Development task

Given precondition $\varphi$ and postcondition $\psi$

develop a program $S^?$ such that

$[\varphi] \xrightarrow{*} [\psi]$
Approach #1

To fulfill the development task

Given precondition $\varphi$ and postcondition $\psi$

develop a program $S$ such that $\begin{array}{c}
\varphi \quad S \\ \hline
\psi
\end{array}$

• first try to have a good idea (or draw on what you learnt at the university) and

write out a program $S$

• then verify that

$\models \begin{array}{c}
\varphi \\ S
\end{array} \quad \psi$

— or rather, prove

$\vdash \begin{array}{c}
\varphi \\ S
\end{array} \quad \psi$

Once this is done, the task is completed, and you can cash your fees.
That is, if you succeed...
Develop $S^?$ so that

$$[n \geq 0] S^? [rt^2 \leq n \land n < (rt + 1)^2]$$

(and $n$ is not modified in $S^?$)

For instance, the following looks like a plausible solution:

```
rt := 0; sqr := 0
while sqr \leq n do
    rt := rt + 1; sqr := sqr + 2 \times rt + 1
```

No, we’re not quite done yet!
Verification

We have to show:

\[ n \geq 0 \]
\[
rt := 0; \ squir := 0
\]
\[
\textbf{while} \ squir \leq n \ \textbf{do}
\]
\[
rt := rt + 1; \ squir := squir + 2 \times rt + 1
\]
\[ rt^2 \leq n \land n < (rt + 1)^2 \]
A proof attempt

For instance, by:

\[
\begin{array}{c}
\vdash \ \begin{array}{c}
\lbrack n \geq 0 \rbrack \\
rt := 0; \ \text{sqr} := 0 \\
\lbrack n \geq 0 \land rt = 0 \land \text{sqr} = 0 \rbrack \\
\text{while} \ [\text{sqr} = rt^2] \ \text{sqr} \leq n \ \text{do} \ \text{decr} \ n + 1 - rt \ \text{in Nat wrt} > \\
\text{rt} := rt + 1; \ \text{sqr} := \text{sqr} + 2 \ast rt + 1 \\
\lbrack rt^2 \leq n \land n < (rt + 1)^2 \rbrack
\end{array}
\end{array}
\]

WRONG!
What’s wrong?

Two possibilities, equally bad:

- the program does not fulfill the specification
- we are not clever enough to prove that the program fulfills the specification

In this case:

\[
\begin{align*}
\mathbf{rt} &:= 0; \mathbf{sqr} := 0 \\
\mathbf{while} \; \mathbf{sqr} \leq n \; \mathbf{do} \\
\mathbf{rt} &:= \mathbf{rt} + 1; \mathbf{sqr} := \mathbf{sqr} + 2 \times \mathbf{rt} + 1 \\
[\mathbf{rt}^2 \leq n \land n < (\mathbf{rt} + 1)^2]
\end{align*}
\]

(this may be shown, for example, by testing the program)
What now?

Trying again

\[
rt := 0; \text{sqr} := 1 \\
\text{while } \text{sqr} \leq n \text{ do} \\
\quad rt := rt + 1; \text{sqr} := \text{sqr} + 2 \times rt + 1
\]

No, we’re not quite done yet!

We have to show:

\[
[ n \geq 0 ] \\
rt := 0; \text{sqr} := 1 \\
\text{while } \text{sqr} \leq n \text{ do} \\
\quad rt := rt + 1; \text{sqr} := \text{sqr} + 2 \times rt + 1 \\
[r t^2 \leq n \land n < (rt + 1)^2]
\]
A proof attempt

For instance, by:

\[
\begin{align*}
\n & [n \geq 0] \\
& rt := 0; \; sqr := 1 \\
& [n \geq 0 \land rt = 0 \land sqr = 1] \\
& \textbf{while} [sqr = (rt + 1)^2] \; sqr \leq n \; \textbf{do} \; \textbf{decr} \; \textbf{n} + 1 - rt \; \textbf{in} \; \textbf{Nat}\; \textbf{wrt} > \\
& \quad rt := rt + 1; \; sqr := sqr + 2 \ast rt + 1 \\
& [rt^2 \leq n \land n < (rt + 1)^2]
\end{align*}
\]

WRONG AGAIN!

Well, this time we were not good enough at proving things...

A stronger loop invariant \([sqr = (rt + 1)^2 \land rt^2 \leq n]\) does the trick
Better approach

Develop the program gradually, making sure at each step that correctness is guaranteed if subsequent steps are correct

Example

Develop $S^?$ so that $[n \geq 0] S^? [rt^2 \leq n \land n < (rt + 1)^2]$

(and $n$ is not modified in $S^?$)
Step 1

We can decide to proceed via:

\[
\begin{align*}
S_1' & \quad [n \geq 0] \quad S_1' [n \geq 0 \land rt = 0 \land sqr = 1] \quad S_2' \\
S_2' & \quad [rt^2 \leq n \land n < (rt + 1)^2]
\end{align*}
\]

That is, we want to:

- **first, develop** \( S_1' \) so that

\[
[n \geq 0] \quad S_1' [n \geq 0 \land rt = 0 \land sqr = 1]
\]

- **independently, develop** \( S_2' \) so that

\[
[n \geq 0 \land rt = 0 \land sqr = 1] \quad S_2' \\
[rt^2 \leq n \land n < (rt + 1)^2]
\]

- **then, put** \( S' \equiv S_1' ; S_2' \)

Correctness follows by the assertion

\[
[n \geq 0 \land rt = 0 \land sqr = 1]
\]
Step 2

Develop $S_1^?$ so that

\[ [n \geq 0] S_1^? [n \geq 0 \land rt = 0 \land sqr = 1] \]

(and $n$ is not modified in $S_1^?$)

EASY!

Just put $S_1^?$ to be

\[ rt := 0; sqr := 1 \]

Verifies immediately!
Step 3

Develop $S_2^2$ so that

$$[n \geq 0 \land rt = 0 \land sqr = 1] S_2^2 [rt^2 \leq n \land n < (rt + 1)^2]$$

(and $n$ is not modified in $S_2^2$)

Design decision: proceed via

$$[n \geq 0 \land rt = 0 \land sqr = 1]$$

while $[\varphi]$ $b$ do $\text{decr } e$ in $W$ wrt $>$?

$S_3^2$

$$[rt^2 \leq n \land n < (rt + 1)^2]$$
Choose $W^?$ and well-founded $\succ^? \subseteq W^? \times W^?$, as well as the invariant $\varphi^?$, boolean expression $b^?$, expression $e^?$, and develop $S_3^?$ so that:

1. \[(n \geq 0 \land rt = 0 \land sqr = 1) \implies \varphi^?\]

2. \[(\varphi^? \land \neg b^?) \implies (rt^2 \leq n \land n < (rt + 1)^2)\]

3. \[\varphi^? \land b^? \]

4. \[\mathcal{E}[e^?] \succeq^? \mathcal{E}[e^?] (\mathcal{S}[S_3^?] \ s)\] for all states $s \in \{\varphi^? \land b^?\}$
Choose:

\[ \varphi^2 \equiv (sqr = (rt + 1)^2 \land rt^2 \leq n) \]

Then:

- The first requirement follows.
- Put \( b^2 \equiv (sqr \leq n) \) — and then the second requirement follows.
- Choose:
  - \( W^? = \text{Nat} \) with well-founded \( \succ^? = \succ \)
  - \( e^? = n - rt \)

Then proceed with further development...
Step 4

Develop $S_3^?$ so that

$$[sqr = (rt + 1)^2 \land rt^2 \leq n \land sqr \leq n]$$

$S_3^?$

$$[sqr = (rt + 1)^2 \land rt^2 \leq n]$$

(and $n$ is not modified in $S_3^?$)

Design decision: proceed via

$$[sqr = (rt + 1)^2 \leq n \land sqr \leq n]$$

$S_4^?$

$$[sqr = rt^2 \leq n]$$

$S_5^?$

$$[sqr = (rt + 1)^2 \land rt^2 \leq n]$$
Let’s not forget:
termination conditions are a part of the requirements

For $S_3^2$ we also require:

- $\mathcal{E}[n - rt] s > \mathcal{E}[n - rt] (S[S_3^2] s)$ for $s \in \{sqr = (rt + 1)^2 \leq n \land rt^2 \leq n\}$

To ensure this, we impose:

- $\mathcal{E}[n - rt] s \geq \mathcal{E}[n - rt] (S[S_4^2] s)$ for $s \in \{sqr = (rt + 1)^2 \leq n \land rt^2 \leq n\}$

- $\mathcal{E}[n - rt] s \geq \mathcal{E}[n - rt] (S[S_5^2] s)$ for $s \in \{sqr = rt^2 \leq n\}$

with at least one of the two inequalities being strict
Steps 5 & 6

Put $S_4$ to be

$$rt := rt + 1$$

and $S_5$ to be

$$sqr := sqr + 2 \times rt + 1$$

Verifies immediately!
(including termination conditions)

EASY!
Putting all the steps together

\[
[n \geq 0] \\
\text{rt} := 0; \text{sqr} := 1 \\
[n \geq 0 \land rt = 0 \land sqr = 1] \\
\text{while } [sqr = (rt + 1)^2 \land rt^2 \leq n] \quad \text{sqr} \leq n \text{ do } \text{decr } n - rt \text{ in Nat wrt } > \\
\quad (rt := rt + 1 \quad [sqr = rt^2 \leq n] \quad \text{sqr} := \text{sqr} + 2 \ast rt + 1) \\
[rt^2 \leq n \land n < (rt + 1)^2]
\]

Correctness by construction!!!

...with proofs ready for use!
Making all this more abstract, and hence more general

Specifications and formal program development