university of groningen

Program Correctness

Block 4

Jorge A. Pérez
(based on slides by Arnold Meijster)

Bernoulli Institute for Mathematics, Computer Science, and AI
University of Groningen, Groningen, the Netherlands

February 26, 2023

Outline

Exercise 7.1: Powers

Exercise 7.2: Factorial

Exercise 7.8: Dijkstra's FUSC

Summing an array

Exercise 7.1

const $n :\ \mathbb{N}$;
var $x,\ y :\ \mathbb{Z}$;
$\{P :\ \textbf{true}\}$
T
$\{Q :\ x = n^2 \wedge y = n^3\}$

- We are only allowed to multiply by 2 and 3, and use addition.
- Use "replace a constant by a variable" to find J and B.

Exercise 7.1: Invariant and Guard

$$P : \textbf{true}$$
$$Q : x = n^2 \wedge y = n^3$$

0 We decide that we need a **while**-program: we are not allowed to use assignments $x := n * n;\ y := n * x;$

1 Choose an invariant J, and guard B such that $J \wedge \neg B \Rightarrow Q$.

Exercise 7.1: Invariant and Guard

$$P : \textbf{true}$$
$$Q : x = n^2 \wedge y = n^3$$

0 We decide that we need a **while**-program: we are not allowed to use assignments $x := n * n;\ y := n * x;$

1 Choose an invariant J, and guard B such that $J \wedge \neg B \Rightarrow Q$. We replace the constant n by the variable k:

$$J : x = k^2 \wedge y = k^3 \wedge 0 \leq k \leq n$$
$$B : k \neq n$$

Clearly, J and $\neg B$ imply Q.

Exercise 7.1: Initialization and Variant

$$P : \textbf{true}$$
$$Q : x = n^2 \wedge y = n^3$$
$$J : x = k^2 \wedge y = k^3 \wedge 0 \le k \le n$$
$$B : k \ne n$$

2 **Initialization**: Find T_0 such that $\{P\}$ T_0 $\{J\}$.

$\{P : \textbf{true}\}$

(* *calculus;* $n \in \mathbb{N}$ *)

$\{0 = 0^2 \wedge 0 = 0^3 \wedge 0 \le 0 \le n\}$

$k := 0;\ x := 0;\ y := 0;$

$\{J :\ x = k^2 \wedge y = k^3 \wedge 0 \le k \le n\}$

Exercise 7.1: Initialization and Variant

$$P : \textbf{true}$$
$$Q : x = n^2 \wedge y = n^3$$
$$J : x = k^2 \wedge y = k^3 \wedge 0 \leq k \leq n$$
$$B : k \neq n$$

2 **Initialization**: Find T_0 such that $\{P\}\ T_0\ \{J\}$.

$\{P : \textbf{true}\}$
(* *calculus;* $n \in \mathbb{N}$ *)
$\{0 = 0^2 \wedge 0 = 0^3 \wedge 0 \leq 0 \leq n\}$
$k := 0;\ x := 0;\ y := 0;$
$\{J :\ x = k^2 \wedge y = k^3 \wedge 0 \leq k \leq n\}$

3 **Variant**: We take $vf = n - k \in \mathbb{Z}$. We must show $vf \geq 0$. Clearly, $J \wedge B \Rightarrow n - k \geq 0$ as J contains the conjunct $k \leq n$.

Exercise 7.1: Body of the Loop

P : **true**

$Q : x = n^2 \wedge y = n^3$

$J : x = k^2 \wedge y = k^3 \wedge 0 \leq k \leq n$

$B : k \neq n$

We can relate x, y, and k. Actually, we look into $k + 1$ (why?):

$$\begin{aligned}(k+1)^3 &= k^3 + 3k^2 + 3k + 1 \\ &= k^3 + 3(k^2 + k) + 1 \\ &\qquad \{y = k^3, x = k^2\} \\ &= y + 3(x + k) + 1\end{aligned}$$

Similarly:

$$\begin{aligned}(k+1)^2 &= k^2 + 2k + 1 \\ &= x + 2k + 1\end{aligned}$$

We shall use these equalities in the body of the loop.

Exercise 7.1: Body of the Loop

$$J : x = k^2 \wedge y = k^3 \wedge 0 \leq k \leq n$$
$$B : k \neq n$$

4 Body of the loop: $\{J \wedge B \wedge vf = V\}\ S\ \{J \wedge vf < V\}$

$\{J \wedge B \wedge vf = V\}$

$y := y + 3 * (x + k) + 1;$

$x := x + 2 * k + 1;$

$k := k + 1;$

$\{J \wedge vf < V\}$

Exercise 7.1: Body of the Loop

$$J : x = k^2 \wedge y = k^3 \wedge 0 \leq k \leq n$$
$$B : k \neq n$$

4 Body of the loop: $\{J \wedge B \wedge vf = V\}\ S\ \{J \wedge vf < V\}$

$\{J \wedge B \wedge vf = V\}$
$\{x = k^2 \ \wedge\ y = k^3 \ \wedge\ 0 \leq k \leq n \ \wedge\ k \neq n \ \wedge\ n - k = V\}$

$y := y + 3 * (x + k) + 1;$

$x := x + 2 * k + 1;$

$k := k + 1;$

$\{J \wedge vf < V\}$

Exercise 7.1: Body of the Loop

$$J : x = k^2 \wedge y = k^3 \wedge 0 \leq k \leq n$$
$$B : k \neq n$$

4 Body of the loop: $\{J \wedge B \wedge vf = V\}\ S\ \{J \wedge vf < V\}$

$\{J \wedge B \wedge vf = V\}$
$\{x = k^2 \ \wedge\ y = k^3 \ \wedge\ 0 \leq k \leq n \ \wedge\ k \neq n \ \wedge\ n - k = V\}$
(* *prepare assignment to* y*: use* $(k+1)^3 = y + 3(x+k) + 1$ *)

$y := y + 3 * (x + k) + 1;$

$x := x + 2 * k + 1;$

$k := k + 1;$

$\{J \wedge vf < V\}$

Exercise 7.1: Body of the Loop

$$J : x = k^2 \wedge y = k^3 \wedge 0 \le k \le n$$
$$B : k \ne n$$

4 Body of the loop: $\{J \wedge B \wedge vf = V\}\ S\ \{J \wedge vf < V\}$

$\{J \wedge B \wedge vf = V\}$
$\{x = k^2 \ \wedge\ y = k^3 \ \wedge\ 0 \le k \le n \ \wedge\ k \ne n \ \wedge\ n - k = V\}$
(* *prepare assignment to* y*: use* $(k+1)^3 = y + 3(x+k) + 1$ *)
$\{x = k^2 \ \wedge\ y + 3(x+k) + 1 = (k+1)^3 \ \wedge\ 0 \le k < n \ \wedge\ n - k = V\}$
$y := y + 3 * (x + k) + 1;$

$x := x + 2 * k + 1;$

$k := k + 1;$

$\{J \wedge vf < V\}$

Exercise 7.1: Body of the Loop

$$J : x = k^2 \wedge y = k^3 \wedge 0 \leq k \leq n$$
$$B : k \neq n$$

4 Body of the loop: $\{J \wedge B \wedge vf = V\}\ S\ \{J \wedge vf < V\}$

$\{J \wedge B \wedge vf = V\}$
$\{x = k^2 \ \wedge\ y = k^3 \ \wedge\ 0 \leq k \leq n \ \wedge\ k \neq n \ \wedge\ n - k = V\}$
(* *prepare assignment to* y*: use* $(k+1)^3 = y + 3(x+k) + 1$ *)
$\{x = k^2 \ \wedge\ y + 3(x+k) + 1 = (k+1)^3 \ \wedge\ 0 \leq k < n \ \wedge\ n - k = V\}$
$y := y + 3 * (x + k) + 1;$
$\{x = k^2 \ \wedge\ y = (k+1)^3 \ \wedge\ 0 \leq k < n \ \wedge\ n - k = V\}$

$x := x + 2 * k + 1;$

$k := k + 1;$

$\{J \wedge vf < V\}$

Exercise 7.1: Body of the Loop

$$J : x = k^2 \wedge y = k^3 \wedge 0 \le k \le n$$
$$B : k \neq n$$

4 Body of the loop: $\{J \wedge B \wedge vf = V\}\ S\ \{J \wedge vf < V\}$

$\{J \wedge B \wedge vf = V\}$
$\{x = k^2 \ \wedge\ y = k^3 \ \wedge\ 0 \le k \le n \ \wedge\ k \neq n \ \wedge\ n - k = V\}$
(* *prepare assignment to* y*: use* $(k+1)^3 = y + 3(x+k) + 1$ *)
$\{x = k^2 \ \wedge\ y + 3(x+k) + 1 = (k+1)^3 \ \wedge\ 0 \le k < n \ \wedge\ n - k = V\}$
$y := y + 3 * (x + k) + 1;$
$\{x = k^2 \ \wedge\ y = (k+1)^3 \ \wedge\ 0 \le k < n \ \wedge\ n - k = V\}$
(* *prepare assignment to* x*: use* $(k+1)^2 = x + 2k + 1$ *)

$x := x + 2 * k + 1;$

$k := k + 1;$

$\{J \wedge vf < V\}$

Exercise 7.1: Body of the Loop

$$J : x = k^2 \wedge y = k^3 \wedge 0 \leq k \leq n$$
$$B : k \neq n$$

4 Body of the loop: $\{J \wedge B \wedge vf = V\}\ S\ \{J \wedge vf < V\}$

$\{J \wedge B \wedge vf = V\}$
$\{x = k^2 \ \wedge\ y = k^3 \ \wedge\ 0 \leq k \leq n \ \wedge\ k \neq n \ \wedge\ n - k = V\}$
(* *prepare assignment to* y*: use* $(k+1)^3 = y + 3(x+k) + 1$ *)
$\{x = k^2 \ \wedge\ y + 3(x+k) + 1 = (k+1)^3 \ \wedge\ 0 \leq k < n \ \wedge\ n - k = V\}$
$y := y + 3 * (x + k) + 1;$
$\{x = k^2 \ \wedge\ y = (k+1)^3 \ \wedge\ 0 \leq k < n \ \wedge\ n - k = V\}$
(* *prepare assignment to* x*: use* $(k+1)^2 = x + 2k + 1$ *)
$\{x + 2k + 1 = (k+1)^2 \wedge y = (k+1)^3 \ \wedge\ 0 \leq k < n \ \wedge\ n - k = V\}$
$x := x + 2 * k + 1;$

$k := k + 1;$

$\{J \wedge vf < V\}$

Exercise 7.1: Body of the Loop

$$J : x = k^2 \wedge y = k^3 \wedge 0 \leq k \leq n$$
$$B : k \neq n$$

4 Body of the loop: $\{J \wedge B \wedge vf = V\}\ S\ \{J \wedge vf < V\}$

$\{J \wedge B \wedge vf = V\}$
$\{x = k^2 \wedge y = k^3 \wedge 0 \leq k \leq n \wedge k \neq n \wedge n - k = V\}$
(* *prepare assignment to* y*: use* $(k+1)^3 = y + 3(x+k) + 1$ *)
$\{x = k^2 \wedge y + 3(x+k) + 1 = (k+1)^3 \wedge 0 \leq k < n \wedge n - k = V\}$
$y := y + 3 * (x + k) + 1;$
$\{x = k^2 \wedge y = (k+1)^3 \wedge 0 \leq k < n \wedge n - k = V\}$
(* *prepare assignment to* x*: use* $(k+1)^2 = x + 2k + 1$ *)
$\{x + 2k + 1 = (k+1)^2 \wedge y = (k+1)^3 \wedge 0 \leq k < n \wedge n - k = V\}$
$x := x + 2 * k + 1;$
$\{x = (k+1)^2 \wedge y = (k+1)^3 \wedge 0 \leq k < n \wedge n - k = V\}$

$k := k + 1;$

$\{J \wedge vf < V\}$

Exercise 7.1: Body of the Loop

$$J : x = k^2 \wedge y = k^3 \wedge 0 \leq k \leq n$$
$$B : k \neq n$$

4 Body of the loop: $\{J \wedge B \wedge vf = V\}\ S\ \{J \wedge vf < V\}$

$\{J \wedge B \wedge vf = V\}$
$\{x = k^2 \ \wedge \ y = k^3 \ \wedge \ 0 \leq k \leq n \ \wedge \ k \neq n \ \wedge \ n - k = V\}$
(* *prepare assignment to* y*: use* $(k+1)^3 = y + 3(x+k) + 1$ *)
$\{x = k^2 \ \wedge \ y + 3(x+k) + 1 = (k+1)^3 \ \wedge \ 0 \leq k < n \ \wedge \ n - k = V\}$
$y := y + 3 * (x + k) + 1;$
$\{x = k^2 \ \wedge \ y = (k+1)^3 \ \wedge \ 0 \leq k < n \ \wedge \ n - k = V\}$
(* *prepare assignment to* x*: use* $(k+1)^2 = x + 2k + 1$ *)
$\{x + 2k + 1 = (k+1)^2 \wedge y = (k+1)^3 \ \wedge \ 0 \leq k < n \ \wedge \ n - k = V\}$
$x := x + 2 * k + 1;$
$\{x = (k+1)^2 \wedge y = (k+1)^3 \ \wedge \ 0 \leq k < n \ \wedge \ n - k = V\}$
(* *complete preparation for* $k := k + 1$ *)

$k := k + 1;$

$\{J \wedge vf < V\}$

Exercise 7.1: Body of the Loop

$$J : x = k^2 \wedge y = k^3 \wedge 0 \leq k \leq n$$
$$B : k \neq n$$

4 Body of the loop: $\{J \wedge B \wedge vf = V\}\ S\ \{J \wedge vf < V\}$

$\{J \wedge B \wedge vf = V\}$
$\{x = k^2 \ \wedge\ y = k^3 \ \wedge\ 0 \leq k \leq n \ \wedge\ k \neq n \ \wedge\ n - k = V\}$
(* *prepare assignment to* y*: use* $(k+1)^3 = y + 3(x+k) + 1$ *)
$\{x = k^2 \ \wedge\ y + 3(x+k) + 1 = (k+1)^3 \ \wedge\ 0 \leq k < n \ \wedge\ n - k = V\}$
$y := y + 3 * (x + k) + 1;$
$\{x = k^2 \ \wedge\ y = (k+1)^3 \ \wedge\ 0 \leq k < n \ \wedge\ n - k = V\}$
(* *prepare assignment to* x*: use* $(k+1)^2 = x + 2k + 1$ *)
$\{x + 2k + 1 = (k+1)^2 \wedge y = (k+1)^3 \ \wedge\ 0 \leq k < n \ \wedge\ n - k = V\}$
$x := x + 2 * k + 1;$
$\{x = (k+1)^2 \wedge y = (k+1)^3 \ \wedge\ 0 \leq k < n \ \wedge\ n - k = V\}$
(* *complete preparation for* $k := k + 1$ *)
$\{x = (k+1)^2 \wedge y = (k+1)^3 \ \wedge\ 0 \leq k + 1 \leq n \ \wedge\ n - (k+1) < V\}$
$k := k + 1;$

$\{J \wedge vf < V\}$

Exercise 7.1: Body of the Loop

$$J : x = k^2 \wedge y = k^3 \wedge 0 \leq k \leq n$$
$$B : k \neq n$$

4 Body of the loop: $\{J \wedge B \wedge vf = V\}\ S\ \{J \wedge vf < V\}$

$\{J \wedge B \wedge vf = V\}$
$\{x = k^2 \ \wedge\ y = k^3 \ \wedge\ 0 \leq k \leq n \ \wedge\ k \neq n \ \wedge\ n - k = V\}$
(* *prepare assignment to* y*: use* $(k+1)^3 = y + 3(x+k) + 1$ *)
$\{x = k^2 \ \wedge\ y + 3(x+k) + 1 = (k+1)^3 \ \wedge\ 0 \leq k < n \ \wedge\ n - k = V\}$
$y := y + 3 * (x + k) + 1;$
$\{x = k^2 \ \wedge\ y = (k+1)^3 \ \wedge\ 0 \leq k < n \ \wedge\ n - k = V\}$
(* *prepare assignment to* x*: use* $(k+1)^2 = x + 2k + 1$ *)
$\{x + 2k + 1 = (k+1)^2 \wedge y = (k+1)^3 \ \wedge\ 0 \leq k < n \ \wedge\ n - k = V\}$
$x := x + 2 * k + 1;$
$\{x = (k+1)^2 \wedge y = (k+1)^3 \ \wedge\ 0 \leq k < n \ \wedge\ n - k = V\}$
(* *complete preparation for* $k := k + 1$ *)
$\{x = (k+1)^2 \wedge y = (k+1)^3 \ \wedge\ 0 \leq k + 1 \leq n \ \wedge\ n - (k+1) < V\}$
$k := k + 1;$
$\{x = k^2 \wedge y = k^3 \ \wedge\ 0 \leq k \leq n \ \wedge\ n - k < V\}$
$\{J \wedge vf < V\}$

Exercise 7.1: Conclusion

5 The command $\{P\}\ T_0;$ **while** B **do** S **end** $\{Q\}$ solves the problem:

const $n :\ \mathbb{N};$
var $x,\ y,\ k :\ \mathbb{Z};$
  $\{P :\ \textbf{true}\}$
$k := 0;$
$x := 0;$
$y := 0;$
  $\{J : x = k^2 \wedge y = k^3 \wedge 0 \le k \le n\}$
    $(^*\ vf = n - k\ ^*)$
while $k \neq n$ **do**
  $y := y + 3 * x + 3 * k + 1;$
  $x := x + 2 * k + 1;$
  $k := k + 1;$
end;
  $\{Q :\ x = n^2 \wedge y = n^3\}$

Outline

Exercise 7.2: Factorial

$$\begin{array}{l}\textbf{var } x,\ n:\ \mathbb{Z};\\ \quad \{P:\ n \geq 0 \wedge X = n!\}\\ T\\ \quad \{Q:\ x = X\}\end{array}$$

Recall the heuristic generalization.

Exercise 7.2: Invariant and Guard

$$P: \; n \geq 0 \wedge X = n!$$
$$Q: x = X$$

0 We assume that there is no function '**fact**' available.
We decide that we need a **while**-program.

1 Choose an invariant J, and guard B such that $J \wedge \neg B \Rightarrow Q$.
We use the heuristic generalization.

$$J: (x \cdot n! = X) \wedge n \geq 0$$
$$B: n \neq 0$$

By definition $0! = 1$.
Therefore, J and $\neg B$ imply Q.

Exercise 7.2: Initialization and Variant

$$
\begin{array}{|l|}
\hline
P: \; n \geq 0 \wedge X = n! \\
Q: x = X \\
J: x \cdot n! = X \wedge n \geq 0 \\
B: n \neq 0 \\
\hline
\end{array}
$$

2 Initialization: Find a command T_0 such that $\{P\}$ T_0 $\{J\}$

$\{P : X = n! \wedge n \geq 0\}$

(* *calculus* *)

$\{X = 1 \cdot n! \wedge n \geq 0\}$

$x := 1;$

$\{J : \; x \cdot n! = X \wedge n \geq 0\}$

3 Variant function: $vf \in \mathbb{Z}$ and $J \wedge B \Rightarrow vf \geq 0$
Clearly, n must decrease until $n = 0$. We choose $vf = n \in \mathbb{N}$.
Because J contains the conjunct $n \geq 0$, we have that
$J \wedge B \Rightarrow vf \geq 0$ holds trivially.

Exercise 7.2: Body of the Loop

$$\boxed{\begin{aligned} J &: x \cdot n! = X \wedge n \geq 0 \\ B &: n \neq 0 \\ vf &= n \end{aligned}}$$

4 Body of the loop: $\{J \wedge B \wedge vf = V\}\ S\ \{J \wedge vf < V\}$

$\{J \wedge B \wedge vf = V\}$

$\{J \wedge vf < V\}$

Exercise 7.2: Body of the Loop

$$J : x \cdot n! = X \wedge n \geq 0$$
$$B : n \neq 0$$
$$vf = n$$

4 Body of the loop: $\{J \wedge B \wedge vf = V\}\ S\ \{J \wedge vf < V\}$

$\{J \wedge B \wedge vf = V\}$
$\{x \cdot n! = X \ \wedge\ n \geq 0 \ \wedge\ n \neq 0 \wedge n = V\}$

$\{J \wedge vf < V\}$

Exercise 7.2: Body of the Loop

$$J : x \cdot n! = X \wedge n \geq 0$$
$$B : n \neq 0$$
$$vf = n$$

4 Body of the loop: $\{J \wedge B \wedge vf = V\}\ S\ \{J \wedge vf < V\}$

$\{J \wedge B \wedge vf = V\}$
$\{x \cdot n! = X \ \wedge \ n \geq 0 \ \wedge \ n \neq 0 \wedge n = V\}$
$(^*\ n = V > 0 \Rightarrow n! = n \cdot (n-1)! \wedge n - 1 \geq 0 \wedge n - 1 < V\ ^*)$

$\{J \wedge vf < V\}$

Exercise 7.2: Body of the Loop

$$J : x \cdot n! = X \wedge n \geq 0$$
$$B : n \neq 0$$
$$vf = n$$

4 Body of the loop: $\{J \wedge B \wedge vf = V\}$ S $\{J \wedge vf < V\}$

$\{J \wedge B \wedge vf = V\}$
$\{x \cdot n! = X \ \wedge \ n \geq 0 \ \wedge \ n \neq 0 \wedge n = V\}$
(* $n = V > 0 \Rightarrow n! = n \cdot (n-1)! \wedge n - 1 \geq 0 \wedge n - 1 < V$ *)
$\{x \cdot n \cdot (n-1)! = X \ \wedge \ n - 1 \geq 0 \ \wedge \ n - 1 < V\}$

$\{J \wedge vf < V\}$

Exercise 7.2: Body of the Loop

$$J : x \cdot n! = X \wedge n \geq 0$$
$$B : n \neq 0$$
$$vf = n$$

4 Body of the loop: $\{J \wedge B \wedge vf = V\}\ S\ \{J \wedge vf < V\}$

$\{J \wedge B \wedge vf = V\}$
$\{x \cdot n! = X \ \wedge\ n \geq 0 \ \wedge\ n \neq 0 \wedge n = V\}$
$(^*\ n = V > 0 \Rightarrow n! = n \cdot (n-1)! \wedge n-1 \geq 0 \wedge n-1 < V\ ^*)$
$\{x \cdot n \cdot (n-1)! = X \ \wedge\ n-1 \geq 0 \ \wedge\ n-1 < V\}$
$x := x * n;$

$\{J \wedge vf < V\}$

Exercise 7.2: Body of the Loop

$$J : x \cdot n! = X \wedge n \geq 0$$
$$B : n \neq 0$$
$$vf = n$$

4 Body of the loop: $\{J \wedge B \wedge vf = V\}\ S\ \{J \wedge vf < V\}$

$\{J \wedge B \wedge vf = V\}$
$\{x \cdot n! = X \ \wedge \ n \geq 0 \ \wedge \ n \neq 0 \wedge n = V\}$
(* $n = V > 0 \Rightarrow n! = n \cdot (n-1)! \wedge n - 1 \geq 0 \wedge n - 1 < V$ *)
$\{x \cdot n \cdot (n-1)! = X \ \wedge \ n - 1 \geq 0 \ \wedge \ n - 1 < V\}$
$x := x * n;$
$\{x \cdot (n-1)! = X \ \wedge \ n - 1 \geq 0 \ \wedge \ n - 1 < V\}$

$\{J \wedge vf < V\}$

Exercise 7.2: Body of the Loop

$$\boxed{\begin{aligned} J &: x \cdot n! = X \wedge n \geq 0 \\ B &: n \neq 0 \\ vf &= n \end{aligned}}$$

4 Body of the loop: $\{J \wedge B \wedge vf = V\}\ S\ \{J \wedge vf < V\}$

$\{J \wedge B \wedge vf = V\}$
$\{x \cdot n! = X \ \wedge \ n \geq 0 \ \wedge \ n \neq 0 \wedge n = V\}$
(* $n = V > 0 \Rightarrow n! = n \cdot (n-1)! \wedge n - 1 \geq 0 \wedge n - 1 < V$ *)
$\{x \cdot n \cdot (n-1)! = X \ \wedge \ n - 1 \geq 0 \ \wedge \ n - 1 < V\}$
$x := x * n;$
$\{x \cdot (n-1)! = X \ \wedge \ n - 1 \geq 0 \ \wedge \ n - 1 < V\}$
$n := n - 1;$

$\{J \wedge vf < V\}$

Exercise 7.2: Body of the Loop

$$J : x \cdot n! = X \wedge n \geq 0$$
$$B : n \neq 0$$
$$vf = n$$

4 Body of the loop: $\{J \wedge B \wedge vf = V\}\ S\ \{J \wedge vf < V\}$

$\{J \wedge B \wedge vf = V\}$
$\{x \cdot n! = X \ \wedge\ n \geq 0 \ \wedge\ n \neq 0 \wedge n = V\}$
(* $n = V > 0 \Rightarrow n! = n \cdot (n-1)! \wedge n - 1 \geq 0 \wedge n - 1 < V$ *)
$\{x \cdot n \cdot (n-1)! = X \ \wedge\ n - 1 \geq 0 \ \wedge\ n - 1 < V\}$
$x := x * n;$
$\{x \cdot (n-1)! = X \ \wedge\ n - 1 \geq 0 \ \wedge\ n - 1 < V\}$
$n := n - 1;$
$\{x \cdot n! = X \wedge n \geq 0 \wedge n < V\}$
$\{J \wedge vf < V\}$

Exercise 7.2: Conclusion

5 The command $\{P\}\ T_0;$ **while** B **do** S **end** $\{Q\}$ solves the problem:

$$
\begin{array}{l}
\textbf{var}\ x,\ n:\ \mathbb{Z};\\
\quad \{P:\ X = n! \wedge n \geq 0\}\\
x := 1;\\
\quad \{J : x \cdot n! = X \wedge n \geq 0\}\\
\qquad (^*\ vf = n\ ^*)\\
\textbf{while}\ n \neq 0\ \textbf{do}\\
\quad x := x * n;\\
\quad n := n - 1;\\
\textbf{end};\\
\{Q:\ x = X\}
\end{array}
$$

Outline

Exercise 7.1: Powers

Exercise 7.2: Factorial

Exercise 7.8: Dijkstra's FUSC

Summing an array

Exercise 7.8: FUSC

Dijkstra's FUSC function (check EWD 570):

$$\begin{aligned} f(0) &= 0 \\ f(1) &= 1 \\ f(2 \cdot n) &= f(n) \\ f(2 \cdot n + 1) &= f(n) + f(n + 1) \end{aligned}$$

Exercise 7.8: FUSC

Dijkstra's FUSC function (check EWD 570):

$$
\begin{aligned}
f(0) &= 0 \\
f(1) &= 1 \\
f(2 \cdot n) &= f(n) \\
f(2 \cdot n + 1) &= f(n) + f(n+1)
\end{aligned}
$$

For instance:

$$f(2) = f(2 \cdot 1) = f(1) = 1$$

Exercise 7.8: FUSC

Dijkstra's FUSC function (check EWD 570):

$$\begin{aligned} f(0) &= 0 \\ f(1) &= 1 \\ f(2 \cdot n) &= f(n) \\ f(2 \cdot n + 1) &= f(n) + f(n+1) \end{aligned}$$

For instance:

$$\begin{aligned} f(2) &= f(2 \cdot 1) = f(1) = 1 \\ f(3) &= f(2 \cdot 1 + 1) = f(1) + f(1+1) = 1 + 1 = 2 \end{aligned}$$

Exercise 7.8: FUSC

Dijkstra's FUSC function (check EWD 570):

$$
\begin{aligned}
f(0) &= 0 \\
f(1) &= 1 \\
f(2 \cdot n) &= f(n) \\
f(2 \cdot n + 1) &= f(n) + f(n+1)
\end{aligned}
$$

For instance:

$$
\begin{aligned}
&f(2) = f(2 \cdot 1) = f(1) = 1 \\
&f(3) = f(2 \cdot 1 + 1) = f(1) + f(1 + 1) = 1 + 1 = 2 \\
&f(4) = f(2 \cdot 2) = f(2) = 1
\end{aligned}
$$

Exercise 7.8: FUSC

Dijkstra's FUSC function (check EWD 570):

$$
\begin{aligned}
f(0) &= 0 \\
f(1) &= 1 \\
f(2 \cdot n) &= f(n) \\
f(2 \cdot n + 1) &= f(n) + f(n+1)
\end{aligned}
$$

For instance:

$$
\begin{aligned}
f(2) &= f(2 \cdot 1) = f(1) = 1 \\
f(3) &= f(2 \cdot 1 + 1) = f(1) + f(1+1) = 1 + 1 = 2 \\
f(4) &= f(2 \cdot 2) = f(2) = 1 \\
f(5) &= \ ??
\end{aligned}
$$

Exercise 7.8: FUSC

Dijkstra's FUSC function (check EWD 570):

$$
\begin{aligned}
f(0) &= 0 \\
f(1) &= 1 \\
f(2 \cdot n) &= f(n) \\
f(2 \cdot n + 1) &= f(n) + f(n+1)
\end{aligned}
$$

For instance:

$$
\begin{aligned}
&f(2) = f(2 \cdot 1) = f(1) = 1 \\
&f(3) = f(2 \cdot 1 + 1) = f(1) + f(1+1) = 1 + 1 = 2 \\
&f(4) = f(2 \cdot 2) = f(2) = 1 \\
&f(5) = f(2) + f(3) = 3
\end{aligned}
$$

Exercise 7.8: FUSC

Dijkstra's FUSC function (check EWD 570):

$$\begin{aligned} f(0) &= 0 \\ f(1) &= 1 \\ f(2 \cdot n) &= f(n) \\ f(2 \cdot n + 1) &= f(n) + f(n+1) \end{aligned}$$

Also notice:

$$\begin{aligned} f(1) &= 1 \\ &= 0 + 1 \\ &= f(0) + f(0+1) \\ &= f(2 \cdot 0 + 1) \end{aligned}$$

Exercise 7.8: FUSC

Dijkstra's FUSC function:

$$\begin{aligned} f(0) &= 0 \\ f(1) &= 1 \\ f(2\cdot n) &= f(n) \\ f(2\cdot n+1) &= f(n)+f(n+1) \end{aligned}$$

We consider the specification:

var $n,\ x:\ \mathbb{Z}$;
  $\{P:\ n \geq 0 \wedge Z = f(n)\}$
T
  $\{Q:\ Z = x\}$

Hint:
Use $Z = y\cdot f(n) + x\cdot f(n+1)$ in the invariant.

Exercise 7.8: FUSC

$$P : n \geq 0 \wedge Z = f(n)$$
$$Q : Z = x$$

0 We decide that we need a **while**-program: We only have a recurrence for $f(n)$, so we need iteration.

1 Choose an invariant J, and guard B such that $J \wedge \neg B \Rightarrow Q$. Following the hint, we choose:

$$J : n \geq 0 \wedge (Z = y \cdot f(n) + x \cdot f(n+1))$$
$$B : n \neq 0$$

We have:

$$\begin{aligned} J \wedge \neg B \Rightarrow Z &= y \cdot f(0) + x \cdot f(0+1) \\ Z &= y \cdot 0 + x \cdot 1 \\ Z &= x \end{aligned}$$

Exercise 7.8: Initialization and Variant

$$\begin{aligned} f(0) &= 0 \\ f(1) &= 1 \\ f(2\cdot n) &= f(n) \\ f(2\cdot n+1) &= f(n)+f(n+1) \end{aligned}$$

$$\begin{aligned} &P: n \geq 0 \wedge Z = f(n) \\ &Q: Z = x \\ &J: n \geq 0 \wedge Z = y\cdot f(n) + x\cdot f(n+1) \\ &B: n \neq 0 \end{aligned}$$

2 Initialization: Find a command T_0 such that $\{P\}\ T_0\ \{J\}$

$\{P:\ n \geq 0 \wedge Z = f(n)\}$
(* *calculus;* $f(n)$ *is defined for* $n \geq 0$ *)
$\{n \geq 0 \wedge Z = 1\cdot f(n) + 0\cdot f(n+1)\}$
$y := 1;\ x := 0;$
$\{J:\ n \geq 0 \wedge Z = y\cdot f(n) + x\cdot f(n+1)\}$

3 Variant function: $vf \in \mathbb{Z}$ and $J \wedge B \Rightarrow vf \geq 0$.
We choose $vf = n \in \mathbb{Z}$ and so $J \wedge B \Rightarrow vf \geq 0$, because J contains the conjunct $n \geq 0$.

Exercise 7.8: Body of the Loop (1/3)

By observing the inductive part of the definition of f:

$$f(2 \cdot n) = f(n)$$
$$f(2 \cdot n + 1) = f(n) + f(n+1)$$

We infer that we should work towards a command of the form:

$\{J:\ n \geq 0 \land Z = y \cdot f(n) + x \cdot f(n+1)\ \land\ B:\ n \neq 0\ \land\ n = V\}$
while $n \neq 0$ **do**
  if n **mod** $2 = 0$ **then**
    S_1; (* *Do something if n is even* *)
  else
    S_2; (* *Do something else if n is odd* *)
  end;
  S_3; (* *Modify n* *)
end;
$\{J \land vf < V\}$

Exercise 7.8: Body of the Loop (2/3)

if n **mod** $2 = 0$ **then**

$\{n \textbf{ mod } 2 = 0 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n+1)\}$

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

else

Exercise 7.8: Body of the Loop (2/3)

if n **mod** $2 = 0$ **then**

$\{n \textbf{ mod } 2 = 0 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n+1)\}$

(* $(n \textbf{ mod } 2 = 0) \Rightarrow n = 2(n \textbf{ div } 2) + n \textbf{ mod } 2 = 2(n \textbf{ div } 2)$ *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

else

Exercise 7.8: Body of the Loop (2/3)

if n **mod** $2 = 0$ **then**

$\{n \textbf{ mod } 2 = 0 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n+1)\}$

(* $(n \textbf{ mod } 2 = 0) \Rightarrow n = 2(n \textbf{ div } 2) + n \textbf{ mod } 2 = 2(n \textbf{ div } 2)$ *)

$\{n \textbf{ mod } 2 = 0 \wedge 0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2)) + x \cdot f(2(n \textbf{ div } 2) + 1)\}$

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

else

Exercise 7.8: Body of the Loop (2/3)

if n **mod** $2 = 0$ **then**

$\{n \textbf{ mod } 2 = 0 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n+1)\}$

(* $(n \textbf{ mod } 2 = 0) \Rightarrow n = 2(n \textbf{ div } 2) + n \textbf{ mod } 2 = 2(n \textbf{ div } 2)$ *)

$\{n \textbf{ mod } 2 = 0 \wedge 0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2)) + x \cdot f(2(n \textbf{ div } 2) + 1)\}$

(* *logic; definition* $f(n)$; $n > 0 \wedge (n \textbf{ mod } 2 = 0) \Rightarrow n \geq 2$ *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

else

Exercise 7.8: Body of the Loop (2/3)

if n **mod** $2 = 0$ **then**

$\{n \textbf{ mod } 2 = 0 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n+1)\}$

(* $(n \textbf{ mod } 2 = 0) \Rightarrow n = 2(n \textbf{ div } 2) + n \textbf{ mod } 2 = 2(n \textbf{ div } 2)$ *)

$\{n \textbf{ mod } 2 = 0 \wedge 0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2)) + x \cdot f(2(n \textbf{ div } 2) + 1)\}$

(* *logic; definition* $f(n)$; $n > 0 \wedge (n \textbf{ mod } 2 = 0) \Rightarrow n \geq 2$ *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot (f(n \textbf{ div } 2) + f(n \textbf{ div } 2 + 1))\}$

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

else

Exercise 7.8: Body of the Loop (2/3)

if n **mod** $2 = 0$ **then**

$\{n \textbf{ mod } 2 = 0 \land 0 < n = V \land Z = y \cdot f(n) + x \cdot f(n+1)\}$

(* $(n \textbf{ mod } 2 = 0) \Rightarrow n = 2(n \textbf{ div } 2) + n \textbf{ mod } 2 = 2(n \textbf{ div } 2)$ *)

$\{n \textbf{ mod } 2 = 0 \land 0 < n = V \land Z = y \cdot f(2(n \textbf{ div } 2)) + x \cdot f(2(n \textbf{ div } 2) + 1)\}$

(* *logic; definition* $f(n)$; $n > 0 \land (n \textbf{ mod } 2 = 0) \Rightarrow n \geq 2$ *)

$\{0 < n = V \land Z = y \cdot f(n \textbf{ div } 2) + x \cdot (f(n \textbf{ div } 2) + f(n \textbf{ div } 2 + 1))\}$

(* *calculus (common factor* $f(n \textbf{ div } 2)$*)* *)

$\{0 < n = V \land Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

else

Exercise 7.8: Body of the Loop (2/3)

if n **mod** $2 = 0$ **then**

$\{n \textbf{ mod } 2 = 0 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n+1)\}$

(* $(n \textbf{ mod } 2 = 0) \Rightarrow n = 2(n \textbf{ div } 2) + n \textbf{ mod } 2 = 2(n \textbf{ div } 2)$ *)

$\{n \textbf{ mod } 2 = 0 \wedge 0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2)) + x \cdot f(2(n \textbf{ div } 2) + 1)\}$

(* *logic; definition* $f(n)$; $n > 0 \wedge (n \textbf{ mod } 2 = 0) \Rightarrow n \geq 2$ *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot (f(n \textbf{ div } 2) + f(n \textbf{ div } 2 + 1))\}$

(* *calculus (common factor* $f(n \textbf{ div } 2)$*)* *)

$\{0 < n = V \wedge Z = (x + y) \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

else

Exercise 7.8: Body of the Loop (2/3)

if n **mod** $2 = 0$ **then**

$\{n \textbf{ mod } 2 = 0 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n+1)\}$

(* $(n \textbf{ mod } 2 = 0) \Rightarrow n = 2(n \textbf{ div } 2) + n \textbf{ mod } 2 = 2(n \textbf{ div } 2)$ *)

$\{n \textbf{ mod } 2 = 0 \wedge 0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2)) + x \cdot f(2(n \textbf{ div } 2) + 1)\}$

(* *logic; definition* $f(n)$; $n > 0 \wedge (n \textbf{ mod } 2 = 0) \Rightarrow n \geq 2$ *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot (f(n \textbf{ div } 2) + f(n \textbf{ div } 2 + 1))\}$

(* *calculus (common factor* $f(n \textbf{ div } 2)$*)* *)

$\{0 < n = V \wedge Z = (x + y) \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

$y := x + y;$

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

else

Exercise 7.8: Body of the Loop (3/3)

if n **mod** $2 = 0$ **then**

$y := x + y$; (* *see previous slide* *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

else

$\{n \textbf{ mod } 2 = 1 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n + 1)\}$

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

end;

Exercise 7.8: Body of the Loop (3/3)

if n **mod** $2 = 0$ **then**

$y := x + y$; (* *see previous slide* *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

else

$\{n \textbf{ mod } 2 = 1 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n + 1)\}$

(* *logic; similarly as before:* $n = 2(n \textbf{ div } 2) + 1$ *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

end;

Exercise 7.8: Body of the Loop (3/3)

if n **mod** $2 = 0$ **then**
$y := x + y$; (* *see previous slide* *)
$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$
else
$\{n \textbf{ mod } 2 = 1 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n + 1)\}$
(* *logic; similarly as before:* $n = 2(n \textbf{ div } 2) + 1$ *)
$\{0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2) + 2)\}$

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$
end;

Exercise 7.8: Body of the Loop (3/3)

if n **mod** $2 = 0$ **then**

$y := x + y$; (* *see previous slide* *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

else

$\{n \textbf{ mod } 2 = 1 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n + 1)\}$

(* *logic; similarly as before:* $n = 2(n \textbf{ div } 2) + 1$ *)

$\{0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2) + 2)\}$

(* *calculus* *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

end;

Exercise 7.8: Body of the Loop (3/3)

if n **mod** $2 = 0$ **then**

$y := x + y$; (* *see previous slide* *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

else

$\{n \textbf{ mod } 2 = 1 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n + 1)\}$

(* *logic; similarly as before:* $n = 2(n \textbf{ div } 2) + 1$ *)

$\{0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2) + 2)\}$

(* *calculus* *)

$\{0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2 + 1))\}$

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

end;

Exercise 7.8: Body of the Loop (3/3)

if n **mod** $2 = 0$ **then**

$y := x + y$; (* *see previous slide* *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

else

$\{n \textbf{ mod } 2 = 1 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n + 1)\}$

(* *logic; similarly as before:* $n = 2(n \textbf{ div } 2) + 1$ *)

$\{0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2) + 2)\}$

(* *calculus* *)

$\{0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2 + 1))\}$

(* *definition* $f(n)$ *expanded twice* *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

end;

Exercise 7.8: Body of the Loop (3/3)

if n **mod** $2 = 0$ **then**

$y := x + y$; (* *see previous slide* *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

else

$\{n \textbf{ mod } 2 = 1 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n + 1)\}$

(* *logic; similarly as before:* $n = 2(n \textbf{ div } 2) + 1$ *)

$\{0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2) + 2)\}$

(* *calculus* *)

$\{0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2 + 1))\}$

(* *definition* $f(n)$ *expanded twice* *)

$\{0 < n = V \wedge Z = y \cdot (f(n \textbf{ div } 2) + f(n \textbf{ div } 2 + 1)) + x \cdot f(n \textbf{ div } 2 + 1)\}$

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

end;

Exercise 7.8: Body of the Loop (3/3)

if n **mod** $2 = 0$ **then**

$y := x + y$; (* *see previous slide* *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

else

$\{n \textbf{ mod } 2 = 1 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n + 1)\}$

(* *logic; similarly as before:* $n = 2(n \textbf{ div } 2) + 1$ *)

$\{0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2) + 2)\}$

(* *calculus* *)

$\{0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2 + 1))\}$

(* *definition* $f(n)$ *expanded twice* *)

$\{0 < n = V \wedge Z = y \cdot (f(n \textbf{ div } 2) + f(n \textbf{ div } 2 + 1)) + x \cdot f(n \textbf{ div } 2 + 1)\}$

(* *calculus (common factor* $f(n \textbf{ div } 2 + 1)$ *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

end;

Exercise 7.8: Body of the Loop (3/3)

if n **mod** $2 = 0$ **then**
$y := x + y$; (* *see previous slide* *)
$\{0 < n = V \wedge Z = y \cdot f(n \text{ div } 2) + x \cdot f(n \text{ div } 2 + 1)\}$
else
$\{n \text{ mod } 2 = 1 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n + 1)\}$
(* *logic; similarly as before:* $n = 2(n \text{ div } 2) + 1$ *)
$\{0 < n = V \wedge Z = y \cdot f(2(n \text{ div } 2) + 1) + x \cdot f(2(n \text{ div } 2) + 2)\}$
(* *calculus* *)
$\{0 < n = V \wedge Z = y \cdot f(2(n \text{ div } 2) + 1) + x \cdot f(2(n \text{ div } 2 + 1))\}$
(* *definition* $f(n)$ *expanded twice* *)
$\{0 < n = V \wedge Z = y \cdot (f(n \text{ div } 2) + f(n \text{ div } 2 + 1)) + x \cdot f(n \text{ div } 2 + 1)\}$
(* *calculus (common factor* $f(n \text{ div } 2 + 1)$ *)
$\{0 < n = V \wedge Z = y \cdot f(n \text{ div } 2) + (x + y) \cdot f(n \text{ div } 2 + 1)\}$

$\{0 < n = V \wedge Z = y \cdot f(n \text{ div } 2) + x \cdot f(n \text{ div } 2 + 1)\}$
end;

Exercise 7.8: Body of the Loop (3/3)

if n **mod** $2 = 0$ **then**

$y := x + y$; (* *see previous slide* *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

else

$\{n \textbf{ mod } 2 = 1 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n+1)\}$

(* *logic; similarly as before:* $n = 2(n \textbf{ div } 2) + 1$ *)

$\{0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2) + 2)\}$

(* *calculus* *)

$\{0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2 + 1))\}$

(* *definition* $f(n)$ *expanded twice* *)

$\{0 < n = V \wedge Z = y \cdot (f(n \textbf{ div } 2) + f(n \textbf{ div } 2 + 1)) + x \cdot f(n \textbf{ div } 2 + 1)\}$

(* *calculus (common factor* $f(n \textbf{ div } 2 + 1)$ *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + (x + y) \cdot f(n \textbf{ div } 2 + 1)\}$

$x := x + y$;

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

end;

Exercise 7.8: Body of the Loop (3/3)

if n **mod** $2 = 0$ **then**

$y := x + y$; *(* see previous slide *)*

$\{0 < n = V \land Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

else

$\{n \textbf{ mod } 2 = 1 \land 0 < n = V \land Z = y \cdot f(n) + x \cdot f(n + 1)\}$

(logic; similarly as before: $n = 2(n \textbf{ div } 2) + 1$ *)*

$\{0 < n = V \land Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2) + 2)\}$

(calculus *)*

$\{0 < n = V \land Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2 + 1))\}$

(definition $f(n)$ expanded twice *)*

$\{0 < n = V \land Z = y \cdot (f(n \textbf{ div } 2) + f(n \textbf{ div } 2 + 1)) + x \cdot f(n \textbf{ div } 2 + 1)\}$

(calculus (common factor $f(n \textbf{ div } 2 + 1)$ *)*

$\{0 < n = V \land Z = y \cdot f(n \textbf{ div } 2) + (x + y) \cdot f(n \textbf{ div } 2 + 1)\}$

$x := x + y$;

$\{0 < n = V \land Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

end; *(* collect branches *)*

$\{0 < n = V \land Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

Exercise 7.8: Body of the Loop (3/3)

if n **mod** $2 = 0$ **then**

$y := x + y$; (* *see previous slide* *)

$\{0 < n = V \wedge Z = y \cdot f(n \text{ **div** } 2) + x \cdot f(n \text{ **div** } 2 + 1)\}$

else

$\{n \textbf{ mod } 2 = 1 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n + 1)\}$

(* *logic; similarly as before:* $n = 2(n \textbf{ div } 2) + 1$ *)

$\{0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2) + 2)\}$

(* *calculus* *)

$\{0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2 + 1))\}$

(* *definition* $f(n)$ *expanded twice* *)

$\{0 < n = V \wedge Z = y \cdot (f(n \textbf{ div } 2) + f(n \textbf{ div } 2 + 1)) + x \cdot f(n \textbf{ div } 2 + 1)\}$

(* *calculus (common factor* $f(n \textbf{ div } 2 + 1)$ *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + (x + y) \cdot f(n \textbf{ div } 2 + 1)\}$

$x := x + y$;

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

end; (* *collect branches* *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

(* $0 < n = V \Rightarrow 0 \leq n \textbf{ div } 2 < V$ *)

Exercise 7.8: Body of the Loop (3/3)

if n **mod** $2 = 0$ **then**

$y := x + y$; (* *see previous slide* *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

else

$\{n \textbf{ mod } 2 = 1 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n + 1)\}$

(* *logic; similarly as before:* $n = 2(n \textbf{ div } 2) + 1$ *)

$\{0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2) + 2)\}$

(* *calculus* *)

$\{0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2 + 1))\}$

(* *definition* $f(n)$ *expanded twice* *)

$\{0 < n = V \wedge Z = y \cdot (f(n \textbf{ div } 2) + f(n \textbf{ div } 2 + 1)) + x \cdot f(n \textbf{ div } 2 + 1)\}$

(* *calculus (common factor* $f(n \textbf{ div } 2 + 1)$ *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + (x + y) \cdot f(n \textbf{ div } 2 + 1)\}$

$x := x + y$;

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

end; (* *collect branches* *)

$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

(* $0 < n = V \Rightarrow 0 \leq n \textbf{ div } 2 < V$ *)

$\{0 \leq n \textbf{ div } 2 < V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$

Exercise 7.8: Body of the Loop (3/3)

if n **mod** $2 = 0$ **then**

$y := x + y$; (* *see previous slide* *)

$\{0 < n = V \wedge Z = y \cdot f(n\ \mathbf{div}\ 2) + x \cdot f(n\ \mathbf{div}\ 2 + 1)\}$

else

$\{n\ \mathbf{mod}\ 2 = 1 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n + 1)\}$

(* *logic; similarly as before:* $n = 2(n\ \mathbf{div}\ 2) + 1$ *)

$\{0 < n = V \wedge Z = y \cdot f(2(n\ \mathbf{div}\ 2) + 1) + x \cdot f(2(n\ \mathbf{div}\ 2) + 2)\}$

(* *calculus* *)

$\{0 < n = V \wedge Z = y \cdot f(2(n\ \mathbf{div}\ 2) + 1) + x \cdot f(2(n\ \mathbf{div}\ 2 + 1))\}$

(* *definition* $f(n)$ *expanded twice* *)

$\{0 < n = V \wedge Z = y \cdot (f(n\ \mathbf{div}\ 2) + f(n\ \mathbf{div}\ 2 + 1)) + x \cdot f(n\ \mathbf{div}\ 2 + 1)\}$

(* *calculus (common factor* $f(n\ \mathbf{div}\ 2 + 1)$ *)

$\{0 < n = V \wedge Z = y \cdot f(n\ \mathbf{div}\ 2) + (x + y) \cdot f(n\ \mathbf{div}\ 2 + 1)\}$

$x := x + y$;

$\{0 < n = V \wedge Z = y \cdot f(n\ \mathbf{div}\ 2) + x \cdot f(n\ \mathbf{div}\ 2 + 1)\}$

end; (* *collect branches* *)

$\{0 < n = V \wedge Z = y \cdot f(n\ \mathbf{div}\ 2) + x \cdot f(n\ \mathbf{div}\ 2 + 1)\}$

(* $0 < n = V \Rightarrow 0 \leq n\ \mathbf{div}\ 2 < V$ *)

$\{0 \leq n\ \mathbf{div}\ 2 < V \wedge Z = y \cdot f(n\ \mathbf{div}\ 2) + x \cdot f(n\ \mathbf{div}\ 2 + 1)\}$

$n := n\ \mathbf{div}\ 2$;

Exercise 7.8: Body of the Loop (3/3)

if n **mod** $2 = 0$ **then**
  $y := x + y$; (* *see previous slide* *)
    $\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$
 else
    $\{n \textbf{ mod } 2 = 1 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n+1)\}$
    (* *logic; similarly as before:* $n = 2(n \textbf{ div } 2) + 1$ *)
    $\{0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2) + 2)\}$
    (* *calculus* *)
    $\{0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2 + 1))\}$
    (* *definition* $f(n)$ *expanded twice* *)
    $\{0 < n = V \wedge Z = y \cdot (f(n \textbf{ div } 2) + f(n \textbf{ div } 2 + 1)) + x \cdot f(n \textbf{ div } 2 + 1)\}$
    (* *calculus (common factor* $f(n \textbf{ div } 2 + 1)$ *)
    $\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + (x + y) \cdot f(n \textbf{ div } 2 + 1)\}$
  $x := x + y$;
    $\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$
end; (* *collect branches* *)
$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$
 (* $0 < n = V \Rightarrow 0 \leq n \textbf{ div } 2 < V$ *)
$\{0 \leq n \textbf{ div } 2 < V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$
$n := n$ **div** 2;
$\{0 \leq n < V \wedge Z = y \cdot f(n) + x \cdot f(n+1)\}$

Exercise 7.8: Body of the Loop (3/3)

if n **mod** $2 = 0$ **then**
$y := x + y$; (* *see previous slide* *)
$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$
else
$\{n \textbf{ mod } 2 = 1 \wedge 0 < n = V \wedge Z = y \cdot f(n) + x \cdot f(n+1)\}$
(* *logic; similarly as before:* $n = 2(n \textbf{ div } 2) + 1$ *)
$\{0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2) + 2)\}$
(* *calculus* *)
$\{0 < n = V \wedge Z = y \cdot f(2(n \textbf{ div } 2) + 1) + x \cdot f(2(n \textbf{ div } 2 + 1))\}$
(* *definition* $f(n)$ *expanded twice* *)
$\{0 < n = V \wedge Z = y \cdot (f(n \textbf{ div } 2) + f(n \textbf{ div } 2 + 1)) + x \cdot f(n \textbf{ div } 2 + 1)\}$
(* *calculus (common factor* $f(n \textbf{ div } 2 + 1)$ *)
$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + (x + y) \cdot f(n \textbf{ div } 2 + 1)\}$
$x := x + y$;
$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$
end; (* *collect branches* *)
$\{0 < n = V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$
(* $0 < n = V \Rightarrow 0 \leq n \textbf{ div } 2 < V$ *)
$\{0 \leq n \textbf{ div } 2 < V \wedge Z = y \cdot f(n \textbf{ div } 2) + x \cdot f(n \textbf{ div } 2 + 1)\}$
$n := n$ **div** 2;
$\{0 \leq n < V \wedge Z = y \cdot f(n) + x \cdot f(n+1)\}$
$\{J \wedge vf < V\}$

Exercise 7.8: Conclusion

5 The following command solves the problem:

var $n,\ x,\ y:\ \mathbb{Z}$;
  $\{P : n \geq 0 \wedge Z = f(n)\}$
$y := 1$;
$x := 0$;
  $\{J :\ n \geq 0 \wedge Z = y \cdot f(n) + x \cdot f(n+1)\}$
    (* $vf = n$ *)
while $n \neq 0$ **do**
  if n **mod** $2 = 0$ **then**
      $y := x + y$;
  else
      $x := x + y$;
  end;
  $n := n$ **div** 2;
end;
  $\{Q : x = Z\}$

Outline

Exercise 7.1: Powers

Exercise 7.2: Factorial

Exercise 7.8: Dijkstra's FUSC

Summing an array

Example: Summing an array

const $n : \mathbb{N}$, $a :$ **array** $[0..n)$ **of** $\mathbb{Z}$;
var $x : \mathbb{Z}$;
  $\{P : \textbf{true}\}$
S
  $\{Q : x = \Sigma(a[i] \mid i : i \in [0..n))\}$

- To reduce the size of our formulas we write, for $0 \leq k \leq n$:

$$S(k) = \Sigma(a[i] \mid i : i \in [0..k))$$

- This way, we rewrite the postcondition: $Q : x = S(n)$.

Summing an array: Recurrence

We consider a recurrence relation for $S(k) = \Sigma(a[i] \mid i : i \in [0..k))$. In this case:

$$\boxed{\begin{array}{rl} & S(0) = 0 \\ 0 \le k < n \Rightarrow & S(k+1) = a[k] + S(k) \end{array}}$$

Summing an array: Recurrence

We consider a recurrence relation for $S(k) = \Sigma(a[i] \mid i : i \in [0..k))$. In this case:

$$\boxed{\begin{aligned} S(0) &= 0 \\ 0 \le k < n \Rightarrow \quad S(k+1) &= a[k] + S(k) \end{aligned}}$$

Justification:

- It is clear that $S(0) = 0$, since the domain of the sum is empty.
- For $0 \le k < n$, we compute $S(k+1)$:

$$\begin{aligned} & S(k+1) \\ = & \text{ (* \textit{definition} *)} \\ & \Sigma(a[i] \mid i : i \in [0..k+1)) \\ = & \text{ (* \textit{split domain:} } i = k \vee i < k \text{ *)} \\ & a[k] + \Sigma(a[i] \mid i : i \in [0..k)) \\ = & \text{ (* \textit{definition} *)} \\ & a[k] + S(k) \end{aligned}$$

Summing an array: Invariant and Guard

$$P : \textbf{true}$$
$$Q : x = S(n)$$

0 We expect to add values iteratively: we need a **while**-program.

1 Choose an invariant J and guard B such that $J \wedge \neg B \Rightarrow Q$.

We obtain J by using "replacing a constant by a variable":
(1) Replace n in Q by variable k and
(2) Include the domain condition $0 \leq k \leq n$:

$$J : 0 \leq k \leq n \wedge x = S(k)$$
$$B : k \neq n$$

Summing an array: Invariant and Guard

$$P : \textbf{true}$$
$$Q : x = S(n)$$

0 We expect to add values iteratively: we need a **while**-program.

1 Choose an invariant J and guard B such that $J \wedge \neg B \Rightarrow Q$.

We obtain J by using "replacing a constant by a variable":
(1) Replace n in Q by variable k and
(2) Include the domain condition $0 \leq k \leq n$:

$$J : 0 \leq k \leq n \wedge x = S(k)$$
$$B : k \neq n$$

The proof obligation holds:

$$\begin{aligned} J \wedge \neg B \equiv\ & 0 \leq k \leq n \wedge x = S(k) \wedge k = n \\ \Rightarrow\ & \text{(* } \textit{substitute } k = n\textit{; logic} \text{ *)} \\ & Q : x = S(n) \end{aligned}$$

Summing an array: Initialization & Variant

$$P : \textbf{true}$$
$$J : 0 \leq k \leq n \wedge x = S(k)$$
$$B : k \neq n$$

2 Initialization: Find a command T_0 such that $\{P\}\ T_0\ \{J\}$.

Summing an array: Initialization & Variant

$$P : \textbf{true}$$
$$J : 0 \le k \le n \wedge x = S(k)$$
$$B : k \neq n$$

2 Initialization: Find a command T_0 such that $\{P\}\ T_0\ \{J\}$.

Since $S(0) = 0$, it suffices to choose $k := 0;\ x := 0;$

$\{P :\ \textbf{true}\}$
(* $n \in \mathbb{N}$; $S(0) = 0$ *)
$\{0 \le 0 \le n \wedge 0 = S(0)\}$
$k := 0;$
$\{0 \le k \le n \wedge 0 = S(k)\}$
$x := 0;$
$\{J :\ 0 \le k \le n \wedge x = S(k)\}$

Summing an array: Initialization & Variant

$$P : \textbf{true}$$
$$J : 0 \leq k \leq n \wedge x = S(k)$$
$$B : k \neq n$$

2 Initialization: Find a command T_0 such that $\{P\}\ T_0\ \{J\}$.
Since $S(0) = 0$, it suffices to choose $k := 0;\ x := 0;$

$$
\begin{array}{l}
\quad \{P:\ \textbf{true}\} \\
\qquad (^*\ n \in \mathbb{N};\ S(0) = 0\ ^*) \\
\quad \{0 \leq 0 \leq n \wedge 0 = S(0)\} \\
k := 0; \\
\quad \{0 \leq k \leq n \wedge 0 = S(k)\} \\
x := 0; \\
\quad \{J:\ 0 \leq k \leq n \wedge x = S(k)\}
\end{array}
$$

3 Variant function: Choose a $vf \in \mathbb{Z}$ and prove $J \wedge B \Rightarrow vf \geq 0$.
Since initially $k = 0$ and $B : k \neq n$, we must increase k.
We choose $vf = n - k \in \mathbb{Z}$.
Clearly, $J \wedge B \Rightarrow J \Rightarrow k \leq n \equiv vf \geq 0$.

Summing an array: Body of the Loop

4 Body of the loop:

$$\{J \wedge B \wedge vf = V\}$$

Summing an array: Body of the Loop

4 Body of the loop:

$\{J \wedge B \wedge vf = V\}$

(* *definitions* J, B, *and* vf *)

$\{0 \leq k \leq n \wedge x = S(k) \wedge k \neq n \wedge n - k = V\}$

Summing an array: Body of the Loop

4 Body of the loop:

$\{J \wedge B \wedge vf = V\}$

(* *definitions* J, B, *and* vf *)

$\{0 \leq k \leq n \wedge x = S(k) \wedge k \neq n \wedge n - k = V\}$

(* *calculus;* $k < n$*; prepare* $k := k + 1$*; use recurrence* *)

$\{0 \leq k + 1 \leq n \ \wedge \ x + a[k] = S(k + 1) \ \wedge \ n - (k + 1) < V\}$

Summing an array: Body of the Loop

4 Body of the loop:

$\{J \wedge B \wedge vf = V\}$

(* *definitions* J, B, *and* vf *)

$\{0 \leq k \leq n \wedge x = S(k) \wedge k \neq n \wedge n - k = V\}$

(* *calculus;* $k < n$*; prepare* $k := k + 1$*; use recurrence* *)

$\{0 \leq k + 1 \leq n \ \wedge \ x + a[k] = S(k + 1) \ \wedge \ n - (k + 1) < V\}$

$x := x + a[k];$

Summing an array: Body of the Loop

4 Body of the loop:

$\{J \wedge B \wedge vf = V\}$

(* *definitions* J, B, *and* vf *)

$\{0 \leq k \leq n \wedge x = S(k) \wedge k \neq n \wedge n - k = V\}$

(* *calculus;* $k < n$*; prepare* $k := k + 1$*; use recurrence* *)

$\{0 \leq k+1 \leq n \ \wedge \ x + a[k] = S(k+1) \ \wedge \ n - (k+1) < V\}$

$x := x + a[k];$

$\{0 \leq k+1 \leq n \ \wedge \ x = S(k+1) \ \wedge \ n - (k+1) < V\}$

Summing an array: Body of the Loop

4 Body of the loop:

$\{J \wedge B \wedge vf = V\}$

(* *definitions* J, B, *and* vf *)

$\{0 \leq k \leq n \wedge x = S(k) \wedge k \neq n \wedge n - k = V\}$

(* *calculus;* $k < n$*; prepare* $k := k + 1$*; use recurrence* *)

$\{0 \leq k + 1 \leq n \ \wedge \ x + a[k] = S(k + 1) \ \wedge \ n - (k + 1) < V\}$

$x := x + a[k];$

$\{0 \leq k + 1 \leq n \ \wedge \ x = S(k + 1) \ \wedge \ n - (k + 1) < V\}$

$k := k + 1;$

Summing an array: Body of the Loop

4 Body of the loop:

$\{J \wedge B \wedge vf = V\}$

(* *definitions* J, B, *and* vf *)

$\{0 \leq k \leq n \wedge x = S(k) \wedge k \neq n \wedge n - k = V\}$

(* *calculus;* $k < n$*; prepare* $k := k + 1$*; use recurrence* *)

$\{0 \leq k + 1 \leq n \ \wedge \ x + a[k] = S(k + 1) \ \wedge \ n - (k + 1) < V\}$

$x := x + a[k];$

$\{0 \leq k + 1 \leq n \ \wedge \ x = S(k + 1) \ \wedge \ n - (k + 1) < V\}$

$k := k + 1;$

$\{0 \leq k \leq n \wedge x = S(k) \wedge n - k < V\}$

Summing an array: Body of the Loop

4 Body of the loop:

$\{J \wedge B \wedge vf = V\}$

(* *definitions* J, B, *and* vf *)

$\{0 \leq k \leq n \wedge x = S(k) \wedge k \neq n \wedge n - k = V\}$

(* *calculus;* $k < n$; *prepare* $k := k + 1$; *use recurrence* *)

$\{0 \leq k + 1 \leq n \ \wedge \ x + a[k] = S(k + 1) \ \wedge \ n - (k + 1) < V\}$

$x := x + a[k];$

$\{0 \leq k + 1 \leq n \ \wedge \ x = S(k + 1) \ \wedge \ n - (k + 1) < V\}$

$k := k + 1;$

$\{0 \leq k \leq n \wedge x = S(k) \wedge n - k < V\}$

(* *definitions* J, *and* vf *)

$\{J \wedge vf < V\}$

Summing an array: Conclusion

5 We conclude that $\{P\}$ T_0; **while** B **do** S **end** $\{Q\}$ solves the problem:

const $n :\ \mathbb{N},\ a :$ **array** $[0..n)$ **of** $\mathbb{Z}$;
var $x :\ \mathbb{Z}$;
  $\{P :$ **true**$\}$
$k := 0$;
$x := 0$;
  $\{J : 0 \leq k \leq n \wedge x = S(k)\}$
    (* $vf = n - k$ *)
while $k \neq n$ **do**
  $x := x + a[k]$;
  $k := k + 1$;
end;
  $\{Q :\ x = \Sigma(a[i] \mid i : i \in [0..n)\ )\}$

The End

- Exercises 7.1, 7.2, and 7.8.
- Next time:
  Square root (Exercises 7.3 and 7.4)
  Integral division (Exercises 7.5 and 7.6)