:
\[\{ num \geq 0 \text{ and } sum = 0 \}\]
\[\text{\quad k := 1;}\]
\[\text{\quad while k<=num do}\]
\[\text{\quad \quad sum := sum+k;} \quad k := k+1\]
\[\text{\quad end while}\]
\[\text{\quad \text{\small{\#}} } \{ sum = num\cdot(num+1)/2 \}\]

Notes

- The declaration \texttt{var k : integer} plays no role in the derivation.
- For the block \texttt{Bod}, Const and Procs are empty.

Conclusion

Since \( P \text{ Bod } Q \),

it follows that

\[ \{ P[num\to A] \} \text{ addup(A) } \{ Q[num\to A] \} \]

Now use (Block) to get the original assertion:
\[\{ A \geq 0 \text{ and } sum = 0 \} \text{ Blk } \{ sum = A\cdot(A+1)/2 \} \]

Parameter Restrictions

- Want pass by value semantics.
- Transform each procedure into one with a new local variable for the parameter that acts in place of the formal parameter.

\begin{verbatim}
procedure p(f : integer) is
  var local#f : integer;
begin
  f := f * f;
  write f
end
\end{verbatim}

\begin{verbatim}
procedure p(f : integer) is
  var local#f : integer;
begin
  local#f := f;
  local#f := local#f * local#f;
  write local#f
end
\end{verbatim}

- Actual parameter may not be altered inside the procedure.
- Add a new variable in the calling environment to pass the value.

\begin{verbatim}
procedure p(f : integer) is
begin
  y := y + f;
  read x
end :
p(x);
\end{verbatim}

\begin{verbatim}
procedure p(f : integer) is
begin
  y := y + f;
  read x
end :
p(new#x);
\end{verbatim}
Recursive Procedures

Example:
Find the first power of 2 bigger than 1000.
Main program:
\[
\begin{align*}
\text{pw} &:= 2; \text{cnt} := 1; \text{done} := \text{false}; \text{pow} \\
\text{procedure pow is} \\
\text{begin} \\
\text{done} := \text{pw}>1000; \\
\text{if not(done) then} \\
\text{cnt} := \text{cnt}+1; \text{pw} := 2*\text{pw}; \text{pow end if} \\
\end{align*}
\]

Using Call₀:
\[
\begin{align*}
\{P\} \text{pow} \{Q\} \\
& \quad \text{if} \ \{P_1\} \text{pow} \{Q_1\} \\
& \quad \text{if} \ \{P_2\} \text{pow} \{Q_2\} \\
& \quad \text{if} \ \{P_3\} \text{pow} \{Q_3\} \\
& \quad \text{if} \ \{P_4\} \text{pow} \{Q_4\} \\
\end{align*}
\]

New Rule: Recursion₀
\[
\begin{align*}
\{P\} \ \text{proc} \ \{Q\} & \rightarrow \ \{P\} \ B \ \{Q\}, \ \text{body}(\text{proc})=B \\
\{P\} \ \text{proc} \ \{Q\} \\
\end{align*}
\]

Continue Example:
Want to prove:

\[
\{\text{true}\} \\
\text{pw} := 2; \text{cnt} := 1; \text{done} := \text{false}; \text{pow} \\
\{\text{pw}=2^{\text{cnt}} > 1000 \text{ and } 2^{\text{cnt}-1} \leq 1000\}
\]

Recursive Assumption:
\[
\{\text{pw}=2^{\text{cnt}} \text{and } 2^{\text{cnt}-1} \leq 1000\} = P
\]

Assume \# has higher precedence than and.

Need to show the following correctness specification for the body of the procedure:
\[
\{ \text{pw}=2^{\text{cnt}} \text{and } 2^{\text{cnt}-1} \leq 1000 \} = P \\
\text{done} := \text{pw}>1000; \\
\text{if not(done) then} \\
\text{cnt} := \text{cnt}+1; \text{pw} := 2*\text{pw}; \text{pow end if} \\
\{ \text{done}=(\text{pw}>1000) \text{ and } \text{pw}=2^{\text{cnt}} \text{ and } 2^{\text{cnt}-1} \leq 1000 \} = Q
\]

We are allowed to use the recursive assumption when pow is called from within itself.

\[
P = \{ \text{pw}=2^{\text{cnt}} \text{and } 2^{\text{cnt}-1} \leq 1000 \} \supseteq \\
\{ \text{pw}>1000 \} = (\text{pw}>1000) \text{ and } \text{pw}=2^{\text{cnt}} \text{ and } 2^{\text{cnt}-1} \leq 1000 \\
\text{done} := \text{pw}>1000; \\
\{ \text{done}=(\text{pw}>1000) \text{ and } \text{pw}=2^{\text{cnt}} \text{ and } 2^{\text{cnt}-1} \leq 1000 \} = S
\]

Let B = not(done)

Case 1: S and B
S and B \supseteq \\
\{ \text{done}=\text{false} \text{ and } \text{pw}\leq1000 \text{ and } \text{pw}=2^{\text{cnt}} \text{ and } 2^{\text{cnt}-1} \leq 1000 \} \supseteq \\
\{ 2^{\text{cnt}+1} \leq 1000 \text{ and } 2*\text{pw}=2^{\text{cnt}+1} \} \\
\text{cnt} := \text{cnt}+1; \\
\{ 2^{\text{cnt}-1} \leq 1000 \text{ and } 2*\text{pw}=2^{\text{cnt}} \} \\
\text{pw} := 2*\text{pw}; \\
\{ 2^{\text{cnt}-1} \leq 1000 \text{ and } \text{pw}=2^{\text{cnt}} \} = P \\
\text{pow} \\
\{ \text{done}=(\text{pw}>1000) \text{ and } \text{pw}=2^{\text{cnt}} \text{ and } 2^{\text{cnt}-1} \leq 1000 \} = Q
\]

by the recursion assumption.

Case 2: S and not(B)
S and not(B) \supseteq \\
\{ \text{done}=(\text{pw}>1000) \text{ and } \text{pw}=2^{\text{cnt}} \text{ and } 2^{\text{cnt}-1} \leq 1000 \} = Q
Now assemble the proof:
\{ true  \} \hspace{1em} \supset \hspace{1em} \{ 2=2 \}
\{ pw := 2; \} \hspace{1em} \supset \hspace{1em} \{ pw=2 \} \hspace{1em} \supset \hspace{1em} \{ pw=2 and 1=1 \}
cnt := 1; \hspace{1em} \{ pw=2 and cnt=1 \} \hspace{1em} \supset \hspace{1em} \{ pw=2 and cnt=1 and false=false \}
done := false; \hspace{1em} \{ pw=2 and cnt=1 and done=false \} \hspace{1em} \supset \hspace{1em} \{ pw=2\text{cnt and } 2^{\text{cnt}-1} \leq 1000 \} = P
pow
\{ done=\text{(pw>1000 and pw=2\text{cnt and } 2^{\text{cnt}-1} \leq 1000)} \} = Q

For partial correctness, we can assume termination of the code.

Inspection indicates that termination of pow means that done=true.

Therefore, we may conclude:
\{ pw>1000 and pw=2\text{cnt and } 2^{\text{cnt}-1} \leq 1000 \}

which implies
\{ pw=2\text{cnt}>1000 and 2^{\text{cnt}-1} \leq 1000 \}

Want to prove:
\{ K > 0 \}
num := K;
\{ num > 0 \} = P[E]
count(num)
\{ 10^{\text{ans}-1} \leq num < 10^{\text{ans}} \}.

assuming as an induction hypotheses
\forall f(\{ f > 0 \} count(f) \{ 10^{\text{ans}-1} \leq f < 10^{\text{ans}} \}),
which is \forall f(\{ P[F\rightarrow f] \} count(f) \{ Q[F\rightarrow f] \})

Want to prove:
\{K > 0 \}
um := K;
\{ num > 0 \} = P[E]
count(num)
\{ 10^{\text{ans}-1} \leq num < 10^{\text{ans}} \}.

assuming as an induction hypotheses
\forall f(\{ f > 0 \} count(f) \{ 10^{\text{ans}-1} \leq f < 10^{\text{ans}} \}),
which is \forall f(\{ P[F\rightarrow f] \} count(f) \{ Q[F\rightarrow f] \})

Recursive Procedure with a Parameter

Recursion1
\forall f(\{ P[F\rightarrow f] \} proc(f) \{ Q[F\rightarrow f] \})
\begin{align*}
| & \{ P \} B \{ Q \}, \text{body(proc)}=B, \text{parameter(proc)}=F \\
\{ P[F\rightarrow E] \} proc(E) \{ Q[F\rightarrow E] \}
\end{align*}

Example: Number of Digits

procedure count(m : integer) is
begin
\text{if } m < 10 \text{ then }
\hspace{1em} \text{ans} := 1
\text{else }
\hspace{1em} \text{count(m/10); ans} := \text{ans}+1
\text{end if;}
end;

Use a global variable “ans” to hold the answer as we return from the recursive calls.
Use the If-Else rule.

**Case 1:** $m < 10$
- $\{ m > 0 \text{ and } m < 10 \} \supset$
- $\{ 10^{1-1} \leq m < 10^1 \}$
  $\text{ans} := 1$
- $\{ 10^{\text{ans}-1} \leq m < 10^\text{ans} \}$

**Case 2:** $m \geq 10$
- $\{ m > 0 \text{ and } m \geq 10 \} \supset$
- $\{ m/10 \geq 1 \} \supset$
- $\{ m/10 > 0 \}$
  $\text{count}(m/10) \quad \text{-- use } f = m/10$
- $\{ 10^{\text{ans}-1} \leq m/10 < 10^\text{ans} \} \supset$
- $\{ 10^{\text{ans}+1-1} \leq m < 10^{\text{ans}+1} \}$
  $\text{ans} := \text{ans}+1$
- $\{ 10^{\text{ans}-1} \leq m < 10^\text{ans} \}$

**Examples of Well-founded Orderings**
1. Natural numbers $\mathbb{N}$ ordered by $>$.  
2. Cartesian product $\mathbb{N} \times \mathbb{N}$ with a lexicographic ordering:  
   $<m_1, m_2> > <n_1, n_2>$  
   if $[m_1 > n_1]$ or $[m_1 = n_1 \text{ and } m_2 > n_2]$.  
3. The positive integers $\mathbb{P}$ ordered by the relation “properly divides”:  
   $m > n$ if $(\exists k [m = n \cdot k \text{ and } m \neq n])$.

**Steps in Showing Termination (while)**
1. Find a set $W$ with a strict well-founded ordering $>$.  
2. Find a termination expression $E$ with the properties:
   a) Whenever control passes through the top of the iterative loop, the value of $E$ is in $W$, and
   b) $E$ takes a smaller value with respect to $>$ each time the top of the iterative loop is passed.

**Termination**

Most commands terminate unconditionally.

**Problem Areas**
- Indefinite iteration (while).
- Calling a recursively defined procedure.

**Defn:** A partial order $>$ on a set $W$ is well-founded if there exists no infinite decreasing sequence of distinct elements from $W$.

**Consequence**
Given a sequence of elements $\{x_i \mid i \geq 1\}$ from $W$ such that $x_1 > x_2 > x_3 > x_4 > \ldots$, the sequence must stop (or repeat) after a finite number of elements.

If the partial order is strict (asymmetric) any decreasing sequence must have distinct elements and so must be finite.

In the context of a while command, “while $B$ do $C$ end while” with invariant $P$, the two conditions take the form

a) $P \supset E \in W$

b) $\{ P \land B \land E = A \} \land C \{ A > E \}$

**Example**

$\{ n \geq 0 \text{ and } A \geq 0 \}$

- $k := n$; $s := 1$
- while $k > 0$ do
  - $s := A \cdot s$
  - $k := k - 1$
- end while

$\{ s = A^n \}$

Take $W = \mathbb{N}$, the set of natural numbers ordered by $>$. Therefore, $m \in W$ if and only if $m \geq 0$. Take $E = k$ as the termination expression.
The loop invariant $P$ is
\[
\{ k \geq 0 \text{ and } sA^k = A^N \} 
\]

The conditions on the termination expression must hold at the location of the invariant.

The two conditions follow immediately:

a) $P \supset \{ k \geq 0 \text{ and } sA^k = A^N \} \\
E = k \in W$

b) $\{ P \text{ and } B \text{ and } E = \sigma \} \supset \{ k \geq 0 \text{ and } sA^k = A^N \text{ and } k > 0 \text{ and } \ldots \}$
\[
s := A^*s; \quad k := k-1 \\
E = k = D - 1 < D 
\]

What if $n \geq 0$ is missing from Precondition?

**Termination of Recursive Procedures**

Use an induction proof for termination.

**Example**: A procedure counts the digits in a number.

```
procedure count(m : integer) is 
begin 
if m < 10 then 
    ans := 1 
else 
    count(m/10); 
    ans := ans+1 
end if 
end;
```

This procedure terminates (normally) if it is passed a nonnegative integer.

\[
\{ num = k > 0 \} \\
count(num) \\
\{ 10^{ans-1} \leq num < 10^{ans} \}.
\]

The depth of recursion depends on the number of digits in num.

**Lemma**: If $num > 0$, the command “count(num)” halts.

Proof: Induction on the number of digits in num.

**Basis**: num has one digit, that is, $0 < num < 10$.

Then count(num) terminates because the if test succeeds.

**Induction Step**: As an induction hypothesis, assume that count(num) terminates when num has $k$ digits, namely $10^{k-1} \leq num < 10^k$.

Suppose that num has $k+1$ digits, namely $10^k \leq num < 10^{k+1}$. Then num/10 has $k$ digits.

So count(num) causes the execution of the code:

```
if num < 10 
    then ans := 1 
else count(num/10); 
    ans := ans+1 
end if
```

which terminates since count(num/10) terminates.