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

March 2, 2023

Outline

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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* $(k+1)^3 = y + 3(x+k) + 1$ *)
$\{x = k^2 \ \wedge\ y + 3(x+k) + 1 = (k+1)^3 \ \wedge\ 0 \leq k < n \ \wedge\ n - k = V\}$
$y := y + 3 * (x + k) + 1;$

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

$k := k + 1;$

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

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* $(k+1)^3 = y + 3(x+k) + 1$ *)
$\{x = k^2 \ \wedge\ y + 3(x+k) + 1 = (k+1)^3 \ \wedge\ 0 \le k < n \ \wedge\ n - k = V\}$
$y := y + 3 * (x + k) + 1;$
$\{x = k^2 \ \wedge\ y = (k+1)^3 \ \wedge\ 0 \le k < n \ \wedge\ n - k = V\}$

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

$k := k + 1;$

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

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* $(k+1)^2 = x + 2k + 1$ *)

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

$k := k + 1;$

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

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

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

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

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

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 $x,\ y,\ k :\ \mathbb{Z}$;
  $\{P :\ \textbf{true}\}$
$k := 0$;
$x := 0$;
$y := 0$;
  $\{J : x = k^2 \wedge y = k^3 \wedge 0 \leq k \leq n\}$
    (* $vf = n - k$ *)
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

var $x,\ n:\ \mathbb{Z}$;
$\{P:\ n \geq 0 \land X = n!\}$
T
$\{Q:\ x = X\}$

Recall the heuristic generalization.

Exercise 7.2: Invariant and Guard

$$\boxed{\begin{array}{l} P: \; n \geq 0 \land X = n! \\ Q: x = X \end{array}}$$

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 $J \land \neg B \Rightarrow Q$.

We use the heuristic generalization.

$$\boxed{\begin{array}{l} J: (x \cdot n! = X) \land n \geq 0 \\ B: n \neq 0 \end{array}}$$

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

Exercise 7.2: Initialization and Variant

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

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

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

(* *calculus* *)

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

$x := 1;$

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

3 Variant function: $vf \in \mathbb{Z}$ and $J \land B \Rightarrow vf \geq 0$
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
$J \land B \Rightarrow vf \geq 0$ holds trivially.

Exercise 7.2: Body of the Loop

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

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

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

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

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

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

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

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

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

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

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

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

Exercise 7.2: Body of the Loop

$$
\begin{array}{|l|}
\hline
J : x \cdot n! = X \land n \geq 0 \\
B : n \neq 0 \\
vf = n \\
\hline
\end{array}
$$

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

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

Exercise 7.2: Conclusion

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

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

Outline

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):

$$f(0) = 0$$
$$f(1) = 1$$
$$f(2 \cdot n) = f(n)$$
$$f(2 \cdot n + 1) = f(n) + f(n + 1)$$

For instance:

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

Exercise 7.8: FUSC

Dijkstra's FUSC function (check EWD 570):

$$f(0) = 0$$
$$f(1) = 1$$
$$f(2 \cdot n) = f(n)$$
$$f(2 \cdot n + 1) = f(n) + f(n + 1)$$

For instance:

$$f(2) = f(2 \cdot 1) = f(1) = 1$$
$$f(3) = f(2 \cdot 1 + 1) = f(1) + f(1 + 1) = 1 + 1 = 2$$

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

$$\boxed{\begin{array}{l} P : n \geq 0 \wedge Z = f(n) \\ Q : Z = x \end{array}}$$

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:

$$\boxed{\begin{array}{l} J : n \geq 0 \wedge (Z = y \cdot f(n) + x \cdot f(n+1)) \\ B : n \neq 0 \end{array}}$$

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

$$\begin{aligned} f(0) &= 0 & P &: n \geq 0 \wedge Z = f(n) \\ f(1) &= 1 & Q &: Z = x \\ f(2 \cdot n) &= f(n) & J &: n \geq 0 \wedge Z = y \cdot f(n) + x \cdot f(n+1) \\ f(2 \cdot n + 1) &= f(n) + f(n+1) & B &: n \neq 0 \end{aligned}$$

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:

$\{J:\ n \geq 0 \wedge Z = y \cdot f(n) + x \cdot f(n+1)\ \wedge\ B:\ n \neq 0\ \wedge\ n = V\}$
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;
$\{J \wedge vf < V\}$

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**

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

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

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

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

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

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

else

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

if $n \textbf{ mod } 2 = 0$ **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* *)

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

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

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

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

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

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

$x := x + y$;

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

end;

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

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

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

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

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* *)

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

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* *)

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

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

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 *)*

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

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 *)*

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

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

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

$n := n$ **div** 2;

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

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:

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

Summing an array: Recurrence

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

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

Justification:

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

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

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:

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

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

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

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

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

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

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

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

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:

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

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;
  $\{Q:\ x = \Sigma(a[i] \mid i : i \in [0..n)\ )\}$

Outline

Exercise 7.3

const $x : \mathbb{N}$;
var $y : \mathbb{Z}$;
$\{P : \textbf{true}\}$
T
$\{Q : y \geq 0 \wedge y^2 \leq x < (y+1)^2\}$

0 We assume that there is no function ‘**sqrt**’ available, and 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 split conjuncts.

$$\boxed{\begin{array}{c} J : y \geq 0 \wedge y^2 \leq x \\ B : (y+1)^2 \leq x \end{array}}$$

Clearly, $J \wedge \neg B \equiv Q$.

Exercise 7.3: Initialization and Variant

2 Initialization: Find a command T_0 such that

$$\{P: \ \textbf{true}\}\ T_0\ \{J: \ y \geq 0 \wedge y^2 \leq x\}$$

We have:

$$
\begin{array}{l}
\quad \{P: \textbf{true}\} \\
\quad\quad (^*\ x \in \mathbb{N}\ ^*) \\
\quad \{0 \geq 0 \wedge 0^2 \leq x\} \\
y := 0; \\
\quad \{J: \ y \geq 0 \wedge y^2 \leq x\}
\end{array}
$$

3 Variant function: $vf = x - y^2 \in \mathbb{Z}$
J contains the conjunct $y^2 \leq x$, so trivially $J \wedge B \Rightarrow vf \geq 0$.

Exercise 7.3: Body of the Loop

$$J : y \geq 0 \wedge y^2 \leq x$$
$$B : (y+1)^2 \leq x$$
$$vf = x - y^2$$

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 7.3: Body of the Loop

$$J : y \geq 0 \wedge y^2 \leq x$$
$$B : (y+1)^2 \leq x$$
$$vf = x - y^2$$

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

$\{J \wedge B \wedge vf = V\}$
$\{y \geq 0 \ \wedge \ y^2 \leq x \ \wedge \ (y+1)^2 \leq x \ \wedge \ x - y^2 = V\}$

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

Exercise 7.3: Body of the Loop

$$J : y \geq 0 \wedge y^2 \leq x$$
$$B : (y+1)^2 \leq x$$
$$vf = x - y^2$$

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

$\{J \wedge B \wedge vf = V\}$
$\{y \geq 0 \ \wedge\ y^2 \leq x \ \wedge\ (y+1)^2 \leq x \ \wedge\ x - y^2 = V\}$
(* *logic; prepare* $y := y + 1$ *)

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

Exercise 7.3: Body of the Loop

$$J : y \geq 0 \wedge y^2 \leq x$$
$$B : (y+1)^2 \leq x$$
$$vf = x - y^2$$

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

$\{J \wedge B \wedge vf = V\}$
$\{y \geq 0 \ \wedge\ y^2 \leq x \ \wedge\ (y+1)^2 \leq x \ \wedge\ x - y^2 = V\}$
(* *logic; prepare* $y := y + 1$ *)
$\{y + 1 \geq 0 \ \wedge\ (y+1)^2 \leq x \ \wedge\ x - (y+1)^2 < V\}$

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

Exercise 7.3: Body of the Loop

$$J : y \geq 0 \wedge y^2 \leq x$$
$$B : (y+1)^2 \leq x$$
$$vf = x - y^2$$

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

$\{J \wedge B \wedge vf = V\}$
$\{y \geq 0 \ \wedge \ y^2 \leq x \ \wedge \ (y+1)^2 \leq x \ \wedge \ x - y^2 = V\}$
(* logic; prepare $y := y + 1$ *)
$\{y + 1 \geq 0 \ \wedge \ (y+1)^2 \leq x \ \wedge \ x - (y+1)^2 < V\}$
$y := y + 1;$

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

Exercise 7.3: Body of the Loop

$$J : y \geq 0 \wedge y^2 \leq x$$
$$B : (y+1)^2 \leq x$$
$$vf = x - y^2$$

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

$\{J \wedge B \wedge vf = V\}$
$\{y \geq 0 \ \wedge\ y^2 \leq x \ \wedge\ (y+1)^2 \leq x \ \wedge\ x - y^2 = V\}$
(* *logic; prepare* $y := y + 1$ *)
$\{y + 1 \geq 0 \ \wedge\ (y+1)^2 \leq x \ \wedge\ x - (y+1)^2 < V\}$
$y := y + 1;$
$\{y \geq 0 \wedge y^2 \leq x \wedge x - y^2 < V\}$
$\{J \wedge vf < V\}$

Exercise 7.3: Conclusion

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

const $x :\ \mathbb{N}$;
var $y :\ \mathbb{Z}$;
$y := 0$;
$\{J : y \geq 0 \wedge y^2 \leq x\}$
(* $vf = x - y^2$ *)
while $(y+1) * (y+1) \leq x$ **do**
$y := y + 1$;
end;
$\{Q :\ y \geq 0 \wedge y^2 \leq x < (y+1)^2\}$

Exercise 7.4: Same Spec, New Invariant

const $x : \mathbb{N}$;
var $y : \mathbb{Z}$;
$\{P : \textbf{true}\}$
T
$\{Q : y \geq 0 \wedge y^2 \leq x < (y+1)^2\}$

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

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

Exercise 7.4: Same Spec, New Invariant

const $x : \mathbb{N}$;
var $y : \mathbb{Z}$;
$\{P : \textbf{true}\}$
T
$\{Q : y \geq 0 \wedge y^2 \leq x < (y+1)^2\}$

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

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

$$y \geq 0 \wedge y^2 \leq x$$

This time, we use the heuristic replace expression by variable, with z in place of $y+1$:

Exercise 7.4: Same Spec, New Invariant

const $x : \mathbb{N}$;
var $y : \mathbb{Z}$;
$\{P : \textbf{true}\}$
T
$\{Q : y \geq 0 \wedge y^2 \leq x < (y+1)^2\}$

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

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

$$y \geq 0 \wedge y^2 \leq x$$

This time, we use the heuristic replace expression by variable, with z in place of $y+1$:

$$\boxed{\begin{array}{l} J : 0 \leq y < z \ \wedge \ y^2 \leq x < z^2 \\ B : z \neq y+1 \end{array}}$$

Clearly, $J \wedge \neg B \Rightarrow Q$.

Exercise 7.4: Initialization and Variant

$$P : \textbf{true}$$
$$J : 0 \leq y < z \wedge y^2 \leq x < z^2$$
$$B : z \neq y + 1$$

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

$\{P : \textbf{true}\}$
(* *calculus;* $x \in \mathbb{N}$ *)
$\{0 \leq 0 < x + 1 \wedge 0^2 \leq x < (x+1)^2\}$
$y := 0;$
$z := x + 1;$
$\{J :\ 0 \leq y < z \wedge y^2 \leq x < z^2\}$

3 Variant function:

Exercise 7.4: Initialization and Variant

P : **true**
$J : 0 \leq y < z \wedge y^2 \leq x < z^2$
$B : z \neq y + 1$

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

$\{P : \textbf{true}\}$
(* *calculus;* $x \in \mathbb{N}$ *)
$\{0 \leq 0 < x + 1 \wedge 0^2 \leq x < (x+1)^2\}$
$y := 0;$
$z := x + 1;$
$\{J :\ 0 \leq y < z \wedge y^2 \leq x < z^2\}$

3 Variant function: We choose $vf = z - y \in \mathbb{Z}$
J contains the conjunct $0 \leq y < z$, so $J \wedge B \Rightarrow vf \geq 0$ holds.
The body of the loop will narrow down the interval $[y, z)$.

Exercise 7.4: Body of the Loop

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

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

Exercise 7.4: Body of the Loop

$\{J \wedge B \wedge vf = V\}$
$\{0 \leq y < z \ \wedge \ y^2 \leq x < z^2 \ \wedge \ y+1 \neq z \ \wedge \ z - y = V\}$

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

Exercise 7.4: Body of the Loop

$\{J \wedge B \wedge vf = V\}$
$\{0 \leq y < z \ \wedge \ y^2 \leq x < z^2 \ \wedge \ y + 1 \neq z \ \wedge \ z - y = V\}$
(* *First,* $y + 1 < z$. *Then* $y + 1 < z \equiv y + 2 \leq z \Rightarrow y < (y + z)$ **div** $2 < z$ *)

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

Exercise 7.4: Body of the Loop

$\{J \wedge B \wedge vf = V\}$
$\{0 \leq y < z \;\wedge\; y^2 \leq x < z^2 \;\wedge\; y + 1 \neq z \;\wedge\; z - y = V\}$
(* *First,* $y + 1 < z$. *Then* $y + 1 < z \equiv y + 2 \leq z \Rightarrow y < (y + z)$ **div** $2 < z$ *)
$\{0 \leq y < (y + z)$ **div** $2 < z \;\wedge\; y^2 \leq x < z^2 \wedge z - y = V\}$

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

Exercise 7.4: Body of the Loop

$\{J \wedge B \wedge vf = V\}$
$\{0 \leq y < z \ \wedge \ y^2 \leq x < z^2 \ \wedge \ y+1 \neq z \ \wedge \ z - y = V\}$
(* *First,* $y+1 < z$. *Then* $y+1 < z \equiv y+2 \leq z \Rightarrow y < (y+z)$ **div** $2 < z$ *)
$\{0 \leq y < (y+z)$ **div** $2 < z \ \wedge \ y^2 \leq x < z^2 \wedge z - y = V\}$
$m := (y+z)$ **div** 2;

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

Exercise 7.4: Body of the Loop

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

$\{0 \leq y < z \ \wedge \ y^2 \leq x < z^2 \ \wedge \ y + 1 \neq z \ \wedge \ z - y = V\}$

(* *First,* $y + 1 < z$. *Then* $y + 1 < z \equiv y + 2 \leq z \Rightarrow y < (y + z)$ **div** $2 < z$ *)

$\{0 \leq y < (y + z)$ **div** $2 < z \ \wedge \ y^2 \leq x < z^2 \wedge z - y = V\}$

$m := (y + z)$ **div** 2;

$\{0 \leq y < m < z \ \wedge \ y^2 \leq x < z^2 \ \wedge \ z - y = V\}$

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

Exercise 7.4: Body of the Loop

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

$\{0 \leq y < z \ \wedge \ y^2 \leq x < z^2 \ \wedge \ y + 1 \neq z \ \wedge \ z - y = V\}$

(* *First,* $y + 1 < z$. *Then* $y + 1 < z \equiv y + 2 \leq z \Rightarrow y < (y + z)$ **div** $2 < z$ *)

$\{0 \leq y < (y + z)$ **div** $2 < z \ \wedge \ y^2 \leq x < z^2 \wedge z - y = V\}$

$m := (y + z)$ **div** 2;

$\{0 \leq y < m < z \ \wedge \ y^2 \leq x < z^2 \ \wedge \ z - y = V\}$

if $m * m \leq x$ **then**

else

end

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

Exercise 7.4: Body of the Loop

$\{J \wedge B \wedge vf = V\}$
$\{0 \leq y < z \ \wedge \ y^2 \leq x < z^2 \ \wedge \ y+1 \neq z \ \wedge \ z - y = V\}$
(* *First,* $y+1 < z$. *Then* $y+1 < z \equiv y+2 \leq z \Rightarrow y < (y+z)$ **div** $2 < z$ *)
$\{0 \leq y < (y+z)$ **div** $2 < z \ \wedge \ y^2 \leq x < z^2 \wedge z - y = V\}$
$m := (y+z)$ **div** 2;
$\{0 \leq y < m < z \ \wedge \ y^2 \leq x < z^2 \ \wedge \ z - y = V\}$
if $m * m \leq x$ **then**
$\{m^2 \leq x \ \wedge \ 0 \leq y < m < z \ \wedge \ y^2 \leq x < z^2 \ \wedge \ z - y = V\}$

else
$\{m^2 > x \ \wedge \ 0 \leq y < m < z \ \wedge \ y^2 \leq x < z^2 \ \wedge \ z - y = V\}$

end

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

Exercise 7.4: Body of the Loop

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

$\{0 \leq y < z \;\wedge\; y^2 \leq x < z^2 \;\wedge\; y+1 \neq z \;\wedge\; z - y = V\}$

(* *First,* $y+1 < z$. *Then* $y + 1 < z \equiv y + 2 \leq z \Rightarrow y < (y+z)$ **div** $2 < z$ *)

$\{0 \leq y < (y+z)\ \textbf{div}\ 2 < z \;\wedge\; y^2 \leq x < z^2 \wedge z - y = V\}$

$m := (y+z)$ **div** 2;

$\{0 \leq y < m < z \;\wedge\; y^2 \leq x < z^2 \;\wedge\; z - y = V\}$

if $m * m \leq x$ **then**

$\{m^2 \leq x \;\wedge\; 0 \leq y < m < z \;\wedge\; y^2 \leq x < z^2 \;\wedge\; z - y = V\}$

(* *logic, combine conjuncts 1 and 3; calculus (prepare update to* y*)* *)

else

$\{m^2 > x \;\wedge\; 0 \leq y < m < z \;\wedge\; y^2 \leq x < z^2 \;\wedge\; z - y = V\}$

end

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

Exercise 7.4: Body of the Loop

$\{J \wedge B \wedge vf = V\}$
$\{0 \leq y < z \ \wedge \ y^2 \leq x < z^2 \ \wedge \ y + 1 \neq z \ \wedge \ z - y = V\}$
(* *First,* $y + 1 < z$. *Then* $y + 1 < z \equiv y + 2 \leq z \Rightarrow y < (y + z)$ **div** $2 < z$ *)
$\{0 \leq y < (y + z)$ **div** $2 < z \ \wedge \ y^2 \leq x < z^2 \wedge z - y = V\}$
$m := (y + z)$ **div** 2;
$\{0 \leq y < m < z \ \wedge \ y^2 \leq x < z^2 \ \wedge \ z - y = V\}$
if $m * m \leq x$ **then**
$\{m^2 \leq x \ \wedge \ 0 \leq y < m < z \ \wedge \ y^2 \leq x < z^2 \ \wedge \ z - y = V\}$
(* *logic, combine conjuncts 1 and 3; calculus (prepare update to* y*)* *)
$\{0 \leq m < z \ \wedge \ m^2 \leq x < z^2 \ \wedge \ z - m < V\}$

else
$\{m^2 > x \ \wedge \ 0 \leq y < m < z \ \wedge \ y^2 \leq x < z^2 \ \wedge \ z - y = V\}$

end

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

Exercise 7.4: Body of the Loop

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

$\{0 \leq y < z \ \wedge \ y^2 \leq x < z^2 \ \wedge \ y+1 \neq z \ \wedge \ z - y = V\}$

(* *First,* $y+1 < z$. *Then* $y+1 < z \equiv y+2 \leq z \Rightarrow y < (y+z)$ **div** $2 < z$ *)

$\{0 \leq y < (y+z)$ **div** $2 < z \ \wedge \ y^2 \leq x < z^2 \wedge z - y = V\}$

$m := (y+z)$ **div** 2;

$\{0 \leq y < m < z \ \wedge \ y^2 \leq x < z^2 \ \wedge \ z - y = V\}$

if $m * m \leq x$ **then**

$\{m^2 \leq x \ \wedge \ 0 \leq y < m < z \ \wedge \ y^2 \leq x < z^2 \ \wedge \ z - y = V\}$

(* *logic, combine conjuncts 1 and 3; calculus (prepare update to* y*)* *)

$\{0 \leq m < z \ \wedge \ m^2 \leq x < z^2 \ \wedge \ z - m < V\}$

$y := m$;

else

$\{m^2 > x \ \wedge \ 0 \leq y < m < z \ \wedge \ y^2 \leq x < z^2 \ \wedge \ z - y = V\}$

end

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

Exercise 7.4: Body of the Loop

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

$\{0 \leq y < z \ \wedge\ y^2 \leq x < z^2 \ \wedge\ y+1 \neq z \ \wedge\ z - y = V\}$

(* *First,* $y+1 < z$*. Then* $y+1 < z \equiv y+2 \leq z \Rightarrow y < (y+z)$ **div** $2 < z$ *)

$\{0 \leq y < (y+z)\ \mathbf{div}\ 2 < z \ \wedge\ y^2 \leq x < z^2 \wedge z - y = V\}$

$m := (y+z)$ **div** 2;

$\{0 \leq y < m < z \ \wedge\ y^2 \leq x < z^2 \ \wedge\ z - y = V\}$

if $m * m \leq x$ **then**

$\{m^2 \leq x \ \wedge\ 0 \leq y < m < z \ \wedge\ y^2 \leq x < z^2 \ \wedge\ z - y = V\}$

(* *logic, combine conjuncts 1 and 3; calculus (prepare update to* y*)* *)

$\{0 \leq m < z \ \wedge\ m^2 \leq x < z^2 \ \wedge\ z - m < V\}$

$y := m$;

$\{0 \leq y < z \ \wedge\ y^2 \leq x < z^2 \ \wedge\ z - y < V\}$

else

$\{m^2 > x \ \wedge\ 0 \leq y < m < z \ \wedge\ y^2 \leq x < z^2 \ \wedge\ z - y = V\}$

end

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

Exercise 7.4: Body of the Loop

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

$\{0 \le y < z \;\wedge\; y^2 \le x < z^2 \;\wedge\; y+1 \ne z \;\wedge\; z - y = V\}$

(* *First,* $y+1 < z$*. Then* $y+1 < z \equiv y+2 \le z \Rightarrow y < (y+z)$ **div** $2 < z$ *)

$\{0 \le y < (y+z)$ **div** $2 < z \;\wedge\; y^2 \le x < z^2 \wedge z - y = V\}$

$m := (y+z)$ **div** 2;

$\{0 \le y < m < z \;\wedge\; y^2 \le x < z^2 \;\wedge\; z - y = V\}$

if $m * m \le x$ **then**

$\{m^2 \le x \;\wedge\; 0 \le y < m < z \;\wedge\; y^2 \le x < z^2 \;\wedge\; z - y = V\}$

(* *logic, combine conjuncts 1 and 3; calculus (prepare update to* y*)* *)

$\{0 \le m < z \;\wedge\; m^2 \le x < z^2 \;\wedge\; z - m < V\}$

$y := m$;

$\{0 \le y < z \;\wedge\; y^2 \le x < z^2 \;\wedge\; z - y < V\}$

else

$\{m^2 > x \;\wedge\; 0 \le y < m < z \;\wedge\; y^2 \le x < z^2 \;\wedge\; z - y = V\}$

(* *logic, combine conjuncts 1 and 3; calculus (prepare update to* z*)* *)

end

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

Exercise 7.4: Body of the Loop

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

$\{0 \leq y < z \;\wedge\; y^2 \leq x < z^2 \;\wedge\; y+1 \neq z \;\wedge\; z - y = V\}$

(* *First,* $y+1 < z$. *Then* $y+1 < z \equiv y+2 \leq z \Rightarrow y < (y+z)$ **div** $2 < z$ *)

$\{0 \leq y < (y+z)\ \mathbf{div}\ 2 < z \;\wedge\; y^2 \leq x < z^2 \wedge z - y = V\}$

$m := (y+z)$ **div** 2;

$\{0 \leq y < m < z \;\wedge\; y^2 \leq x < z^2 \;\wedge\; z - y = V\}$

if $m * m \leq x$ **then**

$\{m^2 \leq x \;\wedge\; 0 \leq y < m < z \;\wedge\; y^2 \leq x < z^2 \;\wedge\; z - y = V\}$

(* *logic, combine conjuncts 1 and 3; calculus (prepare update to* y*)* *)

$\{0 \leq m < z \;\wedge\; m^2 \leq x < z^2 \;\wedge\; z - m < V\}$

$y := m$;

$\{0 \leq y < z \;\wedge\; y^2 \leq x < z^2 \;\wedge\; z - y < V\}$

else

$\{m^2 > x \;\wedge\; 0 \leq y < m < z \;\wedge\; y^2 \leq x < z^2 \;\wedge\; z - y = V\}$

(* *logic, combine conjuncts 1 and 3; calculus (prepare update to* z*)* *)

$\{0 \leq y < m \wedge y^2 \leq x < m^2 \wedge m - y < V\}$

end

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

Exercise 7.4: Body of the Loop

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

$\{0 \leq y < z \;\wedge\; y^2 \leq x < z^2 \;\wedge\; y+1 \neq z \;\wedge\; z - y = V\}$

(* *First,* $y+1 < z$*. Then* $y+1 < z \equiv y+2 \leq z \Rightarrow y < (y+z)$ **div** $2 < z$ *)

$\{0 \leq y < (y+z)\ \textbf{div}\ 2 < z \;\wedge\; y^2 \leq x < z^2 \wedge z - y = V\}$

$m := (y+z)$ **div** 2;

$\{0 \leq y < m < z \;\wedge\; y^2 \leq x < z^2 \;\wedge\; z - y = V\}$

if $m * m \leq x$ **then**

$\{m^2 \leq x \;\wedge\; 0 \leq y < m < z \;\wedge\; y^2 \leq x < z^2 \;\wedge\; z - y = V\}$

(* *logic, combine conjuncts 1 and 3; calculus (prepare update to* y*)* *)

$\{0 \leq m < z \;\wedge\; m^2 \leq x < z^2 \;\wedge\; z - m < V\}$

$y := m$;

$\{0 \leq y < z \;\wedge\; y^2 \leq x < z^2 \;\wedge\; z - y < V\}$

else

$\{m^2 > x \;\wedge\; 0 \leq y < m < z \;\wedge\; y^2 \leq x < z^2 \;\wedge\; z - y = V\}$

(* *logic, combine conjuncts 1 and 3; calculus (prepare update to* z*)* *)

$\{0 \leq y < m \wedge y^2 \leq x < m^2 \wedge m - y < V\}$

$z := m$;

end

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

Exercise 7.4: Body of the Loop

$\{J \wedge B \wedge vf = V\}$
$\{0 \leq y < z \;\wedge\; y^2 \leq x < z^2 \;\wedge\; y+1 \neq z \;\wedge\; z - y = V\}$
(* *First,* $y+1<z$. *Then* $y+1<z \equiv y+2 \leq z \Rightarrow y < (y+z)$ **div** $2 < z$ *)
$\{0 \leq y < (y+z)$ **div** $2 < z \;\wedge\; y^2 \leq x < z^2 \wedge z - y = V\}$
$m := (y+z)$ **div** 2;
$\{0 \leq y < m < z \;\wedge\; y^2 \leq x < z^2 \;\wedge\; z - y = V\}$
if $m * m \leq x$ **then**
$\{m^2 \leq x \;\wedge\; 0 \leq y < m < z \;\wedge\; y^2 \leq x < z^2 \;\wedge\; z - y = V\}$
(* *logic, combine conjuncts 1 and 3; calculus (prepare update to* y*)* *)
$\{0 \leq m < z \;\wedge\; m^2 \leq x < z^2 \;\wedge\; z - m < V\}$
$y := m$;
$\{0 \leq y < z \;\wedge\; y^2 \leq x < z^2 \;\wedge\; z - y < V\}$
else
$\{m^2 > x \;\wedge\; 0 \leq y < m < z \;\wedge\; y^2 \leq x < z^2 \;\wedge\; z - y = V\}$
(* *logic, combine conjuncts 1 and 3; calculus (prepare update to* z*)* *)
$\{0 \leq y < m \wedge y^2 \leq x < m^2 \wedge m - y < V\}$
$z := m$;
$\{0 \leq y < z \wedge y^2 \leq x < z^2 \wedge z - y < V\}$
end

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

Exercise 7.4: Body of the Loop

$\{J \wedge B \wedge vf = V\}$
$\{0 \le y < z \;\wedge\; y^2 \le x < z^2 \;\wedge\; y+1 \ne z \;\wedge\; z - y = V\}$
(* *First,* $y+1 < z$. *Then* $y+1 < z \equiv y+2 \le z \Rightarrow y < (y+z)$ **div** $2 < z$ *)
$\{0 \le y < (y+z)$ **div** $2 < z \;\wedge\; y^2 \le x < z^2 \wedge z - y = V\}$
$m := (y+z)$ **div** 2;
$\{0 \le y < m < z \;\wedge\; y^2 \le x < z^2 \;\wedge\; z - y = V\}$
if $m * m \le x$ **then**
$\{m^2 \le x \;\wedge\; 0 \le y < m < z \;\wedge\; y^2 \le x < z^2 \;\wedge\; z - y = V\}$
(* *logic, combine conjuncts 1 and 3; calculus (prepare update to* y*)* *)
$\{0 \le m < z \;\wedge\; m^2 \le x < z^2 \;\wedge\; z - m < V\}$
$y := m$;
$\{0 \le y < z \;\wedge\; y^2 \le x < z^2 \;\wedge\; z - y < V\}$
else
$\{m^2 > x \;\wedge\; 0 \le y < m < z \;\wedge\; y^2 \le x < z^2 \;\wedge\; z - y = V\}$
(* *logic, combine conjuncts 1 and 3; calculus (prepare update to* z*)* *)
$\{0 \le y < m \wedge y^2 \le x < m^2 \wedge m - y < V\}$
$z := m$;
$\{0 \le y < z \wedge y^2 \le x < z^2 \wedge z - y < V\}$
end (* *collect branches* *)
$\{0 \le y < z \wedge y^2 \le x < z^2 \wedge z - y < V\}$
$\{J \wedge vf < V\}$

Exercise 7.4: Conclusion

5 Conclude that $\{P\}$ T_0; **while** B **do** S **end** $\{Q\}$ solves the problem.

$\{P:$ **true**$\}$
$y := 0;$
$z := x + 1;$
$\{J : 0 \leq y < z \wedge y^2 \leq x < z^2\}$
$(^*\ vf = z - y\ ^*)$
while $y + 1 \neq z$ **do**
  $m := (y + z)$ **div** $2;$
  if $m * m \leq x$ **then**
    $y := m;$
  else
    $z := m;$
  end;
end;
$\{Q:\ y \geq 0 \wedge y^2 \leq x < (y + 1)^2\}$

Comparison between 7.3 and 7.4

Exercise 7.3:

$y := 0;$
while $(y+1)*(y+1) \leq x$ **do**
  $y := y + 1;$
end;

Exercise 7.4:

$y := 0;$
$z := x + 1;$
while $y + 1 \neq z$ **do**
  $m := (y + z)$ **div** $2;$
  if $m * m \leq x$ **then**
    $y := m;$
  else
    $z := m;$
  end;
end;

Comparison between 7.3 and 7.4

Exercise 7.3:

$y := 0;$
while $(y+1)*(y+1) \leq x$ **do**
  $y := y + 1;$
end;

Exercise 7.4:

$y := 0;$
$z := x + 1;$
while $y + 1 \neq z$ **do**
  $m := (y + z)$ **div** $2;$
  if $m * m \leq x$ **then**
    $y := m;$
  else
    $z := m;$
  end;
end;

Take $x = 1000$. Compare the number of iterations:

7.3 31 times.

Comparison between 7.3 and 7.4

Exercise 7.3:

$y := 0;$
while $(y+1)*(y+1) \leq x$ **do**
  $y := y+1;$
end;

Exercise 7.4:

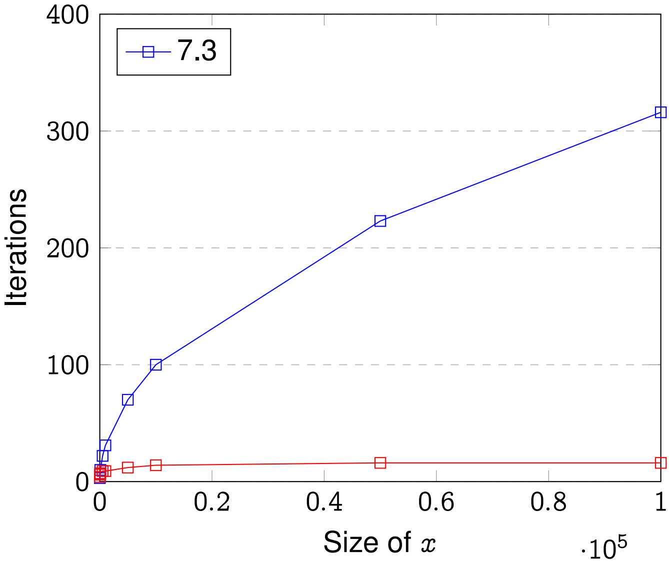
$y := 0;$
$z := x+1;$
while $y+1 \neq z$ **do**
  $m := (y+z)$ **div** $2;$
  if $m*m \leq x$ **then**
    $y := m;$
  else
    $z := m;$
  end;
end;

Take $x = 1000$. Compare the number of iterations:

7.3 31 times.

7.4 9 times - the size of $[y, z)$ decreases in each iteration:
$[0, 1001) \to [0, 500) \to [0, 250) \to [0, 125) \to [0, 62) \to [31, 62)$
$\to [31, 46) \to [31, 38) \to [31, 34) \to [31, 32)$.

Comparison between 7.3 and 7.4



Outline

Exercise 7.5: Invariant

const $y : \mathbb{N}^+$;
var $x,\ q : \mathbb{Z}$;

$\{P :\ x = X \wedge X \geq 0\}$

T

$\{Q :\ X = q \cdot y + x\ \wedge\ 0 \leq x < y\}$

This way, e.g., given $X = 11$ and $y = 4$, we obtain $q = 2$ and $x = 3$.

Exercise 7.5: Invariant

const $y : \mathbb{N}^+$;
var $x, \; q : \mathbb{Z}$;

$\{P : \; x = X \wedge X \geq 0\}$
T
$\{Q : \; X = q \cdot y + x \; \wedge \; 0 \leq x < y\}$

This way, e.g., given $X = 11$ and $y = 4$, we obtain $q = 2$ and $x = 3$.

0 We need a **while**-program: we cannot use **div**, **mod**, and multiplication, so we repeatedly use addition and subtraction.

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

We use the heuristic split conjuncts:

$$\boxed{\begin{array}{l} J : X = q \cdot y + x \; \wedge \; 0 \leq x \\ B : y \leq x \end{array}}$$

Clearly, $J \wedge \neg B \equiv Q$.

Exercise 7.5: Initialization and Variant

$$P : x = X \wedge X \geq 0$$
$$Q : X = q \cdot y + x \wedge 0 \leq x < y$$
$$J : X = q \cdot y + x \wedge 0 \leq x$$
$$B : y \leq x$$

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

$\{P : x = X \wedge X \geq 0\}$

(* *logic; calculus* *)

$\{X = 0 \cdot y + x \wedge 0 \leq x\}$

$q := 0;$

$\{J : \ X = q \cdot y + x \wedge 0 \leq x\}$

3 Variant function:

Exercise 7.5: Initialization and Variant

$$
\begin{aligned}
P &: x = X \wedge X \geq 0 \\
Q &: X = q \cdot y + x \wedge 0 \leq x < y \\
J &: X = q \cdot y + x \wedge 0 \leq x \\
B &: y \leq x
\end{aligned}
$$

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

$\{P : x = X \wedge X \geq 0\}$

(* *logic; calculus* *)

$\{X = 0 \cdot y + x \wedge 0 \leq x\}$

$q := 0;$

$\{J : \; X = q \cdot y + x \wedge 0 \leq x\}$

3 Variant function:
We need to decrease x until $x < y$, so we choose $vf = x \in \mathbb{Z}$.
Since J contains $0 \leq x$, it is trivial that $J \wedge B \Rightarrow vf \geq 0$.

Exercise 7.5: Body of the Loop

4 Body of the loop:

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

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

Exercise 7.5: Body of the Loop

4 Body of the loop:

$$\{J \wedge B \ \wedge \ vf = V\}$$
$$\{X = q \cdot y + x \ \wedge \ 0 \leq x \ \wedge \ y \leq x \ \wedge \ x = V\}$$

$$x := x - y;$$

$$q := q + 1;$$

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

Exercise 7.5: Body of the Loop

4 Body of the loop:

$\{J \wedge B \;\wedge\; vf = V\}$
$\{X = q \cdot y + x \;\wedge\; 0 \leq x \;\wedge\; y \leq x \;\wedge\; x = V\}$
(* $y > 0$; *prepare* $x := x - y$; *calculus; logic* *)

$x := x - y;$

$q := q + 1;$

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

Exercise 7.5: Body of the Loop

4 Body of the loop:

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

$\{X = q \cdot y + x \ \wedge \ 0 \leq x \ \wedge \ y \leq x \ \wedge \ x = V\}$

(* $y > 0$; *prepare* $x := x - y$; *calculus; logic* *)

$\{X = (q+1) \cdot y + x - y \ \wedge \ 0 \leq x - y \ \wedge \ x - y < V\}$

$x := x - y;$

$q := q + 1;$

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

Exercise 7.5: Body of the Loop

4 Body of the loop:

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

$\{X = q \cdot y + x \;\wedge\; 0 \leq x \;\wedge\; y \leq x \;\wedge\; x = V\}$

(* $y > 0$; *prepare* $x := x - y$; *calculus; logic* *)

$\{X = (q + 1) \cdot y + x - y \;\wedge\; 0 \leq x - y \;\wedge\; x - y < V\}$

$x := x - y;$

$q := q + 1;$

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

Exercise 7.5: Body of the Loop

4 Body of the loop:

$$\{J \wedge B \ \wedge \ vf = V\}$$
$$\{X = q \cdot y + x \ \wedge \ 0 \leq x \ \wedge \ y \leq x \ \wedge \ x = V\}$$
(* $y > 0$; *prepare* $x := x - y$; *calculus; logic* *)
$$\{X = (q+1) \cdot y + x - y \ \wedge \ 0 \leq x - y \ \wedge \ x - y < V\}$$
$x := x - y;$
$$\{X = (q+1) \cdot y + x \wedge 0 \leq x \wedge x < V\}$$
$q := q + 1;$

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

Exercise 7.5: Body of the Loop

4 Body of the loop:

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

$\{X = q \cdot y + x \;\wedge\; 0 \leq x \;\wedge\; y \leq x \;\wedge\; x = V\}$

(* $y > 0$; *prepare* $x := x - y$; *calculus; logic* *)

$\{X = (q+1) \cdot y + x - y \;\wedge\; 0 \leq x - y \;\wedge\; x - y < V\}$

$x := x - y;$

$\{X = (q+1) \cdot y + x \wedge 0 \leq x \wedge x < V\}$

$q := q + 1;$

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

Exercise 7.5: Body of the Loop

4 Body of the loop:

$$\{J \wedge B \ \wedge \ vf \ = \ V\}$$
$$\{X \ = q \cdot y + x \ \wedge \ 0 \leq x \ \wedge \ y \leq x \ \wedge \ x = \ V\}$$
(* $y > 0$; *prepare* $x := x - y$; *calculus; logic* *)
$$\{X \ = (q + 1) \cdot y + x - y \ \wedge \ 0 \leq x - y \ \wedge \ x - y < \ V\}$$
$x := x - y;$
$$\{X \ = (q + 1) \cdot y + x \wedge 0 \leq x \wedge x < \ V\}$$
$q := q + 1;$
$$\{X \ = q \cdot y + x \wedge 0 \leq x \wedge x < \ V\}$$
$$\{J \wedge vf \ < \ V\}$$

Exercise 7.5: Conclusion

5 Conclusion: We derived $\{P\}\ T_0;$ **while** B **do** S **end** $\{Q\}$

$$
\begin{array}{l}
\quad \{P:\ x = X \wedge X \geq 0\} \\
q := 0; \\
\quad \{J: X = q \cdot y + x \wedge 0 \leq x\} \\
\qquad (^{*}\ vf = x\ ^{*}) \\
\textbf{while } y \leq x \textbf{ do} \\
\quad x := x - y; \\
\quad q := q + 1; \\
\textbf{end}; \\
\quad \{Q:\ X = q \cdot y + x \wedge 0 \leq x < y\}
\end{array}
$$

Exercise 7.6: Same Spec, New Invariant

const $y : \mathbb{N}^+$;
var $x,\ z,\ q,\ i : \mathbb{Z}$;
$\{P :\ x = X \wedge X \geq 0\}$
T
$\{Q :\ X = q \cdot y + x \wedge 0 \leq x < y\}$

Same exercise as 7.5, now with more hints.

Exercise 7.6: Same Spec, New Invariant

const $y :\ \mathbb{N}^+$;
var $x,\ z,\ q,\ i :\ \mathbb{Z}$;
$\{P :\ x = X \land X \geq 0\}$
T
$\{Q :\ X = q \cdot y + x \land 0 \leq x < y\}$

Same exercise as 7.5, now with more hints.

- We can use multiplication and division by 2.
- Before in each iteration we had '$x := x - y$'. The invariant was

$$X = q \cdot y + x \land 0 \leq x$$

Exercise 7.6: Same Spec, New Invariant

const $y: \mathbb{N}^+$;
var $x, z, q, i: \mathbb{Z}$;
$\{P: x = X \wedge X \geq 0\}$
T
$\{Q: X = q \cdot y + x \wedge 0 \leq x < y\}$

Same exercise as 7.5, now with more hints.

- We can use multiplication and division by 2.
- Before in each iteration we had '$x := x - y$'. The invariant was

$$X = q \cdot y + x \wedge 0 \leq x$$

- Now the invariant involves a new variable z:

$$\boxed{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ z = 2^i \cdot y \ \wedge \ i \geq 0}$$

What is the role of z?

Exercise 7.6: Initialization

$$P : x = X \wedge X \geq 0$$
$$J : X = q \cdot z + x \ \wedge\ 0 \leq x < z \ \wedge\ z = 2^i \cdot y \ \wedge\ i \geq 0$$

1 Choose a guard B such that $J \wedge \neg B \Rightarrow Q$.
We choose $B : z \neq y$.

Exercise 7.6: Initialization

$$P : x = X \wedge X \geq 0$$
$$J : X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ z = 2^i \cdot y \ \wedge \ i \geq 0$$

1 Choose a guard B such that $J \wedge \neg B \Rightarrow Q$.
  We choose $B : z \neq y$.

2 Initialization: We find a command T_0 such that $\{P\}\ T_0\ \{J\}$.
  We can easily initialize the first conjunct of J with $q := 0$.

$\{P : x = X \wedge X \geq 0\}$
T_1
$\{P_0 : x = X \wedge 0 \leq x < z \wedge i \geq 0 \wedge z = 2^i \cdot y\}$
(* *calculus* *)
$\{X = 0 \cdot z + x \wedge 0 \leq x < z \wedge i \geq 0 \wedge z = 2^i \cdot y\}$
$q := 0;$
$\{J : \ X = q \cdot z + x \wedge 0 \leq x < z \wedge i \geq 0 \wedge z = 2^i \cdot y\}$

But deriving T_1 requires more work: an auxiliary loop.

Exercise 7.6: Auxiliary Loop

We derive

$$
\begin{array}{l}
\quad \{P : x = X \wedge X \geq 0\} \\
T_1 \\
\quad \{P_0 : x = X \wedge 0 \leq x < z \wedge i \geq 0 \wedge z = 2^i \cdot y\}
\end{array}
$$

For the invariant and guard we choose:

$$
\boxed{\begin{array}{l}
J_0 : 0 \leq x = X \wedge i \geq 0 \wedge z = 2^i \cdot y \\
B_0 : z \leq x
\end{array}}
$$

Clearly $J_0 \wedge \neg B_0 \equiv P_0$.
J_0 is easy to initialize (without proof): $z := y;\ i := 0;$
We choose the variant function $vf_0 = x - z \in \mathbb{Z}$.
Since $B_0 \equiv vf_0 \geq 0$, it is trivial that $J_0 \wedge B_0 \Rightarrow vf_0 \geq 0$

Exercise 7.6: Body of the Auxiliary Loop

$\{J_0 \wedge B_0 \wedge vf_0 = V\}$

$\{J_0 \wedge vf_0 < V\}$

Exercise 7.6: Body of the Auxiliary Loop

$\{J_0 \wedge B_0 \wedge vf_0 = V\}$
$\{0 \leq x = X \wedge i \geq 0 \wedge z = 2^i \cdot y \wedge z \leq x \wedge x - z = V\}$

$\{J_0 \wedge vf_0 < V\}$

Exercise 7.6: Body of the Auxiliary Loop

$\{J_0 \wedge B_0 \wedge vf_0 = V\}$
$\{0 \leq x = X \wedge i \geq 0 \wedge z = 2^i \cdot y \wedge z \leq x \wedge x - z = V\}$
  (* $y > 0 \Rightarrow z = 2^i \cdot y > 0$; *prepare* $z := 2 * z$ *)
$\{0 \leq x = X \wedge i + 1 \geq 0 \wedge 2 \cdot z = 2^{i+1} \cdot y \wedge x - 2 \cdot z < V\}$

$\{J_0 \wedge vf_0 < V\}$

Exercise 7.6: Body of the Auxiliary Loop

$\{J_0 \wedge B_0 \wedge vf_0 = V\}$
$\{0 \leq x = X \wedge i \geq 0 \wedge z = 2^i \cdot y \wedge z \leq x \wedge x - z = V\}$
(* $y > 0 \Rightarrow z = 2^i \cdot y > 0$; *prepare* $z := 2 * z$ *)
$\{0 \leq x = X \wedge i + 1 \geq 0 \wedge 2 \cdot z = 2^{i+1} \cdot y \wedge x - 2 \cdot z < V\}$
$z := 2 * z;$

$\{J_0 \wedge vf_0 < V\}$

Exercise 7.6: Body of the Auxiliary Loop

$\{J_0 \wedge B_0 \wedge vf_0 = V\}$
$\{0 \leq x = X \wedge i \geq 0 \wedge z = 2^i \cdot y \wedge z \leq x \wedge x - z = V\}$
(* $y > 0 \Rightarrow z = 2^i \cdot y > 0$; *prepare* $z := 2 * z$ *)
$\{0 \leq x = X \wedge i + 1 \geq 0 \wedge 2 \cdot z = 2^{i+1} \cdot y \wedge x - 2 \cdot z < V\}$
$z := 2 * z;$
$\{0 \leq x = X \wedge i + 1 \geq 0 \wedge z = 2^{i+1} \cdot y \wedge x - z < V\}$

$\{J_0 \wedge vf_0 < V\}$

Exercise 7.6: Body of the Auxiliary Loop

$\{J_0 \wedge B_0 \wedge vf_0 = V\}$
$\{0 \leq x = X \wedge i \geq 0 \wedge z = 2^i \cdot y \wedge z \leq x \wedge x - z = V\}$
(* $y > 0 \Rightarrow z = 2^i \cdot y > 0$; *prepare* $z := 2 * z$ *)
$\{0 \leq x = X \wedge i + 1 \geq 0 \wedge 2 \cdot z = 2^{i+1} \cdot y \wedge x - 2 \cdot z < V\}$
$z := 2 * z;$
$\{0 \leq x = X \wedge i + 1 \geq 0 \wedge z = 2^{i+1} \cdot y \wedge x - z < V\}$
$i := i + 1;$

$\{J_0 \wedge vf_0 < V\}$

Exercise 7.6: Body of the Auxiliary Loop

$\{J_0 \wedge B_0 \wedge vf_0 = V\}$
$\{0 \leq x = X \wedge i \geq 0 \wedge z = 2^i \cdot y \wedge z \leq x \wedge x - z = V\}$
(* $y > 0 \Rightarrow z = 2^i \cdot y > 0$; *prepare* $z := 2 * z$ *)
$\{0 \leq x = X \wedge i + 1 \geq 0 \wedge 2 \cdot z = 2^{i+1} \cdot y \wedge x - 2 \cdot z < V\}$
$z := 2 * z;$
$\{0 \leq x = X \wedge i + 1 \geq 0 \wedge z = 2^{i+1} \cdot y \wedge x - z < V\}$
$i := i + 1;$
$\{0 \leq x = X \wedge i \geq 0 \wedge z = 2^i \cdot y \wedge z \leq x \wedge x - z < V\}$
$\{J_0 \wedge vf_0 < V\}$

Exercise 7.6: Summing Up Initialization

We derived the following auxiliary loop for initialization:

$z := y;$
$i := 0;$
while $z \leq x$ **do**
  $z := 2 * z;$
  $i := i + 1;$
end;
$q := 0;$

We may now return to design the main loop.

Exercise 7.6: Variant

Recall:

$$J : X = q \cdot z + x \wedge 0 \leq x < z \wedge i \geq 0 \wedge z = 2^i \cdot y$$
$$B : z \neq y$$

3 Variant function:
We choose $vf = i \in \mathbb{Z}$.
Clearly, $J \wedge B \Rightarrow vf \geq 0$, since $i \geq 0$ is a conjunct of J.

Exercise 7.6: Body of the Main Loop

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

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

Exercise 7.6: Body of the Main Loop

$\{J \land B \ \land \ vf = V\}$
$\{X = q \cdot z + x \ \land \ 0 \leq x < z \ \land \ i \geq 0 \ \land \ z = 2^i \cdot y \ \land \ z \neq y \ \land \ i = V\}$

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

Exercise 7.6: Body of the Main Loop

$\{J \wedge B \ \wedge \ vf = V\}$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ z \neq y \ \wedge \ i = V\}$
(* *prepare* $i := i - 1$; $z \neq y \ \wedge \ z = 2^i \cdot y \ \wedge \ i \geq 0 \Rightarrow i > 0$ *)
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i - 1 \geq 0 \ \wedge \ z = 2 \cdot 2^{i-1} \cdot y \ \wedge \ i - 1 < V\}$

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

Exercise 7.6: Body of the Main Loop

$\{J \wedge B \ \wedge \ vf = V\}$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ z \neq y \ \wedge \ i = V\}$
(* *prepare* $i := i - 1$; $z \neq y \ \wedge \ z = 2^i \cdot y \ \wedge \ i \geq 0 \Rightarrow i > 0$ *)
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i - 1 \geq 0 \ \wedge \ z = 2 \cdot 2^{i-1} \cdot y \ \wedge \ i - 1 < V\}$
$i := i - 1;$

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

Exercise 7.6: Body of the Main Loop

$\{J \wedge B \ \wedge \ vf = V\}$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ z \neq y \ \wedge \ i = V\}$
(* *prepare* $i := i - 1$; $z \neq y \ \wedge \ z = 2^i \cdot y \ \wedge \ i \geq 0 \Rightarrow i > 0$ *)
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i - 1 \geq 0 \ \wedge \ z = 2 \cdot 2^{i-1} \cdot y \ \wedge \ i - 1 < V\}$
$i := i - 1;$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2 \cdot 2^i \cdot y \ \wedge \ i < V\}$

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

Exercise 7.6: Body of the Main Loop

$\{J \wedge B \ \wedge \ vf = V\}$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ z \neq y \ \wedge \ i = V\}$
(* *prepare* $i := i - 1$; $z \neq y \ \wedge \ z = 2^i \cdot y \ \wedge \ i \geq 0 \Rightarrow i > 0$ *)
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i - 1 \geq 0 \ \wedge \ z = 2 \cdot 2^{i-1} \cdot y \ \wedge \ i - 1 < V\}$
$i := i - 1;$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2 \cdot 2^i \cdot y \ \wedge \ i < V\}$
(* z *is even*; $z = 2(z$ **div** $2)$; *calculus* *)

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

Exercise 7.6: Body of the Main Loop

$\{J \wedge B \wedge vf = V\}$
$\{X = q \cdot z + x \wedge 0 \leq x < z \wedge i \geq 0 \wedge z = 2^i \cdot y \wedge z \neq y \wedge i = V\}$
(* *prepare* $i := i - 1$; $z \neq y \wedge z = 2^i \cdot y \wedge i \geq 0 \Rightarrow i > 0$ *)
$\{X = q \cdot z + x \wedge 0 \leq x < z \wedge i - 1 \geq 0 \wedge z = 2 \cdot 2^{i-1} \cdot y \wedge i - 1 < V\}$
$i := i - 1;$
$\{X = q \cdot z + x \wedge 0 \leq x < z \wedge i \geq 0 \wedge z = 2 \cdot 2^i \cdot y \wedge i < V\}$
(* z *is even*; $z = 2(z \textbf{ div } 2)$; *calculus* *)
$\{X = 2 \cdot q \cdot (z \textbf{ div } 2) + x \wedge 0 \leq x < 2(z \textbf{ div } 2) \wedge i \geq 0 \wedge z \textbf{ div } 2 = 2^i \cdot y \wedge i < V\}$

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

Exercise 7.6: Body of the Main Loop

$\{J \wedge B \ \wedge\ vf = V\}$
$\{X = q \cdot z + x \ \wedge\ 0 \leq x < z \ \wedge\ i \geq 0 \ \wedge\ z = 2^i \cdot y \ \wedge\ z \neq y \ \wedge\ i = V\}$
(* *prepare* $i := i - 1$*;* $z \neq y \ \wedge\ z = 2^i \cdot y \ \wedge\ i \geq 0 \Rightarrow i > 0$ *)
$\{X = q \cdot z + x \ \wedge\ 0 \leq x < z \ \wedge\ i - 1 \geq 0 \ \wedge\ z = 2 \cdot 2^{i-1} \cdot y \ \wedge\ i - 1 < V\}$
$i := i - 1;$
$\{X = q \cdot z + x \ \wedge\ 0 \leq x < z \ \wedge\ i \geq 0 \ \wedge\ z = 2 \cdot 2^i \cdot y \ \wedge\ i < V\}$
(* z *is even;* $z = 2(z \ \mathbf{div}\ 2)$*; calculus* *)
$\{X = 2 \cdot q \cdot (z \ \mathbf{div}\ 2) + x \wedge 0 \leq x < 2(z \ \mathbf{div}\ 2) \wedge i \geq 0 \wedge z \ \mathbf{div}\ 2 = 2^i \cdot y \wedge i < V\}$
$z := z \ \mathbf{div}\ 2;$

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

Exercise 7.6: Body of the Main Loop

$\{J \wedge B \ \wedge \ vf = V\}$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ z \neq y \ \wedge \ i = V\}$
(* *prepare* $i := i - 1$; $z \neq y \ \wedge \ z = 2^i \cdot y \ \wedge \ i \geq 0 \Rightarrow i > 0$ *)
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i - 1 \geq 0 \ \wedge \ z = 2 \cdot 2^{i-1} \cdot y \ \wedge \ i - 1 < V\}$
$i := i - 1;$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2 \cdot 2^i \cdot y \ \wedge \ i < V\}$
(* z *is even*; $z = 2(z \ \mathbf{div}\ 2)$; *calculus* *)
$\{X = 2 \cdot q \cdot (z \ \mathbf{div}\ 2) + x \wedge 0 \leq x < 2(z \ \mathbf{div}\ 2) \wedge i \geq 0 \wedge z \ \mathbf{div}\ 2 = 2^i \cdot y \wedge i < V\}$
$z := z \ \mathbf{div}\ 2;$
$\{X = 2 \cdot q \cdot z + x \ \wedge \ 0 \leq x < 2 \cdot z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$

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

Exercise 7.6: Body of the Main Loop

$\{J \land B \ \land \ vf = V\}$
$\{X = q \cdot z + x \ \land \ 0 \leq x < z \ \land \ i \geq 0 \ \land \ z = 2^i \cdot y \ \land \ z \neq y \ \land \ i = V\}$
(* *prepare* $i := i - 1$; $z \neq y \ \land \ z = 2^i \cdot y \ \land \ i \geq 0 \Rightarrow i > 0$ *)
$\{X = q \cdot z + x \ \land \ 0 \leq x < z \ \land \ i - 1 \geq 0 \ \land \ z = 2 \cdot 2^{i-1} \cdot y \ \land \ i - 1 < V\}$
$i := i - 1;$
$\{X = q \cdot z + x \ \land \ 0 \leq x < z \ \land \ i \geq 0 \ \land \ z = 2 \cdot 2^i \cdot y \ \land \ i < V\}$
(* z *is even*; $z = 2(z \textbf{ div } 2)$; *calculus* *)
$\{X = 2 \cdot q \cdot (z \textbf{ div } 2) + x \land 0 \leq x < 2(z \textbf{ div } 2) \land i \geq 0 \land z \textbf{ div } 2 = 2^i \cdot y \land i < V\}$
$z := z \textbf{ div } 2;$
$\{X = 2 \cdot q \cdot z + x \ \land \ 0 \leq x < 2 \cdot z \ \land \ i \geq 0 \ \land \ z = 2^i \cdot y \ \land \ i < V\}$
$q := 2 * q;$

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

Exercise 7.6: Body of the Main Loop

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

$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ z \neq y \ \wedge \ i = V\}$

(* *prepare* $i := i - 1$; $z \neq y \ \wedge \ z = 2^i \cdot y \ \wedge \ i \geq 0 \Rightarrow i > 0$ *)

$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i - 1 \geq 0 \ \wedge \ z = 2 \cdot 2^{i-1} \cdot y \ \wedge \ i - 1 < V\}$

$i := i - 1;$

$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2 \cdot 2^i \cdot y \ \wedge \ i < V\}$

(* z *is even;* $z = 2(z \ \mathbf{div}\ 2)$; *calculus* *)

$\{X = 2 \cdot q \cdot (z \ \mathbf{div}\ 2) + x \wedge 0 \leq x < 2(z \ \mathbf{div}\ 2) \wedge i \geq 0 \wedge z \ \mathbf{div}\ 2 = 2^i \cdot y \wedge i < V\}$

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

$\{X = 2 \cdot q \cdot z + x \ \wedge \ 0 \leq x < 2 \cdot z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$

$q := 2 * q;$

$\{X = q \cdot z + x \ \wedge \ 0 \leq x < 2 \cdot z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$

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

Exercise 7.6: Body of the Main Loop

$\{J \wedge B \ \wedge \ vf = V\}$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ z \neq y \ \wedge \ i = V\}$
(* *prepare* $i := i - 1$; $z \neq y \ \wedge \ z = 2^i \cdot y \ \wedge \ i \geq 0 \Rightarrow i > 0$ *)
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i - 1 \geq 0 \ \wedge \ z = 2 \cdot 2^{i-1} \cdot y \ \wedge \ i - 1 < V\}$
$i := i - 1;$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2 \cdot 2^i \cdot y \ \wedge \ i < V\}$
(* z *is even*; $z = 2(z \ \textbf{div} \ 2)$; *calculus* *)
$\{X = 2 \cdot q \cdot (z \ \textbf{div} \ 2) + x \wedge 0 \leq x < 2(z \ \textbf{div} \ 2) \wedge i \geq 0 \wedge z \ \textbf{div} \ 2 = 2^i \cdot y \wedge i < V\}$
$z := z$ **div** $2;$
$\{X = 2 \cdot q \cdot z + x \ \wedge \ 0 \leq x < 2 \cdot z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
$q := 2 * q;$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < 2 \cdot z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
if $x < z$ **then**
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < 2 \cdot z \ \wedge \ x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$

else
$\{X = q \cdot z + x \ \wedge \ z \leq x < 2 \cdot z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$

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

Exercise 7.6: Body of the Main Loop

$\{J \wedge B \ \wedge \ vf = V\}$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ z \neq y \ \wedge \ i = V\}$
(* *prepare* $i := i - 1$; $z \neq y \ \wedge \ z = 2^i \cdot y \ \wedge \ i \geq 0 \Rightarrow i > 0$ *)
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i - 1 \geq 0 \ \wedge \ z = 2 \cdot 2^{i-1} \cdot y \ \wedge \ i - 1 < V\}$
$i := i - 1;$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2 \cdot 2^i \cdot y \ \wedge \ i < V\}$
(* z *is even;* $z = 2(z \ \textbf{div}\ 2)$; *calculus* *)
$\{X = 2 \cdot q \cdot (z \ \textbf{div}\ 2) + x \wedge 0 \leq x < 2(z \ \textbf{div}\ 2) \wedge i \geq 0 \wedge z \ \textbf{div}\ 2 = 2^i \cdot y \wedge i < V\}$
$z := z$ **div** $2;$
$\{X = 2 \cdot q \cdot z + x \ \wedge \ 0 \leq x < 2 \cdot z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
$q := 2 * q;$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < 2 \cdot z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
if $x < z$ **then**
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < 2 \cdot z \ \wedge \ x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
skip;

else
$\{X = q \cdot z + x \ \wedge \ z \leq x < 2 \cdot z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$

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

Exercise 7.6: Body of the Main Loop

$\{J \wedge B \ \wedge\ vf = V\}$
$\{X = q \cdot z + x \ \wedge\ 0 \leq x < z \ \wedge\ i \geq 0 \ \wedge\ z = 2^i \cdot y \ \wedge\ z \neq y \ \wedge\ i = V\}$
(* prepare $i := i - 1$; $z \neq y \ \wedge\ z = 2^i \cdot y \ \wedge\ i \geq 0 \Rightarrow i > 0$ *)
$\{X = q \cdot z + x \ \wedge\ 0 \leq x < z \ \wedge\ i - 1 \geq 0 \ \wedge\ z = 2 \cdot 2^{i-1} \cdot y \ \wedge\ i - 1 < V\}$
$i := i - 1;$
$\{X = q \cdot z + x \ \wedge\ 0 \leq x < z \ \wedge\ i \geq 0 \ \wedge\ z = 2 \cdot 2^i \cdot y \ \wedge\ i < V\}$
(* z is even; $z = 2(z \textbf{ div } 2)$; calculus *)
$\{X = 2 \cdot q \cdot (z \textbf{ div } 2) + x \wedge 0 \leq x < 2(z \textbf{ div } 2) \wedge i \geq 0 \wedge z \textbf{ div } 2 = 2^i \cdot y \wedge i < V\}$
$z := z$ **div** $2;$
$\{X = 2 \cdot q \cdot z + x \ \wedge\ 0 \leq x < 2 \cdot z \ \wedge\ i \geq 0 \ \wedge\ z = 2^i \cdot y \ \wedge\ i < V\}$
$q := 2 * q;$
$\{X = q \cdot z + x \ \wedge\ 0 \leq x < 2 \cdot z \ \wedge\ i \geq 0 \ \wedge\ z = 2^i \cdot y \ \wedge\ i < V\}$
if $x < z$ **then**
$\{X = q \cdot z + x \ \wedge\ 0 \leq x < 2 \cdot z \ \wedge\ x < z \ \wedge\ i \geq 0 \ \wedge\ z = 2^i \cdot y \ \wedge\ i < V\}$
skip;
$\{J \ \wedge\ vf < V\}$
else
$\{X = q \cdot z + x \ \wedge\ z \leq x < 2 \cdot z \ \wedge\ i \geq 0 \ \wedge\ z = 2^i \cdot y \ \wedge\ i < V\}$

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

Exercise 7.6: Body of the Main Loop

$\{J \land B \ \land \ vf = V\}$
$\{X = q \cdot z + x \ \land \ 0 \leq x < z \ \land \ i \geq 0 \ \land \ z = 2^i \cdot y \ \land \ z \neq y \ \land \ i = V\}$
(* *prepare* $i := i - 1$; $z \neq y \ \land \ z = 2^i \cdot y \ \land \ i \geq 0 \Rightarrow i > 0$ *)
$\{X = q \cdot z + x \ \land \ 0 \leq x < z \ \land \ i - 1 \geq 0 \ \land \ z = 2 \cdot 2^{i-1} \cdot y \ \land \ i - 1 < V\}$
$i := i - 1;$
$\{X = q \cdot z + x \ \land \ 0 \leq x < z \ \land \ i \geq 0 \ \land \ z = 2 \cdot 2^i \cdot y \ \land \ i < V\}$
(* z *is even*; $z = 2(z \ \textbf{div}\ 2)$; *calculus* *)
$\{X = 2 \cdot q \cdot (z \ \textbf{div}\ 2) + x \land 0 \leq x < 2(z \ \textbf{div}\ 2) \land i \geq 0 \land z \ \textbf{div}\ 2 = 2^i \cdot y \land i < V\}$
$z := z$ **div** $2;$
$\{X = 2 \cdot q \cdot z + x \ \land \ 0 \leq x < 2 \cdot z \ \land \ i \geq 0 \ \land \ z = 2^i \cdot y \ \land \ i < V\}$
$q := 2 * q;$
$\{X = q \cdot z + x \ \land \ 0 \leq x < 2 \cdot z \ \land \ i \geq 0 \ \land \ z = 2^i \cdot y \ \land \ i < V\}$
if $x < z$ **then**
$\{X = q \cdot z + x \ \land \ 0 \leq x < 2 \cdot z \ \land \ x < z \ \land \ i \geq 0 \ \land \ z = 2^i \cdot y \ \land \ i < V\}$
skip;
$\{J \ \land \ vf < V\}$
else
$\{X = q \cdot z + x \ \land \ z \leq x < 2 \cdot z \ \land \ i \geq 0 \ \land \ z = 2^i \cdot y \ \land \ i < V\}$
$\{X = (q + 1) \cdot z + x - z \ \land \ 0 \leq x - z < z \ \land \ i \geq 0 \ \land \ z = 2^i \cdot y \ \land \ i < V\}$

end
$\{J \ \land \ vf < V\}$

Exercise 7.6: Body of the Main Loop

$\{J \wedge B \ \wedge \ vf \ = \ V\}$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ z \neq y \ \wedge \ i = V\}$
(* *prepare* $i := i - 1$; $z \neq y \ \wedge \ z = 2^i \cdot y \ \wedge \ i \geq 0 \Rightarrow i > 0$ *)
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i - 1 \geq 0 \ \wedge \ z = 2 \cdot 2^{i-1} \cdot y \ \wedge \ i - 1 < V\}$
$i := i - 1;$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2 \cdot 2^i \cdot y \ \wedge \ i < V\}$
(* z *is even*; $z = 2(z$ **div** $2)$; *calculus* *)
$\{X = 2 \cdot q \cdot (z \textbf{ div } 2) + x \wedge 0 \leq x < 2(z \textbf{ div } 2) \wedge i \geq 0 \wedge z \textbf{ div } 2 = 2^i \cdot y \wedge i < V\}$
$z := z$ **div** 2;
$\{X = 2 \cdot q \cdot z + x \ \wedge \ 0 \leq x < 2 \cdot z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
$q := 2 * q;$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < 2 \cdot z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
if $x < z$ **then**
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < 2 \cdot z \ \wedge \ x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
skip;
$\{J \ \wedge \ vf \ < \ V\}$
else
$\{X = q \cdot z + x \ \wedge \ z \leq x < 2 \cdot z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
$\{X = (q + 1) \cdot z + x - z \ \wedge \ 0 \leq x - z < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
$q := q + 1;$

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

Exercise 7.6: Body of the Main Loop

$\{J \wedge B \ \wedge \ vf = V\}$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ z \neq y \ \wedge \ i = V\}$
(* *prepare* $i := i - 1$; $z \neq y \ \wedge \ z = 2^i \cdot y \ \wedge \ i \geq 0 \Rightarrow i > 0$ *)
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i - 1 \geq 0 \ \wedge \ z = 2 \cdot 2^{i-1} \cdot y \ \wedge \ i - 1 < V\}$
$i := i - 1;$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2 \cdot 2^i \cdot y \ \wedge \ i < V\}$
(* z *is even*; $z = 2(z \textbf{ div } 2)$; *calculus* *)
$\{X = 2 \cdot q \cdot (z \textbf{ div } 2) + x \wedge 0 \leq x < 2(z \textbf{ div } 2) \wedge i \geq 0 \wedge z \textbf{ div } 2 = 2^i \cdot y \wedge i < V\}$
$z := z$ **div** $2;$
$\{X = 2 \cdot q \cdot z + x \ \wedge \ 0 \leq x < 2 \cdot z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
$q := 2 * q;$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < 2 \cdot z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
if $x < z$ **then**
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < 2 \cdot z \ \wedge \ x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
skip;
$\{J \ \wedge \ vf < V\}$
else
$\{X = q \cdot z + x \ \wedge \ z \leq x < 2 \cdot z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
$\{X = (q + 1) \cdot z + x - z \ \wedge \ 0 \leq x - z < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
$q := q + 1;$
$\{X = q \cdot z + x - z \ \wedge \ 0 \leq x - z < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$

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

Exercise 7.6: Body of the Main Loop

$\{J \wedge B \ \wedge \ vf = V\}$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ z \neq y \ \wedge \ i = V\}$
(* prepare $i := i - 1$; $z \neq y \ \wedge \ z = 2^i \cdot y \ \wedge \ i \geq 0 \Rightarrow i > 0$ *)
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i - 1 \geq 0 \ \wedge \ z = 2 \cdot 2^{i-1} \cdot y \ \wedge \ i - 1 < V\}$
$i := i - 1;$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2 \cdot 2^i \cdot y \ \wedge \ i < V\}$
(* z is even; $z = 2(z \textbf{ div } 2)$; calculus *)
$\{X = 2 \cdot q \cdot (z \textbf{ div } 2) + x \wedge 0 \leq x < 2(z \textbf{ div } 2) \wedge i \geq 0 \wedge z \textbf{ div } 2 = 2^i \cdot y \wedge i < V\}$
$z := z$ **div** $2;$
$\{X = 2 \cdot q \cdot z + x \ \wedge \ 0 \leq x < 2 \cdot z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
$q := 2 * q;$
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < 2 \cdot z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
if $x < z$ **then**
$\{X = q \cdot z + x \ \wedge \ 0 \leq x < 2 \cdot z \ \wedge \ x < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
skip;
$\{J \ \wedge \ vf < V\}$
else
$\{X = q \cdot z + x \ \wedge \ z \leq x < 2 \cdot z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
$\{X = (q + 1) \cdot z + x - z \ \wedge \ 0 \leq x - z < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
$q := q + 1;$
$\{X = q \cdot z + x - z \ \wedge \ 0 \leq x - z < z \ \wedge \ i \geq 0 \ \wedge \ z = 2^i \cdot y \ \wedge \ i < V\}$
$x := x - z;$

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

Exercise 7.6: Body of the Main Loop

$\{J \wedge B \;\wedge\; vf = V\}$
$\{X = q \cdot z + x \;\wedge\; 0 \leq x < z \;\wedge\; i \geq 0 \;\wedge\; z = 2^i \cdot y \;\wedge\; z \neq y \;\wedge\; i = V\}$
(* *prepare* $i := i - 1$; $z \neq y \;\wedge\; z = 2^i \cdot y \;\wedge\; i \geq 0 \Rightarrow i > 0$ *)
$\{X = q \cdot z + x \;\wedge\; 0 \leq x < z \;\wedge\; i - 1 \geq 0 \;\wedge\; z = 2 \cdot 2^{i-1} \cdot y \;\wedge\; i - 1 < V\}$
$i := i - 1;$
$\{X = q \cdot z + x \;\wedge\; 0 \leq x < z \;\wedge\; i \geq 0 \;\wedge\; z = 2 \cdot 2^i \cdot y \;\wedge\; i < V\}$
(* z *is even*; $z = 2(z \textbf{ div } 2)$; *calculus* *)
$\{X = 2 \cdot q \cdot (z \textbf{ div } 2) + x \wedge 0 \leq x < 2(z \textbf{ div } 2) \wedge i \geq 0 \wedge z \textbf{ div } 2 = 2^i \cdot y \wedge i < V\}$
$z := z$ **div** $2;$
$\{X = 2 \cdot q \cdot z + x \;\wedge\; 0 \leq x < 2 \cdot z \;\wedge\; i \geq 0 \;\wedge\; z = 2^i \cdot y \;\wedge\; i < V\}$
$q := 2 * q;$
$\{X = q \cdot z + x \;\wedge\; 0 \leq x < 2 \cdot z \;\wedge\; i \geq 0 \;\wedge\; z = 2^i \cdot y \;\wedge\; i < V\}$
if $x < z$ **then**
$\{X = q \cdot z + x \;\wedge\; 0 \leq x < 2 \cdot z \;\wedge\; x < z \;\wedge\; i \geq 0 \;\wedge\; z = 2^i \cdot y \;\wedge\; i < V\}$
skip;
$\{J \;\wedge\; vf < V\}$
else
$\{X = q \cdot z + x \;\wedge\; z \leq x < 2 \cdot z \;\wedge\; i \geq 0 \;\wedge\; z = 2^i \cdot y \;\wedge\; i < V\}$
$\{X = (q + 1) \cdot z + x - z \;\wedge\; 0 \leq x - z < z \;\wedge\; i \geq 0 \;\wedge\; z = 2^i \cdot y \;\wedge\; i < V\}$
$q := q + 1;$
$\{X = q \cdot z + x - z \;\wedge\; 0 \leq x - z < z \;\wedge\; i \geq 0 \;\wedge\; z = 2^i \cdot y \;\wedge\; i < V\}$
$x := x - z;$
$\{J \;\wedge\; vf < V\}$
end (* *collect branches* *)
$\{J \;\wedge\; vf < V\}$

Exercise 7.6: Conclusion

5 Conclusion: We derived the following program fragment.

$\{P : x = X \wedge X \geq 0\}$
$z := y;$
$i := 0;$
while $z \leq x$ **do**
$\quad z := 2 * z;$
$\quad i := i + 1;$
end;
$q := 0;$
while $z \neq y$ **do**
$\quad i := i - 1;$
$\quad z := z$ **div** $2;$
$\quad q := 2 * q;$
$\quad$**if** $x \geq z$ **then**
$\qquad q := q + 1;$
$\qquad x := x - z$
$\quad$**end**;
end;
$\{Q : X = q \cdot y + x \wedge 0 \leq x < y\}$

Above, i is a ghost variable: we only use it to make the proof easier.

Exercise 7.6: Conclusion

5 Conclusion: We derived the following program fragment.

$$\{P : x = X \wedge X \geq 0\}$$

$z := y;$
$i := 0;$
while $z \leq x$ **do**
  $z := 2 * z;$
  $i := i + 1;$
end;
$q := 0;$
while $z \neq y$ **do**
  $i := i - 1;$
  $z := z$ **div** $2;$
  $q := 2 * q;$
  if $x \geq z$ **then**
    $q := q + 1;$
    $x := x - z$
  end;
end;

$$\{Q : X = q \cdot y + x \wedge 0 \leq x < y\}$$

Above, i is a ghost variable: we only use it to make the proof easier.
We can remove all assignments to i.

Exercise 7.6: Conclusion

5 Conclusion: We derived the following program fragment.

$$\{P : x = X \wedge X \geq 0\}$$

$z := y;$
while $z \leq x$ **do**
  $z := 2 * z;$
end;
$q := 0;$
while $z \neq y$ **do**
  $z := z$ **div** $2;$
  $q := 2 * q;$
  if $x \geq z$ **then**
    $q := q + 1;$
    $x := x - z$
  end;
end;

$$\{Q : X = q \cdot y + x \wedge 0 \leq x < y\}$$

The final program.

Comparison between 7.5 and 7.6

Exercise 7.5:

$q := 0$;
while $y \leq x$ **do**
  $x := x - y$;
  $q := q + 1$;
end;

Comparison between 7.5 and 7.6

Exercise 7.5:

$q := 0;$
while $y \leq x$ **do**
  $x := x - y;$
  $q := q + 1;$
end;

Exercise 7.6:

$z := y;$
while $z \leq x$ **do**
  $z := 2 * z;$
end;
$q := 0;$
while $z \neq y$ **do**
  $z := z$ **div** $2;$
  $q := 2 * q;$
  if $x \geq z$ **then**
    $q := q + 1;$
    $x := x - z$
  end;
end;

Comparison between 7.5 and 7.6

The program in 7.6 is generally faster than the one in 7.5.

Comparison between 7.5 and 7.6

The program in 7.6 is generally faster than the one in 7.5.

Consider some sample values: $x = 864$, $y = 23$.

- The program in 7.5 returns $q = 37$ (because $864 = 23 * 37 + 13$)
  That is, the assignment $q := q + 1$ is executed 37 times.

Comparison between 7.5 and 7.6

The program in 7.6 is generally faster than the one in 7.5.

Consider some sample values: $x = 864$, $y = 23$.

- The program in 7.5 returns $q = 37$ (because $864 = 23 * 37 + 13$)
  That is, the assignment $q := q + 1$ is executed 37 times.
- The analysis for the program in 7.6 is more complicated.
  The auxiliary loop is executed n times, where n is the smallest value for which $2^n \cdot y > x$.
  That is, this loop runs at most $n = \lfloor \log_2(x \textbf{ div } y) \rfloor = \lfloor \log_2(q) \rfloor$.
  For $q = 37$, we have $n = 5$ iterations.
- After the auxiliary loop, we have $y \leq z$ <u>and</u> z **div** $2 \leq x < z$.
  The guard of the **if** is true in the first iteration and so $q = 1$.
  In each following iteration q is doubled (at least).
  Since $2^6 = 64 > 37$, this loop is executed at most 6 times.
  For $q = 37$, the total amount of iterations is approximately 10.

In terms of complexity analysis (not in this course):
Linear time (7.5) vs logarithmic (7.6).

The End

- This week:
  Exercises 7.1, 7.2, and 7.8 // Square root (Exercises 7.3 and 7.4) // Integral division (Exercises 7.5 and 7.6)
- Next week: Chapter 8. Read in advance!