Errors

In expressions

Some expressions are erroneous in some states.

For example, x/y is usually considered an error in states where $y = 0$.

Also $a(i)$ is usually considered an error in states where $i < 0$ or $i \geq a.\mathrm{length}$.

In assignments

If the type of a variable is $\mathbb{N}$ (natural numbers) then it is an error to assign a negative number to it.

Correctness

Recall, correctness is as follows

Defn: A proof outline $\{\mathcal{P}\}\ \mathcal{S}\ \{\mathcal{R}\}$ **is partially correct** iff, whenever command $\mathcal{S}$ is executed beginning in any state where $\mathcal{P}$ holds,

- *no errors occur,*
- each internal assertion of $\mathcal{S}$ holds each time it is reached, and
- $\mathcal{R}$ holds if and when $\mathcal{S}$ terminates.

Thus far we have ignored the possibility of errors.

Programming rules ammended

For each expression, $\mathcal{E}$, let $\mathrm{df}(\mathcal{E})$ be a condition that is true in all states where e is defined and false where e is not defined.

E.g., $\mathrm{df}(x/y)$ might be $y \neq 0$, where x and y are reals.

E.g. $\mathrm{df}(a(i))$ might be $0 \le i < a.\mathrm{length}$, where a is a sequence and i an integer variable.

For each program variable, $\mathcal{V}$, let $\mathrm{rng}(\mathcal{V})$ be the set of values $\mathcal{V}$ can represent.

E.g. if x is of type $\mathbb{N}$ then $\mathrm{rng}(x) = \mathbb{N}$.

Now our rules are

The assignment rule (check definedness and range)

If $\mathcal{P} \Rightarrow \mathrm{df}(\mathcal{E})$ is universally true,
$\mathcal{P} \Rightarrow \mathcal{E} \in \mathrm{rng}(\mathcal{V})$ is universally true, and
$\mathcal{P} \Rightarrow \mathcal{R}[\mathcal{V} : \mathcal{E}]$ is universally true
then $\{\mathcal{P}\}\ \mathcal{V} := \mathcal{E}\ \{\mathcal{R}\}$ is correct.

The skip rule (no change)

If $\mathcal{P} \Rightarrow \mathcal{R}$ is universally true
then $\{\mathcal{P}\}\ \mathbf{skip}\ \{\mathcal{R}\}$ is correct.

The sequential composition rule (no change)

If $\{\mathcal{P}\}\ \mathcal{S}\ \{\mathcal{Q}\}$ is correct
and $\{\mathcal{Q}\}\ \mathcal{T}\ \{\mathcal{R}\}$ is correct
then $\{\mathcal{P}\}\ \mathcal{S}\ \{\mathcal{Q}\}\ \mathcal{T}\ \{\mathcal{R}\}$ is correct.

The alternation rules (check definedness)

If $\mathcal{P} \Rightarrow \mathrm{df}(\mathcal{E})$ is universally true,
$\mathcal{P} \wedge \mathcal{E} \Rightarrow \mathcal{Q}_0$ is universally true,
$\mathcal{P} \wedge \neg\mathcal{E} \Rightarrow \mathcal{Q}_1$ is universally true,
$\{\mathcal{Q}_0\}\ \mathcal{S}\ \{\mathcal{R}\}$ is correct,
and $\{\mathcal{Q}_1\}\ \mathcal{T}\ \{\mathcal{R}\}$ is correct
then $\{\mathcal{P}\}$ $\textbf{if}\ \mathcal{E}\ \textbf{then}\ \{\mathcal{Q}_0\}\ \mathcal{S}\ \textbf{else}\ \{\mathcal{Q}_1\}\ \mathcal{T}\ \textbf{end if}$ $\{\mathcal{R}\}$ is correct.

If $\mathcal{P} \Rightarrow \mathrm{df}(\mathcal{E})$ is universally true,
$\mathcal{P} \wedge \mathcal{E} \Rightarrow \mathcal{Q}$ is universally true,
$\mathcal{P} \wedge \neg\mathcal{E} \Rightarrow \mathcal{R}$ is universally true,
and $\{\mathcal{Q}\}\ \mathcal{S}\ \{\mathcal{R}\}$ is correct
then $\{\mathcal{P}\}$ $\textbf{if}\ \mathcal{E}\ \textbf{then}\ \{\mathcal{Q}\}\ \mathcal{S}\ \textbf{end if}$ $\{\mathcal{R}\}$ is correct.

Iteration rule (check definedness)

If $\mathcal{P} \Rightarrow \mathrm{df}(\mathcal{E})$ is universally true,
$\mathcal{P} \wedge \mathcal{E} \Rightarrow \mathcal{Q}$ is universally true,
$\mathcal{P} \wedge \neg\mathcal{E} \Rightarrow \mathcal{R}$ is universally true,
and $\{\mathcal{Q}\}\ \mathcal{S}\ \{\mathcal{P}\}$ is correct,
then $\{\mathcal{P}\}$ $\textbf{while}\ \mathcal{E}\ \textbf{do}\ \{\mathcal{Q}\}\ \mathcal{S}\ \textbf{end while}$ $\{\mathcal{R}\}$ is correct.

An insufficient invariant

Here is another example correct proof outline that is not provably correct.

Here j is of type int and N is any int.

$\{N \geq 1\}$
$j := 1$
$\{j = 1 \wedge N \geq 1\}$
$s := 0$
$\left\{\mathcal{I} : j \leq N \wedge s = \sum_{k \in \{1,..j\}} \frac{1}{k^2}\right\}$
while $j < N$ do
  $\{j < N \wedge \mathcal{I}\}$
  $s := s + \frac{1}{j^2}$
  $j := j + 1$
end while
$\left\{s = \sum_{k \in \{1,..N\}} \frac{1}{k^2}\right\}$

The problem is that

$$\{j < N \wedge \mathcal{I}\}\ s := s + \frac{1}{j^2}\ ;\ j := j + 1\ \{\mathcal{I}\}\text{ is not correct}$$

Consider an initial state where $j = 0$.

The invariant used above is too weak.

What invariant should we use?