university of groningen

Program Correctness

Block 6

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

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

March 9, 2023

Adding Information to the Invariant

- Following the roadmap entails determining an invariant J, a guard B, and a postcondition Q such that

$$J \ \wedge \ \neg B \Rightarrow \ Q$$

Adding Information to the Invariant

- Following the roadmap entails determining an invariant J, a guard B, and a postcondition Q such that

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

- Adding conjuncts to J makes it stronger:

$$(\underbrace{J \land J_1 \land \cdots \land J_n}_{J'} \Rightarrow J)$$

- This is safe:

$$(J \land \neg B \Rightarrow Q) \land (J' \Rightarrow J) \Rightarrow (J' \land \neg B \Rightarrow Q)$$

We illustrate this technique on a number of examples.

Outline

Longest positive subsequence (LPS)

Given $n \in \mathbb{N}^+$ and an array $a[0..n)$ of $\mathbb{Z}$, compute the length of the longest subsequence of $[0..n)$ for which a is positive.

Example: A simple array $a[0..9)$:

0	1	2	3	4	5	6	7	8
-1	4	5	0	-3	6	4	2	0

Longest positive subsequence (LPS)

Given $n \in \mathbb{N}^+$ and an array $a[0..n)$ of $\mathbb{Z}$, compute the length of the longest subsequence of $[0..n)$ for which a is positive.

Example: A simple array $a[0..9)$:

-1	4	5	0	-3	6	4	2	0
0	1	2	3	4	5	6	7	8

Two positive subsequences: $(4, 5)$ and $(6, 4, 2)$.

Longest positive subsequence (LPS)

Given $n \in \mathbb{N}^+$ and an array $a[0..n)$ of $\mathbb{Z}$, compute the length of the longest subsequence of $[0..n)$ for which a is positive.

Example: A simple array $a[0..9)$:

-1	4	5	0	-3	6	4	2	0
0	1	2	3	4	5	6	7	8

Two positive subsequences: $(4, 5)$ and $(6, 4, 2)$.

A predicate to characterize the interval where the LPS occurs:

- $C(p, q) \equiv (\forall i \in [p, q) : a[i] > 0)$ defines subsequences.
  Above, we have $C(1, 3)$ and $C(5, 8)$.
  Note: $C(p, p)$ holds for any p.

LPS

How to define the LPS in terms of minimum and maximum?

- Consider the set below, with q being a fixed extreme for the subsequences:

$$\text{Min}\ \{p \mid p : 0 \leq p \leq q \ \wedge\ C(p, q)\}$$

Note: the minimum p gives us the longest subsequence for q.

LPS

How to define the LPS in terms of minimum and maximum?

- Consider the set below, with q being a fixed extreme for the subsequences:

  $$\text{Min } \{p \mid p : 0 \leq p \leq q \ \wedge \ C(p, q)\}$$

  Note: the minimum p gives us the longest subsequence for q.
- We need something more general, for arbitrary extremes:

  $$\text{Max } \{q - p \mid p, q : 0 \leq p \leq q \leq n \ \wedge \ C(p, q)\}$$

  Note: we maximize the difference between the extremes.

Using the predicate

$$C(p, q) \equiv (\forall i \in [p, q) : a[i] > 0)$$

we can now specify the problem as follows:

$\textbf{const}\ n :\ \mathbb{N}^+,\ a :\ \textbf{array}\ [0..n)\ \textbf{of}\ \mathbb{Z};$
$\textbf{var}\ z :\ \mathbb{Z};$
$\quad \{P :\ \textbf{true}\}$
C
$\quad \{Q :\ z = \text{Max}\,\{q - p \mid p, q : 0 \leq p \leq q \leq n\ \wedge\ C(p, q)\}\}$

LPS

Up to here we have

$$C(p, q) \equiv (\forall i \in [p, q) : a[i] > 0)$$
$$Q : \; z = \text{Max}\,\{q - p \mid p, q : 0 \leq p \leq q \leq n \;\wedge\; C(p, q)\}$$

We replace the constant n by variable k in Q. We define:

$$L(k) = \text{Max}\,\{q - p \mid p, q : 0 \leq p \leq q \leq k \;\wedge\; C(p, q)\}$$

and we rewrite Q as $z = L(n)$.

LPS: Rewriting $L(k)$

Let's define (actually, recall) the following:

$$E(q) = \text{Min}\ \{p \mid p : 0 \leq p \leq q\ \wedge\ C(p, q)\}$$

LPS: Rewriting $L(k)$

Let's define (actually, recall) the following:

$$E(q) = \text{Min}\ \{p \mid p : 0 \leq p \leq q\ \wedge\ C(p,q)\}$$

We can now rewrite $L(k)$:

$$L(k) \quad = \quad \text{Max}\ \{q - p \mid p, q : 0 \leq p \leq q \leq k\ \wedge\ C(p,q)\}$$

LPS: Rewriting $L(k)$

Let's define (actually, recall) the following:

$$E(q) = \text{Min}\ \{p \mid p : 0 \leq p \leq q\ \wedge\ C(p, q)\}$$

We can now rewrite $L(k)$:

$$\begin{aligned} L(k) &= \text{Max}\ \{q - p \mid p, q : 0 \leq p \leq q \leq k\ \wedge\ C(p, q)\} \\ &= \text{Max}\ \{\text{Max}\ \{q - p \mid p : 0 \leq p \leq q\ \wedge\ C(p, q)\} \mid q : q \leq k\} \end{aligned}$$

LPS: Rewriting $L(k)$

Let's define (actually, recall) the following:

$$E(q) = \text{Min}\ \{p \mid p : 0 \le p \le q\ \wedge\ C(p, q)\}$$

We can now rewrite $L(k)$:

$$\begin{aligned} L(k) &= \text{Max}\ \{q - p \mid p, q : 0 \le p \le q \le k\ \wedge\ C(p, q)\} \\ &= \text{Max}\ \{\text{Max}\ \{q - p \mid p : 0 \le p \le q\ \wedge\ C(p, q)\} \mid q : q \le k\} \\ &= \text{Max}\ \{q + \text{Max}\ \{-p \mid p : 0 \le p \le q\ \wedge\ C(p, q)\} \mid q : q \le k\} \end{aligned}$$

LPS: Rewriting $L(k)$

Let's define (actually, recall) the following:

$$E(q) = \text{Min}\ \{p \mid p : 0 \leq p \leq q\ \wedge\ C(p, q)\}$$

We can now rewrite $L(k)$:

$$\begin{aligned}
L(k) &= \text{Max}\ \{q - p \mid p, q : 0 \leq p \leq q \leq k\ \wedge\ C(p, q)\} \\
&= \text{Max}\ \{\text{Max}\ \{q - p \mid p : 0 \leq p \leq q\ \wedge\ C(p, q)\} \mid q : q \leq k\} \\
&= \text{Max}\ \{q + \text{Max}\ \{-p \mid p : 0 \leq p \leq q\ \wedge\ C(p, q)\} \mid q : q \leq k\} \\
&= \text{Max}\ \{q - \underbrace{\text{Min}\ \{p \mid p : 0 \leq p \leq q\ \wedge\ C(p, q)\}}_{E(q)} \mid q : q \leq k\}
\end{aligned}$$

LPS: Rewriting $L(k)$

Let's define (actually, recall) the following:

$$E(q) = \text{Min}\ \{p \mid p : 0 \leq p \leq q\ \wedge\ C(p,q)\}$$

We can now rewrite $L(k)$:

$$\begin{aligned}
L(k) &= \text{Max}\ \{q - p \mid p, q : 0 \leq p \leq q \leq k\ \wedge\ C(p,q)\} \\
&= \text{Max}\ \{\text{Max}\ \{q - p \mid p : 0 \leq p \leq q\ \wedge\ C(p,q)\} \mid q : q \leq k\} \\
&= \text{Max}\ \{q + \text{Max}\ \{-p \mid p : 0 \leq p \leq q\ \wedge\ C(p,q)\} \mid q : q \leq k\} \\
&= \text{Max}\ \{q - \underbrace{\text{Min}\ \{p \mid p : 0 \leq p \leq q\ \wedge\ C(p,q)\}}_{E(q)} \mid q : q \leq k\} \\
&= \text{Max}\ \{q - E(q) \mid q : q \leq k\}
\end{aligned}$$

LPS: Examining $L(k)$

The idea is to increment k in each iteration.
Let us first examine $L(k+1)$:

LPS: Examining $L(k)$

The idea is to increment k in each iteration.
Let us first examine $L(k+1)$:

$$\begin{array}{ll} & L(k+1) \\ = & \quad \{\text{definition } L\} \\ & \text{Max } \{q - E(q) \mid q : q \leq k+1\} \end{array}$$

LPS: Examining $L(k)$

The idea is to increment k in each iteration.
Let us first examine $L(k+1)$:

$$
\begin{aligned}
& L(k+1) \\
= \quad & \{\text{definition } L\} \\
& \text{Max}\,\{q - E(q) \mid q : q \leq k+1\} \\
= \quad & \{\text{split domain: } q \leq k \vee q = k+1\} \\
& \text{Max}\,\{q - E(q) \mid q : q \leq k\} \ \mathtt{max}\ (k+1-E(k+1))
\end{aligned}
$$

LPS: Examining $L(k)$

The idea is to increment k in each iteration.
Let us first examine $L(k+1)$:

$$
\begin{aligned}
& L(k+1) \\
= \quad & \{\text{definition } L\} \\
& \text{Max}\ \{q - E(q) \mid q : q \leq k+1\} \\
= \quad & \{\text{split domain: } q \leq k \vee q = k+1\} \\
& \text{Max}\ \{q - E(q) \mid q : q \leq k\} \ \mathtt{max}\ (k+1-E(k+1)) \\
= \quad & \{\text{definition } L\} \\
& L(k)\ \mathtt{max}\ (k+1-E(k+1))
\end{aligned}
$$

We now examine $E(k+1)$. Note that:

- $C(p, k+1) \equiv C(p, q) \wedge a[q] > 0$
- $E(q) \leq q$ (for every $q \geq 0$)

LPS: Examining $E(k)$ (1/2)

$$
\begin{array}{ll}
& E(k+1) \\
= & \quad \{\text{definition } E\} \\
& \text{Min}\,\{p \mid p : 0 \le p \le k+1 \ \wedge\ C(p, k+1)\}
\end{array}
$$

LPS: Examining $E(k)$ (1/2)

$$
\begin{array}{ll}
 & E(k+1) \\
= & \quad \{\text{definition } E\} \\
 & \text{Min } \{p \mid p : 0 \le p \le k+1 \ \wedge \ C(p, k+1)\} \\
= & \quad \{\textbf{assume } k \ge 0\text{; split domain: } p \le k \vee p = k+1\text{; use } C(k+1, k+1)\}
\end{array}
$$

LPS: Examining $E(k)$ (1/2)

$$
\begin{array}{ll}
 & E(k+1) \\
= & \quad \{\text{definition } E\} \\
 & \text{Min}\,\{p \mid p : 0 \le p \le k+1 \ \wedge\ C(p,k+1)\} \\
= & \quad \{\textbf{assume } k \ge 0\text{; split domain: } p \le k \vee p = k+1\text{; use } C(k+1,k+1)\} \\
 & \text{Min}\,\{p \mid p : 0 \le p \le k \ \wedge\ C(p,k+1)\}\ \min\ (k+1)
\end{array}
$$

LPS: Examining $E(k)$ (1/2)

$$
\begin{array}{ll}
& E(k+1) \\
= & \quad \{\text{definition } E\} \\
& \text{Min}\ \{p \mid p : 0 \leq p \leq k+1 \ \wedge \ C(p, k+1)\} \\
= & \quad \{\textbf{assume } k \geq 0\text{; split domain: } p \leq k \vee p = k+1\text{; use } C(k+1, k+1)\} \\
& \text{Min}\ \{p \mid p : 0 \leq p \leq k \ \wedge \ C(p, k+1)\} \ \mathrm{min} \ (k+1) \\
= & \quad \{(\forall i \in [p, k+1) : a[i] > 0) \equiv (a[k] > 0 \ \wedge \ (\forall i \in [p, k) : a[i] > 0))\} \\
& \text{Min}\ \{p \mid p : 0 \leq p \leq k \ \wedge \ C(p, k) \ \wedge \ a[k] > 0\} \ \mathrm{min} \ (k+1)
\end{array}
$$

LPS: Examining $E(k)$ (1/2)

$$
\begin{array}{ll}
& E(k+1) \\
= & \quad \{\text{definition } E\} \\
& \text{Min}\ \{p \mid p : 0 \le p \le k+1\ \wedge\ C(p, k+1)\} \\
= & \quad \{\textbf{assume } k \ge 0\text{; split domain: } p \le k \vee p = k+1\text{; use } C(k+1, k+1)\} \\
& \text{Min}\ \{p \mid p : 0 \le p \le k\ \wedge\ C(p, k+1)\}\ \min\ (k+1) \\
= & \quad \{(\forall i \in [p, k+1) : a[i] > 0) \equiv (a[k] > 0\ \wedge\ (\forall i \in [p, k) : a[i] > 0))\} \\
& \text{Min}\ \{p \mid p : 0 \le p \le k\ \wedge\ C(p, k)\ \wedge\ a[k] > 0\}\ \min\ (k+1) \\
= & \quad \{\textbf{assume } a[k] > 0\} \\
& \text{Min}\ \{p \mid p : 0 \le p \le k\ \wedge\ C(p, k)\}\ \min\ (k+1)
\end{array}
$$

LPS: Examining $E(k)$ (1/2)

$$
\begin{array}{ll}
 & E(k+1) \\
= & \{\text{definition } E\} \\
 & \text{Min } \{p \mid p : 0 \le p \le k+1 \ \wedge \ C(p, k+1)\} \\
= & \{\textbf{assume } k \ge 0\text{; split domain: } p \le k \vee p = k+1\text{; use } C(k+1, k+1)\} \\
 & \text{Min } \{p \mid p : 0 \le p \le k \ \wedge \ C(p, k+1)\} \ \min \ (k+1) \\
= & \{(\forall i \in [p, k+1) : a[i] > 0) \equiv (a[k] > 0 \ \wedge \ (\forall i \in [p, k) : a[i] > 0))\} \\
 & \text{Min } \{p \mid p : 0 \le p \le k \ \wedge \ C(p, k) \ \wedge \ a[k] > 0\} \ \min \ (k+1) \\
= & \{\textbf{assume } a[k] > 0\} \\
 & \text{Min } \{p \mid p : 0 \le p \le k \ \wedge \ C(p, k)\} \ \min \ (k+1) \\
= & \{\text{Min } \{p \mid p : 0 \le p \le k \ \wedge \ C(p, k)\} \le k < k+1\}
\end{array}
$$

LPS: Examining $E(k)$ (1/2)

$$
\begin{array}{ll}
 & E(k+1) \\
= & \quad \{\text{definition } E\} \\
 & \text{Min}\,\{p \mid p : 0 \leq p \leq k+1 \ \wedge \ C(p, k+1)\} \\
= & \quad \{\textbf{assume } k \geq 0\text{; split domain: } p \leq k \vee p = k+1\text{; use } C(k+1, k+1)\} \\
 & \text{Min}\,\{p \mid p : 0 \leq p \leq k \ \wedge \ C(p, k+1)\} \ \min \ (k+1) \\
= & \quad \{(\forall i \in [p, k+1) : a[i] > 0) \equiv (a[k] > 0 \ \wedge \ (\forall i \in [p, k) : a[i] > 0))\} \\
 & \text{Min}\,\{p \mid p : 0 \leq p \leq k \ \wedge \ C(p, k) \ \wedge \ a[k] > 0\} \ \min \ (k+1) \\
= & \quad \{\textbf{assume } a[k] > 0\} \\
 & \text{Min}\,\{p \mid p : 0 \leq p \leq k \ \wedge \ C(p, k)\} \ \min \ (k+1) \\
= & \quad \{\text{Min}\,\{p \mid p : 0 \leq p \leq k \ \wedge \ C(p, k)\} \leq k < k+1\} \\
 & \text{Min}\,\{p \mid p : 0 \leq p \leq k \ \wedge \ C(p, k)\}
\end{array}
$$

LPS: Examining $E(k)$ (1/2)

$$
\begin{array}{ll}
& E(k+1) \\
= & \{\text{definition } E\} \\
& \text{Min}\ \{p \mid p : 0 \le p \le k+1 \ \wedge\ C(p, k+1)\} \\
= & \{\textbf{assume } k \ge 0\text{; split domain: } p \le k \vee p = k+1\text{; use } C(k+1, k+1)\} \\
& \text{Min}\ \{p \mid p : 0 \le p \le k \ \wedge\ C(p, k+1)\}\ \mathrm{min}\ (k+1) \\
= & \{(\forall i \in [p, k+1) : a[i] > 0) \equiv (a[k] > 0 \ \wedge\ (\forall i \in [p, k) : a[i] > 0))\} \\
& \text{Min}\ \{p \mid p : 0 \le p \le k \ \wedge\ C(p, k) \ \wedge\ a[k] > 0\}\ \mathrm{min}\ (k+1) \\
= & \{\textbf{assume } a[k] > 0\} \\
& \text{Min}\ \{p \mid p : 0 \le p \le k \ \wedge\ C(p, k)\}\ \mathrm{min}\ (k+1) \\
= & \{\text{Min}\ \{p \mid p : 0 \le p \le k \ \wedge\ C(p, k)\} \le k < k+1\} \\
& \text{Min}\ \{p \mid p : 0 \le p \le k \ \wedge\ C(p, k)\} \\
= & \{\text{definition } E\} \\
& E(k)
\end{array}
$$

LPS: Examining $E(k)$ (2/2)

LPS: Examining $E(k)$ (2/2)

$$
\begin{array}{ll}
 & E(k+1) \\
= & \{\text{see previous slide}\} \\
 & \text{Min}\ \{p \mid p : 0 \le p \le k\ \wedge\ C(p,k)\ \wedge\ a[k] > 0\}\ \min\ (k+1)
\end{array}
$$

LPS: Examining $E(k)$ (2/2)

$$
\begin{array}{ll}
 & E(k+1) \\
= & \quad \{\text{see previous slide}\} \\
 & \text{Min } \{p \mid p : 0 \leq p \leq k \ \wedge \ C(p,k) \ \wedge \ a[k] > 0\} \ \min \ (k+1) \\
= & \quad \{\textbf{assume } a[k] \leq 0\} \\
 & \text{Min } \{p \mid p : \textbf{false}\} \ \min \ (k+1)
\end{array}
$$

LPS: Examining $E(k)$ (2/2)

$$
\begin{aligned}
& E(k+1) \\
= \quad & \{\text{see previous slide}\} \\
& \text{Min}\, \{p \mid p : 0 \leq p \leq k \ \wedge\ C(p,k) \ \wedge\ a[k] > 0\} \ \min\ (k+1) \\
= \quad & \{\textbf{assume } a[k] \leq 0\} \\
& \text{Min}\, \{p \mid p : \textbf{false}\} \ \min\ (k+1) \\
= \quad & \{\text{Minimum over empty domain is } \infty\} \\
& k+1
\end{aligned}
$$

LPS: Recurrences

For the following definitions

$$
\begin{aligned}
L(k) &= \text{Max}\,\{q - E(q) \mid q : q \leq k\} \\
E(k) &= \text{Min}\,\{p \mid p : 0 \leq p \leq k \;\wedge\; C(p,k)\} \\
C(p,q) &\equiv (\forall i \in [p,q) : a[i] > 0)
\end{aligned}
$$

We found the recurrences:

$$
\begin{aligned}
& & L(0) &= 0 \\
& & E(0) &= 0 \\
k \geq 0 &\Rightarrow & L(k+1) &= L(k) \;\mathrm{max}\; (k+1-E(k+1)) \\
k \geq 0 &\Rightarrow & E(k+1) &= (a[k] > 0 \;?\; E(k) : k+1)
\end{aligned}
$$

LSP: Invariant & Variant

0 We decide that we need a **while**-program.

1 Choose an invariant J and guard B.
Since $Q \equiv z = L(n)$, we want to keep $z = L(k)$ invariant, while we increment k:

$$J : \; z = L(k) \;\wedge\; 0 \leq k \leq n \;\wedge\; y = E(k)$$

Clearly, we choose $B : \; k \neq n$, such that $J \;\wedge\; \neg B \Rightarrow Q$.

LSP: Invariant & Variant

0 We decide that we need a **while**-program.

1 Choose an invariant J and guard B.
Since $Q \equiv z = L(n)$, we want to keep $z = L(k)$ invariant, while we increment k:

$$J : \ z = L(k) \ \wedge \ 0 \leq k \leq n \ \wedge \ y = E(k)$$

Clearly, we choose $B : \ k \neq n$, such that $J \ \wedge \ \neg B \Rightarrow \ Q$.

2 Initialization: The initialization is easy.

$\{P : \ \textbf{true}\}$
(* *base cases recurrences; calculus;* $n \in \mathbb{N}^+$ *)
$\{0 = L(0) \ \wedge \ 0 \leq 0 \leq n \ \wedge \ 0 = E(0)\}$
$z := 0; \ k := 0; \ y := 0;$
$\{J : \ z = L(k) \ \wedge \ 0 \leq k \leq n \ \wedge \ y = E(k)\}$

LSP: Invariant & Variant

0 We decide that we need a **while**-program.

1 Choose an invariant J and guard B.
Since $Q \equiv z = L(n)$, we want to keep $z = L(k)$ invariant, while we increment k:

$$J: \ z = L(k) \ \wedge \ 0 \leq k \leq n \ \wedge \ y = E(k)$$

Clearly, we choose $B: \ k \neq n$, such that $J \ \wedge \ \neg B \Rightarrow Q$.

2 Initialization: The initialization is easy.

$\{P: \ \textbf{true}\}$
 (* *base cases recurrences; calculus;* $n \in \mathbb{N}^+$ *)
$\{0 = L(0) \ \wedge \ 0 \leq 0 \leq n \ \wedge \ 0 = E(0)\}$
$z := 0; \ k := 0; \ y := 0;$
$\{J: \ z = L(k) \ \wedge \ 0 \leq k \leq n \ \wedge \ y = E(k)\}$

3 Variant function: $vf = n - k \in \mathbb{Z}$. Clearly, $J \wedge B \Rightarrow vf \geq 0$.

LPS: Body of the Loop

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

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

LPS: Body of the Loop

$\{J \wedge B \wedge vf = V\}$
(* *definitions* J, B, *and* vf *)
$\{z = L(k) \;\wedge\; 0 \leq k < n \;\wedge\; y = E(k) \;\wedge n - k = V\}$

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

LPS: Body of the Loop

$\{J \wedge B \wedge vf = V\}$
(* *definitions* J, B, *and* vf *)
$\{z = L(k) \ \wedge \ 0 \leq k < n \ \wedge \ y = E(k) \ \wedge n - k = V\}$

$y := (a[k] > 0 \ ? \ y : k + 1);$

$z := z \ \max \ (k + 1 - y);$

$k := k + 1;$

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

LPS: Body of the Loop

$\{J \wedge B \wedge vf = V\}$
(* definitions J, B, and vf *)
$\{z = L(k) \ \wedge\ 0 \leq k < n \ \wedge\ y = E(k) \ \wedge n - k = V\}$
(* recurrence $(a[k] > 0 \; ? \; E(k) : k + 1) = E(k+1)$; substitution *)
$\{z = L(k) \ \wedge\ 0 \leq k < n \ \wedge\ (a[k] > 0 \; ? \; y : k + 1) = E(k+1) \ \wedge n - k = V\}$
$y := (a[k] > 0 \; ? \; y : k + 1);$

$z := z \ \max \ (k + 1 - y);$

$k := k + 1;$

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

LPS: Body of the Loop

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

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

$\{z = L(k) \wedge 0 \le k < n \wedge y = E(k) \wedge n - k = V\}$

(* *recurrence* $(a[k] > 0\ ?\ E(k) : k+1) = E(k+1)$*; substitution* *)

$\{z = L(k) \wedge 0 \le k < n \wedge (a[k] > 0\ ?\ y : k+1) = E(k+1) \wedge n - k = V\}$

$y := (a[k] > 0\ ?\ y : k+1);$

$\{z = L(k) \wedge 0 \le k < n \wedge y = E(k+1) \wedge n - k = V\}$

$z := z\ \max\ (k + 1 - y);$

$k := k + 1;$

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

LPS: Body of the Loop

$\{J \wedge B \wedge vf = V\}$
(* *definitions* J, B, *and* vf *)
$\{z = L(k) \ \wedge \ 0 \leq k < n \ \wedge \ y = E(k) \ \wedge n - k = V\}$
(* *recurrence* $(a[k] > 0 \ ? \ E(k) : k+1) = E(k+1)$; *substitution* *)
$\{z = L(k) \ \wedge \ 0 \leq k < n \ \wedge \ (a[k] > 0 \ ? \ y : k+1) = E(k+1) \ \wedge n - k = V\}$
$y := (a[k] > 0 \ ? \ y : k+1);$
$\{z = L(k) \ \wedge \ 0 \leq k < n \ \wedge y = E(k+1) \ \wedge n - k = V\}$
(* *recurrence* $L(k+1) = L(k) \ \max \ (k+1-E(k+1))$; *substitution* *)
$\{z \ \max \ (k+1-y) = L(k+1) \wedge 0 \leq k < n \wedge y = E(k+1) \wedge n - k = V\}$
$z := z \ \max \ (k+1-y);$

$k := k+1;$

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

LPS: Body of the Loop

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

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

$\{z = L(k) \ \wedge\ 0 \leq k < n \ \wedge\ y = E(k) \ \wedge n - k = V\}$

(* *recurrence* $(a[k] > 0\ ?\ E(k) : k+1) = E(k+1)$; *substitution* *)

$\{z = L(k) \ \wedge\ 0 \leq k < n \ \wedge\ (a[k] > 0\ ?\ y : k+1) = E(k+1) \ \wedge n - k = V\}$

$y := (a[k] > 0\ ?\ y : k+1);$

$\{z = L(k) \ \wedge\ 0 \leq k < n \ \wedge y = E(k+1) \ \wedge n - k = V\}$

(* *recurrence* $L(k+1) = L(k)\ \max\ (k + 1 - E(k+1))$; *substitution* *)

$\{z\ \max\ (k+1-y) = L(k+1) \wedge 0 \leq k < n \wedge y = E(k+1) \wedge n - k = V\}$

$z := z\ \max\ (k+1-y);$

$\{z = L(k+1) \ \wedge\ 0 \leq k < n \ \wedge\ y = E(k+1) \ \wedge\ n - k = V\}$

$k := k + 1;$

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

LPS: Body of the Loop

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

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

$\{z = L(k) \ \wedge \ 0 \leq k < n \ \wedge \ y = E(k) \ \wedge n - k = V\}$

(* *recurrence* $(a[k] > 0 \ ? \ E(k) : k+1) = E(k+1)$*; substitution* *)

$\{z = L(k) \ \wedge \ 0 \leq k < n \ \wedge \ (a[k] > 0 \ ? \ y : k+1) = E(k+1) \ \wedge n - k = V\}$

$y := (a[k] > 0 \ ? \ y : k+1);$

$\{z = L(k) \ \wedge \ 0 \leq k < n \ \wedge y = E(k+1) \ \wedge n - k = V\}$

(* *recurrence* $L(k+1) = L(k) \ \max \ (k+1-E(k+1))$*; substitution* *)

$\{z \ \max \ (k+1-y) = L(k+1) \wedge 0 \leq k < n \wedge y = E(k+1) \wedge n - k = V\}$

$z := z \ \max \ (k+1-y);$

$\{z = L(k+1) \ \wedge \ 0 \leq k < n \ \wedge \ y = E(k+1) \ \wedge \ n - k = V\}$

(* *prepare* $k := k+1$ *)

$\{z = L(k+1) \ \wedge \ 0 \leq k+1 \leq n \ \wedge \ y = E(k+1) \ \wedge \ n - (k+1) < V\}$

$k := k+1;$

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

LPS: Body of the Loop

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

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

$\{z = L(k) \wedge 0 \le k < n \wedge y = E(k) \wedge n - k = V\}$

(* *recurrence* $(a[k] > 0\ ?\ E(k) : k+1) = E(k+1)$; *substitution* *)

$\{z = L(k) \wedge 0 \le k < n \wedge (a[k] > 0\ ?\ y : k+1) = E(k+1) \wedge n - k = V\}$

$y := (a[k] > 0\ ?\ y : k+1);$

$\{z = L(k) \wedge 0 \le k < n \wedge y = E(k+1) \wedge n - k = V\}$

(* *recurrence* $L(k+1) = L(k) \max (k+1 - E(k+1))$; *substitution* *)

$\{z \max (k+1-y) = L(k+1) \wedge 0 \le k < n \wedge y = E(k+1) \wedge n - k = V\}$

$z := z \max (k+1-y);$

$\{z = L(k+1) \wedge 0 \le k < n \wedge y = E(k+1) \wedge n - k = V\}$

(* *prepare* $k := k+1$ *)

$\{z = L(k+1) \wedge 0 \le k+1 \le n \wedge y = E(k+1) \wedge n - (k+1) < V\}$

$k := k+1;$

$\{z = L(k) \wedge 0 \le k \le n \wedge y = E(k) \wedge n - k < V\}$

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

LPS: Body of the Loop

$\{J \wedge B \wedge vf = V\}$
(* *definitions* J, B, *and* vf *)
$\{z = L(k) \wedge 0 \le k < n \wedge y = E(k) \wedge n - k = V\}$
(* *recurrence* $(a[k] > 0 \,?\, E(k) : k+1) = E(k+1)$; *substitution* *)
$\{z = L(k) \wedge 0 \le k < n \wedge (a[k] > 0 \,?\, y : k+1) = E(k+1) \wedge n - k = V\}$
$y := (a[k] > 0 \,?\, y : k+1);$
$\{z = L(k) \wedge 0 \le k < n \wedge y = E(k+1) \wedge n - k = V\}$
(* *recurrence* $L(k+1) = L(k) \max (k+1 - E(k+1))$; *substitution* *)
$\{z \max (k+1-y) = L(k+1) \wedge 0 \le k < n \wedge y = E(k+1) \wedge n - k = V\}$
$z := z \max (k+1-y);$
$\{z = L(k+1) \wedge 0 \le k < n \wedge y = E(k+1) \wedge n - k = V\}$
(* *prepare* $k := k+1$ *)
$\{z = L(k+1) \wedge 0 \le k+1 \le n \wedge y = E(k+1) \wedge n - (k+1) < V\}$
$k := k+1;$
$\{z = L(k) \wedge 0 \le k \le n \wedge y = E(k) \wedge n - k < V\}$
(* *definitions* J, *and* vf *)
$\{J \wedge vf < V\}$

LPS: Conclusion

We derived the program fragment:

const $n : \mathbb{N}^+$, $a :$ **array** $[0..n)$ **of** $\mathbb{Z}$;
var $z, k, y : \mathbb{Z}$;
$\{P : \textbf{true}\}$
$z := 0;\ k := 0;\ y := 0;$
$\{J : z = L(k) \wedge 0 \leq k \leq n \wedge y = E(k)\}$
(* $vf = n - k$ *)
while $k \neq n$ **do**
$y := (a[k] > 0 \ ?\ y : k + 1);$
$z := z \ \max\ (k + 1 - y);$
$k := k + 1;$
end;
$\{Q : z = \text{Max}\,\{q - p \mid p, q : 0 \leq p \leq q \leq n \wedge (\forall i \in [p, q) : a[i] > 0)\}\}$

Outline

Longest positive subsequence (LPS)

Exercise 10.1

Exercise 10.2

Exercise 10.13

Exercises 10.1, 10.2, and 10.3

We now move on to discuss further exercises:

- Exercise 10.1 shows how a careful development of the recurrence relation leads to substantial improvements in time complexity.
- Exercise 10.2 presents clear differences wrt previous exercises, and is arguably the most interesting one.
- Exercise 10.3 involves two different arrays.

Exercise 10.1

Derive a command to compute

$$\Sigma(a[i] \cdot a[j] \cdot a[k] \mid i, j, k : 0 \leq i < j \leq k < n)$$

Exercise 10.1

Derive a command to compute

$$\Sigma(a[i] \cdot a[j] \cdot a[k] \mid i, j, k : 0 \le i < j \le k < n)$$

Formally, find a command C that satisfies the specification:

const $n :\ \mathbb{N}^+,\ a :$ **array** $[0..n)$ **of** $\mathbb{Z}$;
var $s :\ \mathbb{Z}$;
$\{P :$ **true**$\}$
C
$\{Q :\ s = \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i, j, k : 0 \le i < j \le k < n)\}$

Exercise 10.1: Naive Solution

$$
\begin{array}{l}
\textbf{const } n : \mathbb{N}^+,\ a : \textbf{ array } [0..n) \textbf{ of } \mathbb{Z};\\
\textbf{var } \ i, j, k, s : \mathbb{Z};\\
\quad \{P : \textbf{ true}\}\\
s := 0;\ i := 0;\\
\textbf{while } i < n - 1 \textbf{ do}\\
\quad j := i + 1;\\
\quad \textbf{while } j < n \textbf{ do}\\
\quad\quad k := j;\\
\quad\quad \textbf{while } k < n \textbf{ do}\\
\quad\quad\quad s := s + a[i] * a[j] * a[k];\\
\quad\quad\quad k := k + 1;\\
\quad\quad \textbf{end};\\
\quad\quad j := j + 1;\\
\quad \textbf{end};\\
\quad i := i + 1;\\
\textbf{end};\\
\quad \{Q : \ s = \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i, j, k : 0 \le i < j \le k < n)\}
\end{array}
$$

Time complexity is $O(n^3)$. We can do better!

Exercise 10.1: Guard & First Invariant

We start by introducing

$$S(x) = \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i, j, k : 0 \leq i < j \leq k < x)$$

We can rewrite the postcondition: $Q: \ s = S(n)$

Exercise 10.1: Guard & First Invariant

We start by introducing

$$S(x) = \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i, j, k : 0 \leq i < j \leq k < x)$$

We can rewrite the postcondition: $Q: \ s = S(n)$

0 We decide that we need a **while**-program.

1 Choose an invariant J and guard B.
As a first attempt we introduce a variable x and try to maintain

$$\boxed{J : s = S(x) \ \wedge \ 1 \leq x \leq n}$$

Clearly, we choose $B: \ x \neq n$, such that $J \ \wedge \ \neg B \Rightarrow \ Q$.

Exercise 10.1: Guard & First Invariant

We start by introducing

$$S(x) = \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i, j, k : 0 \leq i < j \leq k < x)$$

We can rewrite the postcondition: $Q: \ s = S(n)$

0 We decide that we need a **while**-program.

1 Choose an invariant J and guard B.
As a first attempt we introduce a variable x and try to maintain

$$\boxed{J : s = S(x) \ \wedge \ 1 \leq x \leq n}$$

Clearly, we choose $B: \ x \neq n$, such that $J \ \wedge \ \neg B \Rightarrow \ Q$.

We will examine the definition of $S(x)$ to strengthen J.

Exercise 10.1: Examining $S(x)$

The loop will proceed by incrementing x, so we first have a look at $S(x+1)$:

$$
\begin{array}{ll}
& S(x+1) \\
= & \quad \{\text{definition } S\} \\
& \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i, j, k : 0 \leq i < j \leq k < x+1)
\end{array}
$$

Exercise 10.1: Examining $S(x)$

The loop will proceed by incrementing x, so we first have a look at $S(x+1)$:

$$
\begin{array}{cl}
& S(x+1) \\
= & \quad \{\text{definition } S\} \\
& \Sigma(a[i]\cdot a[j]\cdot a[k] \mid i,j,k : 0 \le i < j \le k < x+1) \\
= & \quad \{\textbf{assume } x \ge 1\text{; split domain: } k < x \vee k = x\} \\
& \Sigma(a[i]\cdot a[j]\cdot a[k] \mid i,j,k : 0 \le i < j \le k < x) \\
& + \\
& \Sigma(a[i]\cdot a[j]\cdot a[x] \mid i,j : 0 \le i < j \le x)
\end{array}
$$

Exercise 10.1: Examining $S(x)$

The loop will proceed by incrementing x, so we first have a look at $S(x+1)$:

$$
\begin{array}{ll}
& S(x+1) \\
= & \quad \{\text{definition } S\} \\
& \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i,j,k : 0 \leq i < j \leq k < x+1) \\
= & \quad \{\textbf{assume } x \geq 1\text{; split domain: } k < x \vee k = x\} \\
& \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i,j,k : 0 \leq i < j \leq k < x) \\
& + \\
& \Sigma(a[i] \cdot a[j] \cdot a[x] \mid i,j : 0 \leq i < j \leq x) \\
= & \quad \{\text{definition } S \text{ and calculus}\} \\
& S(x) + a[x] \cdot \Sigma(a[i] \cdot a[j] \mid i,j : 0 \leq i < j \leq x)
\end{array}
$$

Exercise 10.1: Examining $S(x)$

The loop will proceed by incrementing x, so we first have a look at $S(x+1)$:

$$
\begin{array}{ll}
 & S(x+1) \\
= & \{\text{definition } S\} \\
 & \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i,j,k : 0 \le i < j \le k < x+1) \\
= & \{\textbf{assume } x \ge 1\text{; split domain: } k < x \vee k = x\} \\
 & \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i,j,k : 0 \le i < j \le k < x) \\
 & + \\
 & \Sigma(a[i] \cdot a[j] \cdot a[x] \mid i,j : 0 \le i < j \le x) \\
= & \{\text{definition } S \text{ and calculus}\} \\
 & S(x) + a[x] \cdot \Sigma(a[i] \cdot a[j] \mid i,j : 0 \le i < j \le x) \\
= & \{\text{we prefer half-open intervals}\} \\
 & S(x) + a[x] \cdot \Sigma(a[i] \cdot a[j] \mid i,j : 0 \le i < j < x+1)
\end{array}
$$

Exercise 10.1: Examining $S(x)$

The loop will proceed by incrementing x, so we first have a look at $S(x+1)$:

$$
\begin{array}{ll}
 & S(x+1) \\
= & \quad \{\text{definition } S\} \\
 & \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i,j,k : 0 \le i < j \le k < x+1) \\
= & \quad \{\textbf{assume } x \ge 1\text{; split domain: } k < x \vee k = x\} \\
 & \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i,j,k : 0 \le i < j \le k < x) \\
 & + \\
 & \Sigma(a[i] \cdot a[j] \cdot a[x] \mid i,j : 0 \le i < j \le x) \\
= & \quad \{\text{definition } S \text{ and calculus}\} \\
 & S(x) + a[x] \cdot \Sigma(a[i] \cdot a[j] \mid i,j : 0 \le i < j \le x) \\
= & \quad \{\text{we prefer half-open intervals}\} \\
 & S(x) + a[x] \cdot \Sigma(a[i] \cdot a[j] \mid i,j : 0 \le i < j < x+1) \\
= & \quad \{\textbf{introduce } T\} \\
 & S(x) + a[x] \cdot T(x+1) \quad \text{where } T(x) = \Sigma(a[i] \cdot a[j] \mid i,j : 0 \le i < j < x)
\end{array}
$$

So, if we want to increment x, we need $T(x+1)$.

Exercise 10.1: Examining $T(x+1)$

$$
\begin{array}{ll}
 & T(x+1) \\
= & \quad \{\text{definition } T\} \\
 & \Sigma(a[i]\cdot a[j] \mid i,j : 0 \leq i < j < x+1)
\end{array}
$$

Exercise 10.1: Examining $T(x+1)$

$$
\begin{array}{ll}
& T(x+1) \\
= & \quad \{\text{definition } T\} \\
& \Sigma(a[i] \cdot a[j] \mid i, j : 0 \leq i < j < x+1) \\
= & \quad \{\textbf{assume } x \geq 1\text{; split domain: } j < x \vee j = x\} \\
& \Sigma(a[i] \cdot a[j] \mid i, j, k : 0 \leq i < j < x) \ + \ \Sigma(a[i] \cdot a[x] \mid i : 0 \leq i < x)
\end{array}
$$

Exercise 10.1: Examining $T(x+1)$

$$
\begin{array}{ll}
 & T(x+1) \\
= & \quad \{\text{definition } T\} \\
 & \Sigma(a[i]\cdot a[j] \mid i,j : 0 \le i < j < x+1) \\
= & \quad \{\textbf{assume } x \ge 1\text{; split domain: } j < x \vee j = x\} \\
 & \Sigma(a[i]\cdot a[j] \mid i,j,k : 0 \le i < j < x) \;+\; \Sigma(a[i]\cdot a[x] \mid i : 0 \le i < x) \\
= & \quad \{\text{definition } T\text{; calculus}\} \\
 & T(x) \;+\; a[x]\cdot\Sigma(a[i] \mid i : 0 \le i < x)
\end{array}
$$

Exercise 10.1: Examining $T(x+1)$

$$
\begin{array}{ll}
& T(x+1) \\
= & \quad \{\text{definition } T\} \\
& \Sigma(a[i]\cdot a[j] \mid i,j : 0 \le i < j < x+1) \\
= & \quad \{\textbf{assume } x \ge 1\text{; split domain: } j < x \vee j = x\} \\
& \Sigma(a[i]\cdot a[j] \mid i,j,k : 0 \le i < j < x) \ + \ \Sigma(a[i]\cdot a[x] \mid i : 0 \le i < x) \\
= & \quad \{\text{definition } T\text{; calculus}\} \\
& T(x) \ + \ a[x]\cdot\Sigma(a[i] \mid i : 0 \le i < x) \\
= & \quad \{\textbf{introduce } U\} \\
& T(x) + a[x]\cdot U(x) \quad \text{where } U(x) = \Sigma(a[i] \mid i : 0 \le i < x)
\end{array}
$$

Exercise 10.1: Examining $T(x+1)$

$$
\begin{array}{ll}
& T(x+1) \\
= & \quad \{\text{definition } T\} \\
& \Sigma(a[i] \cdot a[j] \mid i,j : 0 \le i < j < x+1) \\
= & \quad \{\textbf{assume } x \ge 1\text{; split domain: } j < x \vee j = x\} \\
& \Sigma(a[i] \cdot a[j] \mid i,j,k : 0 \le i < j < x) \ + \ \Sigma(a[i] \cdot a[x] \mid i : 0 \le i < x) \\
= & \quad \{\text{definition } T\text{; calculus}\} \\
& T(x) \ + \ a[x] \cdot \Sigma(a[i] \mid i : 0 \le i < x) \\
= & \quad \{\textbf{introduce } U\} \\
& T(x) + a[x] \cdot U(x) \quad \text{where } U(x) = \Sigma(a[i] \mid i : 0 \le i < x)
\end{array}
$$

We also have a look at $U(x+1)$:

$$
\begin{array}{ll}
& U(x+1) \\
= & \quad \{\text{definition } U\} \\
& \Sigma(a[i] \mid i : 0 \le i < x+1)
\end{array}
$$

Exercise 10.1: Examining $T(x+1)$

$$
\begin{array}{rl}
& T(x+1) \\
= & \quad \{\text{definition } T\} \\
& \Sigma(a[i] \cdot a[j] \mid i,j : 0 \leq i < j < x+1) \\
= & \quad \{\textbf{assume } x \geq 1\text{; split domain: } j < x \vee j = x\} \\
& \Sigma(a[i] \cdot a[j] \mid i,j,k : 0 \leq i < j < x) \;+\; \Sigma(a[i] \cdot a[x] \mid i : 0 \leq i < x) \\
= & \quad \{\text{definition } T\text{; calculus}\} \\
& T(x) \;+\; a[x] \cdot \Sigma(a[i] \mid i : 0 \leq i < x) \\
= & \quad \{\textbf{introduce } U\} \\
& T(x) + a[x] \cdot U(x) \quad \text{where } U(x) = \Sigma(a[i] \mid i : 0 \leq i < x)
\end{array}
$$

We also have a look at $U(x+1)$:

$$
\begin{array}{rl}
& U(x+1) \\
= & \quad \{\text{definition } U\} \\
& \Sigma(a[i] \mid i : 0 \leq i < x+1) \\
= & \quad \{\textbf{assume } x \geq 0\text{; split domain: } i < x \vee i = x\} \\
& \Sigma(a[i] \mid i : 0 \leq i < x) \;+\; a[x]
\end{array}
$$

Exercise 10.1: Examining $T(x+1)$

$$
\begin{array}{ll}
& T(x+1) \\
= & \{\text{definition } T\} \\
& \Sigma(a[i] \cdot a[j] \mid i, j : 0 \leq i < j < x+1) \\
= & \{\textbf{assume } x \geq 1\text{; split domain: } j < x \vee j = x\} \\
& \Sigma(a[i] \cdot a[j] \mid i, j, k : 0 \leq i < j < x) \; + \; \Sigma(a[i] \cdot a[x] \mid i : 0 \leq i < x) \\
= & \{\text{definition } T\text{; calculus}\} \\
& T(x) \; + \; a[x] \cdot \Sigma(a[i] \mid i : 0 \leq i < x) \\
= & \{\textbf{introduce } U\} \\
& T(x) + a[x] \cdot U(x) \quad \text{where } U(x) = \Sigma(a[i] \mid i : 0 \leq i < x)
\end{array}
$$

We also have a look at $U(x+1)$:

$$
\begin{array}{ll}
& U(x+1) \\
= & \{\text{definition } U\} \\
& \Sigma(a[i] \mid i : 0 \leq i < x+1) \\
= & \{\textbf{assume } x \geq 0\text{; split domain: } i < x \vee i = x\} \\
& \Sigma(a[i] \mid i : 0 \leq i < x) \; + \; a[x] \\
= & \{\text{definition } U\} \\
& U(x) \; + \; a[x]
\end{array}
$$

Exercise 10.1: Recurrences

Summing up, we started from

$$S(x) = \Sigma(a[i] \cdot a[j] \cdot a[k] \mid 0 \leq i < j \leq k < x)$$

and expressed it in terms of

$$\begin{aligned} T(x) &= \ \Sigma(a[i] \cdot a[j] \mid i, j : 0 \leq i < j < x) \\ U(x) &= \ \Sigma(a[i] \mid i : 0 \leq i < x) \end{aligned}$$

Exercise 10.1: Recurrences

Summing up, we started from

$$S(x) = \Sigma(a[i] \cdot a[j] \cdot a[k] \mid 0 \le i < j \le k < x)$$

and expressed it in terms of

$$\begin{aligned} T(x) &= \Sigma(a[i] \cdot a[j] \mid i, j : 0 \le i < j < x) \\ U(x) &= \Sigma(a[i] \mid i : 0 \le i < x) \end{aligned}$$

We found the recurrences:

$$\begin{aligned}
x < 1 \Rightarrow \quad && S(x) &= 0 \\
x \ge 1 \Rightarrow \quad && S(x+1) &= S(x) + a[x] \cdot T(x+1) \\
x < 1 \Rightarrow \quad && T(x) &= 0 \\
x \ge 1 \Rightarrow \quad && T(x+1) &= T(x) + a[x] \cdot U(x) \\
x \le 0 \Rightarrow \quad && U(x) &= 0 \\
x \ge 1 \Rightarrow \quad && U(x+1) &= a[x] + U(x)
\end{aligned}$$

Exercise 10.1: Invariant & Variant

$$S(x) = \Sigma(a[i] \cdot a[j] \cdot a[k] \mid 0 \leq i < j \leq k < x)$$
$$T(x) = \Sigma(a[i] \cdot a[j] \mid i, j : 0 \leq i < j < x)$$
$$U(x) = \Sigma(a[i] \mid i : 0 \leq i < x)$$

2 Initialization:

$$B : x \neq n$$
$$J : s = S(x) \ \wedge \ 1 \leq x \leq n$$

Exercise 10.1: Invariant & Variant

$$S(x) = \Sigma(a[i] \cdot a[j] \cdot a[k] \mid 0 \leq i < j \leq k < x)$$
$$T(x) = \Sigma(a[i] \cdot a[j] \mid i, j : 0 \leq i < j < x)$$
$$U(x) = \Sigma(a[i] \mid i : 0 \leq i < x)$$

2 Initialization: We now strengthen the invariant and initialize it.

$$B : x \neq n$$
$$J : s = S(x) \wedge t = T(x) \wedge u = U(x) \wedge 1 \leq x \leq n$$

Exercise 10.1: Invariant & Variant

$$S(x) = \Sigma(a[i] \cdot a[j] \cdot a[k] \mid 0 \leq i < j \leq k < x)$$
$$T(x) = \Sigma(a[i] \cdot a[j] \mid i, j : 0 \leq i < j < x)$$
$$U(x) = \Sigma(a[i] \mid i : 0 \leq i < x)$$

2 Initialization: We now strengthen the invariant and initialize it.

$$B : x \neq n$$
$$J : s = S(x) \land t = T(x) \land u = U(x) \land 1 \leq x \leq n$$

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

$\{J : s = S(x) \land t = T(x) \land u = U(x) \land 1 \leq x \leq n\}$

Exercise 10.1: Invariant & Variant

$$S(x) = \Sigma(a[i] \cdot a[j] \cdot a[k] \mid 0 \leq i < j \leq k < x)$$
$$T(x) = \Sigma(a[i] \cdot a[j] \mid i, j : 0 \leq i < j < x)$$
$$U(x) = \Sigma(a[i] \mid i : 0 \leq i < x)$$

2 Initialization: We now strengthen the invariant and initialize it.

$$B : x \neq n$$
$$J : s = S(x) \wedge t = T(x) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x \leq n$$

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

$x := 1; \ s := 0; \ t := 0; \ u := a[0];$

$\{J : \ s = S(x) \ \wedge \ t = T(x) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x \leq n\}$

Exercise 10.1: Invariant & Variant

$$S(x) = \Sigma(a[i] \cdot a[j] \cdot a[k] \mid 0 \leq i < j \leq k < x)$$
$$T(x) = \Sigma(a[i] \cdot a[j] \mid i, j : 0 \leq i < j < x)$$
$$U(x) = \Sigma(a[i] \mid i : 0 \leq i < x)$$

2 Initialization: We now strengthen the invariant and initialize it.

$$B : x \neq n$$
$$J : s = S(x) \wedge t = T(x) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x \leq n$$

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

$\{0 = S(1) \ \wedge \ 0 = T(1) \ \wedge \ a[0] = U(1) \ \wedge \ 1 \leq 1 \leq n\}$
$x := 1; \ s := 0; \ t := 0; \ u := a[0];$
$\{J : \ s = S(x) \ \wedge \ t = T(x) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x \leq n\}$

Exercise 10.1: Invariant & Variant

$$S(x) = \Sigma(a[i] \cdot a[j] \cdot a[k] \mid 0 \leq i < j \leq k < x)$$
$$T(x) = \Sigma(a[i] \cdot a[j] \mid i, j : 0 \leq i < j < x)$$
$$U(x) = \Sigma(a[i] \mid i : 0 \leq i < x)$$

2 Initialization: We now strengthen the invariant and initialize it.

$$B : x \neq n$$
$$J : s = S(x) \wedge t = T(x) \wedge u = U(x) \wedge 1 \leq x \leq n$$

$\{P :$ **true**$\}$
(* *base cases recurrences;* $n \in \mathbb{N}^+$ *)
$\{0 = S(1) \wedge 0 = T(1) \wedge 1 \leq 1 \leq n\}$
(* $U(1) = a[0] + U(0) = a[0]$ *)
$\{0 = S(1) \wedge 0 = T(1) \wedge a[0] = U(1) \wedge 1 \leq 1 \leq n\}$
$x := 1;\ s := 0;\ t := 0;\ u := a[0];$
$\{J : s = S(x) \wedge t = T(x) \wedge u = U(x) \wedge 1 \leq x \leq n\}$

Exercise 10.1: Invariant & Variant

$$S(x) = \Sigma(a[i] \cdot a[j] \cdot a[k] \mid 0 \leq i < j \leq k < x)$$
$$T(x) = \Sigma(a[i] \cdot a[j] \mid i, j : 0 \leq i < j < x)$$
$$U(x) = \Sigma(a[i] \mid i : 0 \leq i < x)$$

2 Initialization: We now strengthen the invariant and initialize it.

$$B : x \neq n$$
$$J : s = S(x) \wedge t = T(x) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x \leq n$$

$\{P : \ \textbf{true}\}$
(* *base cases recurrences;* $n \in \mathbb{N}^+$ *)
$\{0 = S(1) \ \wedge \ 0 = T(1) \ \wedge \ 1 \leq 1 \leq n\}$
(* $U(1) = a[0] + U(0) = a[0]$ *)
$\{0 = S(1) \ \wedge \ 0 = T(1) \ \wedge \ a[0] = U(1) \ \wedge \ 1 \leq 1 \leq n\}$
$x := 1;\ s := 0;\ t := 0;\ u := a[0];$
$\{J : \ s = S(x) \ \wedge \ t = T(x) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x \leq n\}$

3 Variant function: $vf = n - x \in \mathbb{Z}$. Then $J \wedge B \Rightarrow vf \geq 0$.

Exercise 10.1: Body of the Loop

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

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

Exercise 10.1: Body of the Loop

$\{J \ \wedge \ B \ \wedge \ vf = V\}$
(* *definitions* J, B, *and* vf *)
$\{s = S(x) \ \wedge \ t = T(x) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$

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

Exercise 10.1: Body of the Loop

$\{J \ \wedge \ B \ \wedge \ vf = V\}$
  (* *definitions* J, B, *and* vf *)
$\{s = S(x) \ \wedge \ t = T(x) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$

$t := t + a[x] * u;$

$s := s + a[x] * t;$

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

$x := x + 1;$

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

Exercise 10.1: Body of the Loop

$\{J \ \wedge \ B \ \wedge \ vf = V\}$
  (* definitions J, B, and vf *)
$\{s = S(x) \ \wedge \ t = T(x) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
  (* recurrence $T(x+1) = T(x) + a[x] \cdot U(x)$; substitution; logic *)
$\{s = S(x) \ \wedge \ t + a[x] \cdot u = T(x+1) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
$t := t + a[x] * u;$

$s := s + a[x] * t;$

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

$x := x + 1;$

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

Exercise 10.1: Body of the Loop

$\{J \ \wedge \ B \ \wedge \ vf = V\}$
(* definitions J, B, and vf *)
$\{s = S(x) \ \wedge \ t = T(x) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
(* recurrence $T(x+1) = T(x) + a[x] \cdot U(x)$; substitution; logic *)
$\{s = S(x) \ \wedge \ t + a[x] \cdot u = T(x+1) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
$t := t + a[x] * u;$
$\{s = S(x) \ \wedge \ t = T(x+1) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$

$s := s + a[x] * t;$

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

$x := x + 1;$

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

Exercise 10.1: Body of the Loop

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

(* definitions J, B, and vf *)

$\{s = S(x) \ \wedge \ t = T(x) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$

(* recurrence $T(x+1) = T(x) + a[x] \cdot U(x)$; substitution; logic *)

$\{s = S(x) \ \wedge \ t + a[x] \cdot u = T(x+1) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$

$t := t + a[x] * u;$

$\{s = S(x) \ \wedge \ t = T(x+1) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$

(* recurrence $S(x+1) = S(x) + a[x] \cdot T(x+1)$; substitution *)

$\{s + a[x] \cdot t = S(x+1) \wedge t = T(x+1) \wedge u = U(x) \wedge 1 \leq x < n \wedge n - x = V\}$

$s := s + a[x] * t;$

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

$x := x + 1;$

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

Exercise 10.1: Body of the Loop

$\{J \ \wedge \ B \ \wedge \ vf = V\}$
(* definitions J, B, and vf *)
$\{s = S(x) \ \wedge \ t = T(x) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
(* recurrence $T(x+1) = T(x) + a[x] \cdot U(x)$; substitution; logic *)
$\{s = S(x) \ \wedge \ t + a[x] \cdot u = T(x+1) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
$t := t + a[x] * u;$
$\{s = S(x) \ \wedge \ t = T(x+1) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
(* recurrence $S(x+1) = S(x) + a[x] \cdot T(x+1)$; substitution *)
$\{s + a[x] \cdot t = S(x+1) \wedge t = T(x+1) \wedge u = U(x) \wedge 1 \leq x < n \wedge n - x = V\}$
$s := s + a[x] * t;$
$\{s = S(x+1) \ \wedge \ t = T(x+1) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$

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

$x := x + 1;$

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

Exercise 10.1: Body of the Loop

$\{J \ \wedge \ B \ \wedge \ vf = V\}$
(* definitions J, B, and vf *)
$\{s = S(x) \ \wedge \ t = T(x) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
(* recurrence $T(x+1) = T(x) + a[x] \cdot U(x)$; substitution; logic *)
$\{s = S(x) \ \wedge \ t + a[x] \cdot u = T(x+1) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
$t := t + a[x] * u;$
$\{s = S(x) \ \wedge \ t = T(x+1) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
(* recurrence $S(x+1) = S(x) + a[x] \cdot T(x+1)$; substitution *)
$\{s + a[x] \cdot t = S(x+1) \wedge t = T(x+1) \wedge u = U(x) \wedge 1 \leq x < n \wedge n - x = V\}$
$s := s + a[x] * t;$
$\{s = S(x+1) \ \wedge \ t = T(x+1) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
(* recurrence $U(x+1) = U(x) + a[x]$ *)
$\{s = S(x+1) \wedge t = T(x+1) \wedge u + a[x] = U(x+1) \wedge 1 \leq x < n \wedge n - x = V\}$
$u := u + a[x];$

$x := x + 1;$

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

Exercise 10.1: Body of the Loop

$\{J \;\wedge\; B \;\wedge\; vf = V\}$
(* definitions J, B, and vf *)
$\{s = S(x) \;\wedge\; t = T(x) \;\wedge\; u = U(x) \;\wedge\; 1 \leq x < n \;\wedge\; n - x = V\}$
(* recurrence $T(x+1) = T(x) + a[x] \cdot U(x)$; substitution; logic *)
$\{s = S(x) \;\wedge\; t + a[x] \cdot u = T(x+1) \;\wedge\; u = U(x) \;\wedge\; 1 \leq x < n \;\wedge\; n - x = V\}$
$t := t + a[x] * u;$
$\{s = S(x) \;\wedge\; t = T(x+1) \;\wedge\; u = U(x) \;\wedge\; 1 \leq x < n \;\wedge\; n - x = V\}$
(* recurrence $S(x+1) = S(x) + a[x] \cdot T(x+1)$; substitution *)
$\{s + a[x] \cdot t = S(x+1) \wedge t = T(x+1) \wedge u = U(x) \wedge 1 \leq x < n \wedge n - x = V\}$
$s := s + a[x] * t;$
$\{s = S(x+1) \;\wedge\; t = T(x+1) \;\wedge\; u = U(x) \;\wedge\; 1 \leq x < n \;\wedge\; n - x = V\}$
(* recurrence $U(x+1) = U(x) + a[x]$ *)
$\{s = S(x+1) \wedge t = T(x+1) \wedge u + a[x] = U(x+1) \wedge 1 \leq x < n \wedge n - x = V\}$
$u := u + a[x];$
$\{s = S(x+1) \;\wedge\; t = T(x+1) \;\wedge\; u = U(x+1) \;\wedge\; 1 \leq x < n \;\wedge\; n - x = V\}$

$x := x + 1;$

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

Exercise 10.1: Body of the Loop

$\{J \ \wedge \ B \ \wedge \ vf = V\}$
  (* definitions J, B, and vf *)
$\{s = S(x) \ \wedge \ t = T(x) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
  (* recurrence $T(x+1) = T(x) + a[x] \cdot U(x)$; substitution; logic *)
$\{s = S(x) \ \wedge \ t + a[x] \cdot u = T(x+1) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
$t := t + a[x] * u;$
$\{s = S(x) \ \wedge \ t = T(x+1) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
  (* recurrence $S(x+1) = S(x) + a[x] \cdot T(x+1)$; substitution *)
$\{s + a[x] \cdot t = S(x+1) \wedge t = T(x+1) \wedge u = U(x) \wedge 1 \leq x < n \wedge n - x = V\}$
$s := s + a[x] * t;$
$\{s = S(x+1) \ \wedge \ t = T(x+1) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
  (* recurrence $U(x+1) = U(x) + a[x]$ *)
$\{s = S(x+1) \wedge t = T(x+1) \wedge u + a[x] = U(x+1) \wedge 1 \leq x < n \wedge n - x = V\}$
$u := u + a[x];$
$\{s = S(x+1) \ \wedge \ t = T(x+1) \ \wedge \ u = U(x+1) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
  (* prepare $x := x + 1$ *)
$\{s = S(x+1) \wedge t = T(x+1) \wedge u = U(x+1) \wedge 1 \leq x+1 \leq n \wedge n - (x+1) < V\}$
$x := x + 1;$

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

Exercise 10.1: Body of the Loop

$\{J \ \wedge \ B \ \wedge \ vf = V\}$
(* definitions J, B, and vf *)
$\{s = S(x) \ \wedge \ t = T(x) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
(* recurrence $T(x+1) = T(x) + a[x] \cdot U(x)$; substitution; logic *)
$\{s = S(x) \ \wedge \ t + a[x] \cdot u = T(x+1) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
$t := t + a[x] * u;$
$\{s = S(x) \ \wedge \ t = T(x+1) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
(* recurrence $S(x+1) = S(x) + a[x] \cdot T(x+1)$; substitution *)
$\{s + a[x] \cdot t = S(x+1) \wedge t = T(x+1) \wedge u = U(x) \wedge 1 \leq x < n \wedge n - x = V\}$
$s := s + a[x] * t;$
$\{s = S(x+1) \ \wedge \ t = T(x+1) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
(* recurrence $U(x+1) = U(x) + a[x]$ *)
$\{s = S(x+1) \wedge t = T(x+1) \wedge u + a[x] = U(x+1) \wedge 1 \leq x < n \wedge n - x = V\}$
$u := u + a[x];$
$\{s = S(x+1) \ \wedge \ t = T(x+1) \ \wedge \ u = U(x+1) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
(* prepare $x := x + 1$ *)
$\{s = S(x+1) \wedge t = T(x+1) \wedge u = U(x+1) \wedge 1 \leq x + 1 \leq n \wedge n - (x+1) < V\}$
$x := x + 1;$
$\{s = S(x) \ \wedge \ t = T(x) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x \leq n \ \wedge \ n - x < V\}$

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

Exercise 10.1: Body of the Loop

$\{J \ \wedge \ B \ \wedge \ vf = V\}$
(* definitions J, B, and vf *)
$\{s = S(x) \ \wedge \ t = T(x) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
(* recurrence $T(x+1) = T(x) + a[x] \cdot U(x)$; substitution; logic *)
$\{s = S(x) \ \wedge \ t + a[x] \cdot u = T(x+1) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
$t := t + a[x] * u;$
$\{s = S(x) \ \wedge \ t = T(x+1) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
(* recurrence $S(x+1) = S(x) + a[x] \cdot T(x+1)$; substitution *)
$\{s + a[x] \cdot t = S(x+1) \wedge t = T(x+1) \wedge u = U(x) \wedge 1 \leq x < n \wedge n - x = V\}$
$s := s + a[x] * t;$
$\{s = S(x+1) \ \wedge \ t = T(x+1) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
(* recurrence $U(x+1) = U(x) + a[x]$ *)
$\{s = S(x+1) \wedge t = T(x+1) \wedge u + a[x] = U(x+1) \wedge 1 \leq x < n \wedge n - x = V\}$
$u := u + a[x];$
$\{s = S(x+1) \ \wedge \ t = T(x+1) \ \wedge \ u = U(x+1) \ \wedge \ 1 \leq x < n \ \wedge \ n - x = V\}$
(* prepare $x := x + 1$ *)
$\{s = S(x+1) \wedge t = T(x+1) \wedge u = U(x+1) \wedge 1 \leq x + 1 \leq n \wedge n - (x+1) < V\}$
$x := x + 1;$
$\{s = S(x) \ \wedge \ t = T(x) \ \wedge \ u = U(x) \ \wedge \ 1 \leq x \leq n \ \wedge \ n - x < V\}$
(* definitions J, and vf *)
$\{J \ \wedge \ vf < V\}$

Exercise 10.1: Conclusion

$$
\begin{array}{l}
\textbf{const } n:\ \mathbb{N}^+,\ \ a:\ \textbf{array } [0..n) \textbf{ of } \mathbb{Z};\\
\textbf{var } \ x, s, t, u:\ \mathbb{Z};\\
\quad \{P:\ \textbf{true}\}\\
s := 0;\ \ t := 0;\ \ u := a[0];\ \ x := 1;\\
\quad \{J:\ \ s = S(x)\ \wedge\ t = T(x)\ \wedge\ u = U(x)\ \wedge\ 1 \leq x \leq n\}\\
\qquad (^*\ vf = n - x\ ^*)\\
\textbf{while } x < n \textbf{ do}\\
\quad t := t + a[x] * u;\\
\quad s := s + a[x] * t;\\
\quad u := u + a[x];\\
\quad x := x + 1;\\
\textbf{end};\\
\quad \{Q:\ \ s = \Sigma(a[i]\cdot a[j]\cdot a[k] \mid i, j, k : 0 \leq i < j \leq k < n)\}
\end{array}
$$

Complexity is $O(n)$: a major improvement over the $O(n^3)$ algorithm.

Outline

Exercise 10.2

Derive a command to compute

$$\Sigma(a[i] \cdot a[j] \cdot a[k] \mid i, j, k \ : \ 0 \leq i \leq j < n \ \wedge \ i \leq k < n)$$

Exercise 10.2

Derive a command to compute

$$\Sigma(a[i] \cdot a[j] \cdot a[k] \mid i, j, k \ : \ 0 \leq i \leq j < n \ \wedge \ i \leq k < n)$$

We start by introducing:

$$L(x) = \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i, j, k \ : \ x \leq i \leq j < n \ \wedge \ i \leq k < n)$$

Note the x in the lower bound!

We want to find a command C that satisfies the specification:

const $n : \mathbb{N}^+, \ a : $ **array** $[0..n)$ **of** $\mathbb{Z}$;
var $s : \mathbb{Z}$;
  $\{P : \textbf{true}\}$
C
  $\{Q : s = L(0)\}$

Exercise 10.2: Guard & First Invariant

$$P : \textbf{true}$$
$$Q : s = L(0)$$
$$L(x) = \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i, j, k : x \leq i \leq j < n \ \wedge \ i \leq k < n)$$

0 We decide that we need a **while**-program.

1 Choose an invariant J and guard B.
As a first attempt we introduce a variable x and try to maintain

$$J : \ s = L(x) \ \wedge \ 0 \leq x \leq n$$

Clearly, we choose $B : \ x \neq 0$, such that $J \ \wedge \ \neg B \Rightarrow \ Q$.

As before, we can safely add conjuncts to J.

Exercise 10.2: Examining $L(x)$

The loop will decrement x, so we first examine $L(x-1)$, for $x > 0$.

$$
\begin{array}{ll}
 & L(x-1) \\
= & \quad \{\text{definition } L\} \\
 & \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i, j, k : x-1 \le i \le j < n \ \wedge \ i \le k < n)
\end{array}
$$

Exercise 10.2: Examining $L(x)$

The loop will decrement x, so we first examine $L(x-1)$, for $x > 0$.

$$
\begin{array}{ll}
& L(x-1) \\
= & \quad \{\text{definition } L\} \\
& \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i, j, k : x-1 \leq i \leq j < n \ \wedge \ i \leq k < n) \\
= & \quad \{\text{split domain: } x \leq i \vee i = x-1\} \\
& \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i, j, k : x \leq i \leq j < n \ \wedge \ i \leq k < n) + \\
& \Sigma(a[x-1] \cdot a[j] \cdot a[k] \mid j, k : x-1 \leq j < n \ \wedge \ x-1 \leq k < n)
\end{array}
$$

Exercise 10.2: Examining $L(x)$

The loop will decrement x, so we first examine $L(x-1)$, for $x > 0$.

$$
\begin{array}{cl}
& L(x-1) \\
= & \quad \{\text{definition } L\} \\
& \Sigma(a[i]\cdot a[j]\cdot a[k] \mid i,j,k : x-1 \le i \le j < n \ \wedge \ i \le k < n) \\
= & \quad \{\text{split domain: } x \le i \vee i = x-1\} \\
& \Sigma(a[i]\cdot a[j]\cdot a[k] \mid i,j,k : x \le i \le j < n \ \wedge \ i \le k < n) + \\
& \Sigma(a[x-1]\cdot a[j]\cdot a[k] \mid j,k : x-1 \le j < n \ \wedge \ x-1 \le k < n) \\
= & \quad \{\text{definition } L\text{; calculus}\} \\
& L(x) + a[x-1]\cdot \\
& \qquad\qquad \Sigma(a[j]\cdot a[k] \mid j,k : x-1 \le j < n \ \wedge \ x-1 \le k < n)
\end{array}
$$

Exercise 10.2: Examining $L(x)$

The loop will decrement x, so we first examine $L(x-1)$, for $x > 0$.

$$
\begin{array}{ll}
& L(x-1) \\
= & \{\text{definition } L\} \\
& \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i,j,k : x-1 \leq i \leq j < n \ \wedge \ i \leq k < n) \\
= & \{\text{split domain: } x \leq i \vee i = x-1\} \\
& \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i,j,k : x \leq i \leq j < n \ \wedge \ i \leq k < n) + \\
& \Sigma(a[x-1] \cdot a[j] \cdot a[k] \mid j,k : x-1 \leq j < n \ \wedge \ x-1 \leq k < n) \\
= & \{\text{definition } L\text{; calculus}\} \\
& L(x) + a[x-1] \cdot \\
& \qquad\qquad \Sigma(a[j] \cdot a[k] \mid j,k : x-1 \leq j < n \ \wedge \ x-1 \leq k < n) \\
= & \{\textbf{introduce } T\} \\
& L(x) + a[x-1] \cdot T(x-1)
\end{array}
$$

where $T(x) = \Sigma(a[j] \cdot a[k] \mid j,k : x \leq j < n \ \wedge \ x \leq k < n)$.

Exercise 10.2: Examining $T(x)$

$$\boxed{T(x) = \Sigma(a[j] \cdot a[k] \mid j, k : x \leq j < n \ \wedge \ x \leq k < n)}$$

So, if we want to decrement x, we need $T(x-1)$ for $x > 0$:

$T(x-1)$

Exercise 10.2: Examining $T(x)$

$$\boxed{T(x) = \Sigma(a[j] \cdot a[k] \mid j, k : x \leq j < n \ \wedge \ x \leq k < n)}$$

So, if we want to decrement x, we need $T(x-1)$ for $x > 0$:

$$
\begin{array}{ll}
 & T(x-1) \\
= & \quad \{\text{definition } T\} \\
 & \Sigma(a[j] \cdot a[k] \mid j, k : x-1 \leq j < n \ \wedge \ x-1 \leq k < n)
\end{array}
$$

Exercise 10.2: Examining $T(x)$

$$T(x) = \Sigma(\, a[j] \cdot a[k] \mid j, k : x \le j < n \;\wedge\; x \le k < n)$$

So, if we want to decrement x, we need $T(x-1)$ for $x > 0$:

$$\begin{array}{ll}
 & T(x-1) \\
= & \quad \{\text{definition } T\} \\
 & \Sigma(\, a[j] \cdot a[k] \mid j, k : x-1 \le j < n \;\wedge\; x-1 \le k < n) \\
= & \quad \{\text{split domain: } x \le j \vee j = x-1\} \\
 & \Sigma(\, a[j] \cdot a[k] \mid j, k : x \le j < n \;\wedge\; x-1 \le k < n) \;+ \\
 & \Sigma(\, a[x-1] \cdot a[k] \mid k : x-1 \le k < n)
\end{array}$$

Exercise 10.2: Examining $T(x)$

$$T(x) = \Sigma(a[j] \cdot a[k] \mid j,k : x \le j < n \ \wedge \ x \le k < n)$$

So, if we want to decrement x, we need $T(x-1)$ for $x > 0$:

$$\begin{array}{ll}
 & T(x-1) \\
= & \quad \{\text{definition } T\} \\
 & \Sigma(a[j] \cdot a[k] \mid j,k : x-1 \le j < n \ \wedge \ x-1 \le k < n) \\
= & \quad \{\text{split domain: } x \le j \vee j = x-1\} \\
 & \Sigma(a[j] \cdot a[k] \mid j,k : x \le j < n \ \wedge \ x-1 \le k < n) + \\
 & \Sigma(a[x-1] \cdot a[k] \mid k : x-1 \le k < n) \\
= & \quad \{\text{split domain of 1st term: } k = x \le k \vee k = x-1\} \\
 & \Sigma(a[j] \cdot a[k] \mid j,k : x \le j < n \ \wedge \ x \le k < n) + \\
 & \Sigma(a[j] \cdot a[x-1] \mid j : x \le j < n) + \\
 & \Sigma(a[x-1] \cdot a[k] \mid k : x-1 \le k < n)
\end{array}$$

Exercise 10.2: Examining $T(x)$

$$\boxed{T(x) = \Sigma(a[j] \cdot a[k] \mid j,k : x \leq j < n \ \wedge \ x \leq k < n)}$$

So, if we want to decrement x, we need $T(x-1)$ for $x > 0$:

$$\begin{array}{cl}
 & T(x-1) \\
= & \quad \{\text{definition } T\} \\
 & \Sigma(a[j] \cdot a[k] \mid j,k : x-1 \leq j < n \ \wedge \ x-1 \leq k < n) \\
= & \quad \{\text{split domain: } x \leq j \vee j = x-1\} \\
 & \Sigma(a[j] \cdot a[k] \mid j,k : x \leq j < n \ \wedge \ x-1 \leq k < n) + \\
 & \Sigma(a[x-1] \cdot a[k] \mid k : x-1 \leq k < n) \\
= & \quad \{\text{split domain of 1st term: } k = x \leq k \vee k = x-1\} \\
 & \Sigma(a[j] \cdot a[k] \mid j,k : x \leq j < n \ \wedge \ x \leq k < n) + \\
 & \Sigma(a[j] \cdot a[x-1] \mid j : x \leq j < n) + \\
 & \Sigma(a[x-1] \cdot a[k] \mid k : x-1 \leq k < n) \\
= & \quad \{\text{definition } T\text{; calculus}\} \\
 & T(x) \ + \ a[x-1] \cdot \big(\Sigma(a[k] \mid k : x-1 \leq k < n) \ + \Sigma(a[j] \mid j : x \leq j < n)\big)
\end{array}$$

Exercise 10.2: Examining $T(x)$

$$T(x) = \Sigma(a[j] \cdot a[k] \mid j, k : x \le j < n \ \wedge \ x \le k < n)$$

So, if we want to decrement x, we need $T(x-1)$ for $x > 0$:

$$
\begin{array}{cl}
 & T(x-1) \\
= & \{\text{definition } T\} \\
 & \Sigma(a[j] \cdot a[k] \mid j, k : x-1 \le j < n \ \wedge \ x-1 \le k < n) \\
= & \{\text{split domain: } x \le j \vee j = x-1\} \\
 & \Sigma(a[j] \cdot a[k] \mid j, k : x \le j < n \ \wedge \ x-1 \le k < n) + \\
 & \Sigma(a[x-1] \cdot a[k] \mid k : x-1 \le k < n) \\
= & \{\text{split domain of 1st term: } k = x \le k \vee k = x-1\} \\
 & \Sigma(a[j] \cdot a[k] \mid j, k : x \le j < n \ \wedge \ x \le k < n) + \\
 & \Sigma(a[j] \cdot a[x-1] \mid j : x \le j < n) + \\
 & \Sigma(a[x-1] \cdot a[k] \mid k : x-1 \le k < n) \\
= & \{\text{definition } T\text{; calculus}\} \\
 & T(x) \ + \ a[x-1] \cdot \big(\Sigma(a[k] \mid k : x-1 \le k < n) \ + \Sigma(a[j] \mid j : x \le j < n)\big) \\
= & \{\text{rename bound variable: } k \rightsquigarrow j\} \\
 & T(x) \ + \ a[x-1] \cdot \big(\Sigma(a[j] \mid j : x-1 \le j < n) \ + \Sigma(a[j] \mid j : x \le j < n)\big)
\end{array}
$$

Exercise 10.2: Examining $T(x)$

$$\boxed{T(x) = \Sigma(a[j] \cdot a[k] \mid j,k : x \le j < n \ \wedge \ x \le k < n)}$$

So, if we want to decrement x, we need $T(x-1)$ for $x > 0$:

$$
\begin{array}{ll}
 & T(x-1) \\
= & \quad \{\text{definition } T\} \\
 & \Sigma(a[j] \cdot a[k] \mid j,k : x-1 \le j < n \ \wedge \ x-1 \le k < n) \\
= & \quad \{\text{split domain: } x \le j \vee j = x-1\} \\
 & \Sigma(a[j] \cdot a[k] \mid j,k : x \le j < n \ \wedge \ x-1 \le k < n) + \\
 & \Sigma(a[x-1] \cdot a[k] \mid k : x-1 \le k < n) \\
= & \quad \{\text{split domain of 1st term: } k = x \le k \vee k = x-1\} \\
 & \Sigma(a[j] \cdot a[k] \mid j,k : x \le j < n \ \wedge \ x \le k < n) + \\
 & \Sigma(a[j] \cdot a[x-1] \mid j : x \le j < n) + \\
 & \Sigma(a[x-1] \cdot a[k] \mid k : x-1 \le k < n) \\
= & \quad \{\text{definition } T\text{; calculus}\} \\
 & T(x) \ + \ a[x-1] \cdot \big(\Sigma(a[k] \mid k : x-1 \le k < n) \ + \Sigma(a[j] \mid j : x \le j < n)\big) \\
= & \quad \{\text{rename bound variable: } k \rightsquigarrow j\} \\
 & T(x) \ + \ a[x-1] \cdot \big(\Sigma(a[j] \mid j : x-1 \le j < n) \ + \Sigma(a[j] \mid j : x \le j < n)\big) \\
= & \quad \{\textbf{introduce } U(x) = \Sigma(a[i] \mid i : x \le i < n)\} \\
 & T(x) + a[x-1] \cdot (U(x-1) + U(x))
\end{array}
$$

Exercise 10.2: Examining $U(x)$

$$\boxed{U(x) = \Sigma(a[i] \mid i : x \leq i < n)}$$

We now look into $U(x-1)$, for $x > 0$:

$$U(x-1)$$

Exercise 10.2: Examining $U(x)$

$$\boxed{U(x) = \Sigma(a[i] \mid i : x \leq i < n)}$$

We now look into $U(x-1)$, for $x > 0$:

$$\begin{array}{ll} & U(x-1) \\ = & \quad \{\text{definition } U\} \\ & \Sigma(a[i] \mid i : x-1 \leq i < n) \end{array}$$

Exercise 10.2: Examining $U(x)$

$$\boxed{U(x) = \Sigma(a[i] \mid i : x \leq i < n)}$$

We now look into $U(x-1)$, for $x > 0$:

$$
\begin{array}{ll}
 & U(x-1) \\
= & \quad \{\text{definition } U\} \\
 & \Sigma(a[i] \mid i : x-1 \leq i < n) \\
= & \quad \{\text{split domain: } x \leq i \vee i = x-1\} \\
 & \Sigma(a[i] \mid i : x \leq i < n) \ + \ a[x-1]
\end{array}
$$

Exercise 10.2: Examining $U(x)$

$$\boxed{U(x) = \Sigma(a[i] \mid i : x \leq i < n)}$$

We now look into $U(x-1)$, for $x > 0$:

$$
\begin{array}{ll}
 & U(x-1) \\
= & \quad \{\text{definition } U\} \\
 & \Sigma(a[i] \mid i : x-1 \leq i < n) \\
= & \quad \{\text{split domain: } x \leq i \vee i = x-1\} \\
 & \Sigma(a[i] \mid i : x \leq i < n) \ + \ a[x-1] \\
= & \quad \{\text{definition } U\} \\
 & U(x) \ + \ a[x-1]
\end{array}
$$

Exercise 10.2: Recurrences

Summing up, for the following definitions

$$
\begin{array}{rcl}
L(x) & = & \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i, j, k : x \leq i \leq j < n \ \wedge \ i \leq k < n) \\
T(x) & = & \Sigma(a[j] \cdot a[k] \mid j, k : x \leq j < n \ \wedge \ x \leq k < n) \\
U(x) & = & \Sigma(a[i] \mid i : x \leq i < n)
\end{array}
$$

We found the recurrences:

$$
\begin{array}{rcl}
x = n & \Rightarrow & L(x) = T(x) = U(x) = 0 \\
x > 0 & \Rightarrow & L(x-1) = L(x) + a[x-1] \cdot T(x-1) \\
x > 0 & \Rightarrow & T(x-1) = T(x) + a[x-1] \cdot (U(x-1) + U(x)) \\
x > 0 & \Rightarrow & U(x-1) = a[x-1] + U(x)
\end{array}
$$

Exercise 10.2: Invariant & Variant

2 Initialization:

$$\boxed{\begin{aligned} B &: x \neq 0 \\ J &: s = L(x) \;\wedge\; 0 \leq x \leq n \end{aligned}}$$

Exercise 10.2: Invariant & Variant

2 Initialization: We now strengthen the invariant and initialize it.

$$B : x \neq 0$$

$$J : s = L(x) \wedge t = T(x) \wedge u = U(x) \wedge 0 \leq x \leq n$$

Exercise 10.2: Invariant & Variant

2 Initialization: We now strengthen the invariant and initialize it.

$$B : x \neq 0$$
$$J : s = L(x) \wedge t = T(x) \wedge u = U(x) \wedge 0 \leq x \leq n$$

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

$\{J : s = L(x) \wedge t = T(x) \wedge u = U(x) \wedge 0 \leq x \leq n\}$

Exercise 10.2: Invariant & Variant

2 Initialization: We now strengthen the invariant and initialize it.

$$B : x \neq 0$$
$$J : s = L(x) \wedge t = T(x) \wedge u = U(x) \wedge 0 \leq x \leq n$$

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

$s := 0;\ t := 0;\ u := 0;\ x := n;$
$\{J :\ s = L(x) \wedge t = T(x) \wedge u = U(x) \wedge 0 \leq x \leq n\}$

Exercise 10.2: Invariant & Variant

2 Initialization: We now strengthen the invariant and initialize it.

$$B : x \neq 0$$
$$J : s = L(x) \wedge t = T(x) \wedge u = U(x) \wedge 0 \leq x \leq n$$

$\{P: \textbf{true}\}$
(* *base cases recurrences; calculus;* $n \in \mathbb{N}^+$ *)
$\{0 = L(n) \wedge 0 = T(n) \wedge 0 = U(n) \wedge 0 \leq n \leq n\}$
$s := 0;\ t := 0;\ u := 0;\ x := n;$
$\{J: s = L(x) \wedge t = T(x) \wedge u = U(x) \wedge 0 \leq x \leq n\}$

Exercise 10.2: Invariant & Variant

2 Initialization: We now strengthen the invariant and initialize it.

$$\boxed{\begin{array}{l} B : x \neq 0 \\ J : s = L(x) \wedge t = T(x) \wedge u = U(x) \wedge 0 \leq x \leq n \end{array}}$$

$$\begin{array}{l} \quad \{P : \textbf{true}\} \\ \qquad (^{*}\ \textit{base cases recurrences; calculus; } n \in \mathbb{N}^{+}\ ^{*}) \\ \quad \{0 = L(n) \wedge 0 = T(n) \wedge 0 = U(n) \wedge 0 \leq n \leq n\} \\ s := 0;\ t := 0;\ u := 0;\ x := n; \\ \quad \{J : s = L(x) \wedge t = T(x) \wedge u = U(x) \wedge 0 \leq x \leq n\} \end{array}$$

3 Variant function: $vf = x \in \mathbb{Z}$. Clearly, $J \wedge B \Rightarrow vf \geq 0$.

Exercise 10.2: Body of The Loop (1/2)

$\{J \wedge B \ \wedge \ vf = V\}$
(* *definitions* J, B, *and* vf ; *logic* *)
$\{s = L(x) \ \wedge \ \underline{t = T(x)} \ \wedge \ u = U(x) \ \wedge \ 0 < x = V \leq n\}$

Exercise 10.2: Body of The Loop (1/2)

$\{J \wedge B \ \wedge \ vf = V\}$
(* *definitions* J, B, *and* vf; *logic* *)
$\{s = L(x) \ \wedge \ \underline{t = T(x)} \ \wedge \ u = U(x) \ \wedge \ 0 < x = V \leq n\}$
(* *recurrence* $T(x-1) = T(x) + a[x-1] \cdot (U(x-1) + U(x))$; *substitution* *)
$\{s = L(x) \ \wedge \ \underline{t + a[x-1] \cdot (U(x-1) + u) = T(x-1)} \wedge u = U(x) \wedge ....\}$

Exercise 10.2: Body of The Loop (1/2)

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

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

$\{s = L(x) \ \wedge \ \underline{t = T(x)} \ \wedge \ u = U(x) \ \wedge \ 0 < x = V \leq n\}$

  (* *recurrence* $T(x-1) = T(x) + a[x-1] \cdot (U(x-1) + U(x))$; *substitution* *)

$\{s = L(x) \ \wedge \ \underline{t + a[x-1] \cdot (U(x-1) + u) = T(x-1)} \wedge u = U(x) \wedge ....\}$

  (* *calculus* *)

$\{s = L(x) \ \wedge \ t + \underline{a[x-1] \cdot u + a[x-1] \cdot U(x-1) = T(x-1)} \wedge ....\}$

Exercise 10.2: Body of The Loop (1/2)

$\{J \wedge B \ \wedge \ vf = V\}$
(* definitions J, B, and vf; logic *)
$\{s = L(x) \ \wedge \ \underline{t = T(x)} \ \wedge \ u = U(x) \ \wedge \ 0 < x = V \leq n\}$
(* recurrence $T(x-1) = T(x) + a[x-1] \cdot (U(x-1) + U(x))$; substitution *)
$\{s = L(x) \ \wedge \ \underline{t + a[x-1] \cdot (U(x-1) + u) = T(x-1)} \wedge u = U(x) \wedge ....\}$
(* calculus *)
$\{s = L(x) \ \wedge \ t + \underline{a[x-1] \cdot u + a[x-1] \cdot U(x-1) = T(x-1)} \wedge ....\}$
$t := t + a[x-1] * u;$
$\{s = L(x) \ \wedge \ t + \underline{a[x-1] \cdot U(x-1) = T(x-1)} \ \wedge \ \underline{u = U(x)} \ \wedge \ 0 < x = V \leq n\}$

Exercise 10.2: Body of The Loop (1/2)

$\{J \wedge B \ \wedge \ vf = V\}$
  (* *definitions* J, B, *and* vf; *logic* *)
$\{s = L(x) \ \wedge \ \underline{t = T(x)} \ \wedge \ u = U(x) \ \wedge \ 0 < x = V \leq n\}$
  (* *recurrence* $T(x-1) = T(x) + a[x-1] \cdot (U(x-1) + U(x))$; *substitution* *)
$\{s = L(x) \ \wedge \ \underline{t + a[x-1] \cdot (U(x-1) + u) = T(x-1)} \wedge u = U(x) \wedge ....\}$
  (* *calculus* *)
$\{s = L(x) \ \wedge \ t + \underline{a[x-1] \cdot u + a[x-1] \cdot U(x-1) = T(x-1)} \wedge ....\}$
$t := t + a[x-1] * u;$
$\{s = L(x) \ \wedge \ t + \underline{a[x-1] \cdot U(x-1) = T(x-1)} \ \wedge \ \underline{u = U(x)} \ \wedge \ 0 < x = V \leq n\}$
  (* *recurrence* $U(x-1) = U(x) + a[x-1]$ *)
$\{s = L(x) \ \wedge \ t + a[x-1] \cdot U(x-1) = T(x-1) \ \wedge \ \underline{u + a[x-1] = U(x-1)} \ \wedge \ ....\}$

Exercise 10.2: Body of The Loop (1/2)

$\{J \wedge B \ \wedge \ vf = V\}$
  (* *definitions* J, B, *and* vf*; logic* *)
$\{s = L(x) \ \wedge \ \underline{t = T(x)} \ \wedge \ u = U(x) \ \wedge \ 0 < x = V \leq n\}$
  (* *recurrence* $T(x-1) = T(x) + a[x-1] \cdot (U(x-1) + U(x))$*; substitution* *)
$\{s = L(x) \ \wedge \ \underline{t + a[x-1] \cdot (U(x-1) + u) = T(x-1)} \wedge u = U(x) \wedge ....\}$
  (* *calculus* *)
$\{s = L(x) \ \wedge \ t + \underline{a[x-1] \cdot u + a[x-1] \cdot U(x-1) = T(x-1)} \wedge ....\}$
$t := t + a[x-1] * u;$
$\{s = L(x) \ \wedge \ t + \underline{a[x-1] \cdot U(x-1) = T(x-1)} \ \wedge \ \underline{u = U(x)} \ \wedge \ 0 < x = V \leq n\}$
  (* *recurrence* $U(x-1) = U(x) + a[x-1]$ *)
$\{s = L(x) \ \wedge \ t + a[x-1] \cdot U(x-1) = T(x-1) \ \wedge \ \underline{u + a[x-1] = U(x-1)} \ \wedge \ ....\}$
$u := u + a[x-1];$
$\{s = L(x) \wedge t + a[x-1] \cdot U(x-1) = T(x-1) \ \wedge \ \underline{u = U(x-1)} \ \wedge \ldots\}$
  (* *substitution* *)
$\{s = L(x) \ \wedge \ \underline{t + a[x-1] \cdot u} = T(x-1) \ \wedge \ u = U(x-1) \ \wedge \ 0 < x = V \leq n\}$

Exercise 10.2: Body of The Loop (1/2)

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

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

$\{s = L(x) \ \wedge \ \underline{t = T(x)} \ \wedge \ u = U(x) \ \wedge \ 0 < x = V \leq n\}$

(* *recurrence* $T(x-1) = T(x) + a[x-1] \cdot (U(x-1) + U(x))$; *substitution* *)

$\{s = L(x) \ \wedge \ \underline{t + a[x-1] \cdot (U(x-1) + u) = T(x-1)} \wedge u = U(x) \wedge \ldots.\}$

(* *calculus* *)

$\{s = L(x) \ \wedge \ t + \underline{a[x-1] \cdot u + a[x-1] \cdot U(x-1) = T(x-1)} \wedge \ldots.\}$

$t := t + a[x-1] * u;$

$\{s = L(x) \ \wedge \ t + \underline{a[x-1] \cdot U(x-1) = T(x-1)} \ \wedge \ \underline{u = U(x)} \ \wedge \ 0 < x = V \leq n\}$

(* *recurrence* $U(x-1) = U(x) + a[x-1]$ *)

$\{s = L(x) \ \wedge \ t + a[x-1] \cdot U(x-1) = T(x-1) \ \wedge \ \underline{u + a[x-1] = U(x-1)} \ \wedge \ \ldots.\}$

$u := u + a[x-1];$

$\{s = L(x) \wedge t + a[x-1] \cdot U(x-1) = T(x-1) \ \wedge \ \underline{u = U(x-1)} \ \wedge \ldots\}$

(* *substitution* *)

$\{s = L(x) \ \wedge \ \underline{t + a[x-1] \cdot u} = T(x-1) \ \wedge \ u = U(x-1) \ \wedge \ 0 < x = V \leq n\}$

$t := t + a[x-1] * u;$

$\{s = L(x) \ \wedge \ \underline{t = T(x-1)} \ \wedge \ u = U(x-1) \wedge 0 < x = V \leq n\}$

Exercise 10.2: Body of The Loop (2/2)

$$\{s = L(x) \ \wedge \ t = T(x-1) \ \wedge \ u = U(x-1) \ \wedge \ 0 < x = V \leq n\}$$

Exercise 10.2: Body of The Loop (2/2)

$\{s = L(x) \ \wedge\ t = T(x-1) \ \wedge\ u = U(x-1) \ \wedge\ 0 < x = V \leq n\}$
(* *recurrence* $L(x-1) = L(x) + a[x-1] \cdot T(x-1)$; *substitution* *)
$\{\underline{s + a[x-1] \cdot t = L(x-1)} \ \wedge\ t = T(x-1) \ \wedge\ u = U(x-1) \ \wedge\ 0 < x = V \leq n\}$

Exercise 10.2: Body of The Loop (2/2)

$\{s = L(x) \ \wedge\ t = T(x-1) \ \wedge\ u = U(x-1) \ \wedge\ 0 < x = V \leq n\}$

(* *recurrence* $L(x-1) = L(x) + a[x-1] \cdot T(x-1)$*; substitution* *)

$\{\underline{s + a[x-1] \cdot t = L(x-1)} \ \wedge\ t = T(x-1) \ \wedge\ u = U(x-1) \ \wedge\ 0 < x = V \leq n\}$

$s := s + a[x-1] * t;$

$\underline{\{s = L(x-1)} \ \wedge\ t = T(x-1) \ \wedge\ u = U(x-1) \ \wedge\ 0 < x = V \leq n\}$

Exercise 10.2: Body of The Loop (2/2)

$\{s = L(x) \ \wedge\ t = T(x-1) \ \wedge\ u = U(x-1) \ \wedge\ 0 < x = V \leq n\}$

(* *recurrence* $L(x-1) = L(x) + a[x-1] \cdot T(x-1)$; *substitution* *)

$\{\underline{s + a[x-1] \cdot t = L(x-1)} \ \wedge\ t = T(x-1) \ \wedge\ u = U(x-1) \ \wedge\ 0 < x = V \leq n\}$

$s := s + a[x-1] * t;$

$\underline{\{s = L(x-1)} \ \wedge\ t = T(x-1) \ \wedge\ u = U(x-1) \ \wedge\ 0 < x = V \leq n\}$

(* *calculus* *)

$\{s = L(x-1) \ \wedge\ t = T(x-1) \ \wedge\ u = U(x-1) \ \wedge\ \underline{0 \leq x-1 \leq n \ \wedge\ x-1 < V}\}$

Exercise 10.2: Body of The Loop (2/2)

$$\{s = L(x) \ \wedge\ t = T(x-1) \ \wedge\ u = U(x-1) \ \wedge\ 0 < x = V \leq n\}$$

(* *recurrence* $L(x-1) = L(x) + a[x-1] \cdot T(x-1)$*; substitution* *)

$$\{\underline{s + a[x-1] \cdot t = L(x-1)} \ \wedge\ t = T(x-1) \ \wedge\ u = U(x-1) \ \wedge\ 0 < x = V \leq n\}$$

$s := s + a[x-1] * t;$

$$\{\underline{s = L(x-1)} \ \wedge\ t = T(x-1) \ \wedge\ u = U(x-1) \ \wedge\ 0 < x = V \leq n\}$$

(* *calculus* *)

$$\{s = L(x-1) \ \wedge\ t = T(x-1) \ \wedge\ u = U(x-1) \ \wedge\ \underline{0 \leq x-1 \leq n \ \wedge\ x-1 < V}\}$$

$x := x - 1;$

$$\{s = L(x) \ \wedge\ t = T(x) \ \wedge\ u = U(x) \ \wedge\ 0 \leq x \leq n \ \wedge\ x < V\}$$

Exercise 10.2: Body of The Loop (2/2)

$\{s = L(x) \ \wedge\ t = T(x-1) \ \wedge\ u = U(x-1) \ \wedge\ 0 < x = V \leq n\}$

(* recurrence $L(x-1) = L(x) + a[x-1] \cdot T(x-1)$; substitution *)

$\{\underline{s + a[x-1] \cdot t = L(x-1)} \ \wedge\ t = T(x-1) \ \wedge\ u = U(x-1) \ \wedge\ 0 < x = V \leq n\}$

$s := s + a[x-1] * t;$

$\underline{\{s = L(x-1)} \ \wedge\ t = T(x-1) \ \wedge\ u = U(x-1) \ \wedge\ 0 < x = V \leq n\}$

(* calculus *)

$\{s = L(x-1) \ \wedge\ t = T(x-1) \ \wedge\ u = U(x-1) \ \wedge\ \underline{0 \leq x-1 \leq n \ \wedge\ x-1 < V}\}$

$x := x - 1;$

$\{s = L(x) \ \wedge\ t = T(x) \ \wedge\ u = U(x) \ \wedge\ 0 \leq x \leq n \ \wedge\ x < V\}$

(* definitions J, and vf *)

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

Exercise 10.2: Conclusion

We derived the program fragment:

$$
\begin{array}{l}
\textbf{const } n : \mathbb{N}^+,\ a : \textbf{array } [0..n) \textbf{ of } \mathbb{Z};\\
\textbf{var } x, s, t, u : \mathbb{Z};\\
\quad \{P : \textbf{true}\}\\
s := 0;\ t := 0;\ u := 0;\ x := n;\\
\quad \{J : s = L(x) \wedge t = T(x) \wedge u = U(x) \wedge 0 \le x \le n\}\\
\qquad (^*\ vf = x\ ^*)\\
\textbf{while } x \neq 0 \textbf{ do}\\
\quad t := t + a[x-1] * u;\\
\quad u := u + a[x-1];\\
\quad t := t + a[x-1] * u;\\
\quad s := s + a[x-1] * t;\\
\quad x := x - 1;\\
\textbf{end};\\
\quad \{Q : s = \Sigma(a[i] \cdot a[j] \cdot a[k] \mid i, j, k : 0 \le i \le j < n \wedge i \le k < n)\}
\end{array}
$$

Outline

Exercise 10.13

Given are two arrays declared in

$$\textbf{const } n : \mathbb{N}, \quad a, b \;:\; \textbf{array } [0..n) \textbf{ of } \mathbb{R};$$

Determine a command S to compute

$$\Sigma(\, a[i] \cdot b[j] \mid i, j :\; 0 \leq j \leq i < n)$$

The time complexity of S should be $O(n)$. First derive recurrence relations for relevant functions and give a formal specification.

Exercise 10.13

Given are two arrays declared in

$$\textbf{const } n : \mathbb{N}, \quad a, b \ : \ \textbf{array } [0..n) \textbf{ of } \mathbb{R};$$

Determine a command S to compute

$$\Sigma(a[i] \cdot b[j] \mid i, j : \ 0 \le j \le i < n)$$

The time complexity of S should be $O(n)$. First derive recurrence relations for relevant functions and give a formal specification.

We introduce $S(k) = \Sigma(a[i] \cdot b[j] \mid i, j : \ 0 \le j \le i < k)$. We want a command that satisfies:

const $n : \mathbb{N}, \quad a, b \ : \$ **array** $[0..n)$ **of** $\mathbb{R}$;
 var $x : \ \mathbb{Z}$;
 $\{P : \ \textbf{true}\}$
 S;
 $\{Q : \ x = S(n)\}$

Exercise 10.13: Examining $S(x)$

$$\boxed{S(k) = \Sigma(a[i] \cdot b[j] \mid i, j :\ 0 \leq j \leq i < k)}$$

Clearly, $0 = S(0)$.

We need to increment k. We examine $S(k+1)$, for $k < n$:

$S(k+1)$

Exercise 10.13: Examining $S(x)$

$$\boxed{S(k) = \Sigma(a[i] \cdot b[j] \mid i, j :\ 0 \leq j \leq i < k)}$$

Clearly, $0 = S(0)$.

We need to increment k. We examine $S(k+1)$, for $k < n$:

$$\begin{aligned}
& S(k+1) \\
= \quad & \{\text{definition } S\} \\
& \Sigma(a[i] \cdot b[j] \mid i, j :\ 0 \leq j \leq i < k+1)
\end{aligned}$$

Exercise 10.13: Examining $S(x)$

$$\boxed{S(k) = \Sigma(a[i] \cdot b[j] \mid i, j : \ 0 \le j \le i < k)}$$

Clearly, $0 = S(0)$.

We need to increment k. We examine $S(k+1)$, for $k < n$:

$$\begin{array}{ll} & S(k+1) \\ = & \quad \{\text{definition } S\} \\ & \Sigma(a[i] \cdot b[j] \mid i, j : \ 0 \le j \le i < k+1) \\ = & \quad \{\text{split domain: } i < k \vee i = k\} \end{array}$$

Exercise 10.13: Examining $S(x)$

$$\boxed{S(k) = \Sigma(a[i] \cdot b[j] \mid i, j :\ 0 \leq j \leq i < k)}$$

Clearly, $0 = S(0)$.

We need to increment k. We examine $S(k+1)$, for $k < n$:

$$
\begin{array}{ll}
 & S(k+1) \\
= & \{\text{definition } S\} \\
 & \Sigma(a[i] \cdot b[j] \mid i, j :\ 0 \leq j \leq i < k+1) \\
= & \{\text{split domain: } i < k \vee i = k\} \\
 & \Sigma(a[i] \cdot b[j] \mid i, j :\ 0 \leq j \leq i < k) + \Sigma(a[k] \cdot b[j] \mid j :\ 0 \leq j \leq k)
\end{array}
$$

Exercise 10.13: Examining $S(x)$

$$\boxed{S(k) = \Sigma(\, a[i] \cdot b[j] \mid i, j :\ 0 \le j \le i < k)}$$

Clearly, $0 = S(0)$.

We need to increment k. We examine $S(k+1)$, for $k < n$:

$$
\begin{array}{ll}
& S(k+1) \\
= & \{\text{definition } S\} \\
& \Sigma(\, a[i] \cdot b[j] \mid i, j :\ 0 \le j \le i < k+1) \\
= & \{\text{split domain: } i < k \vee i = k\} \\
& \Sigma(\, a[i] \cdot b[j] \mid i, j :\ 0 \le j \le i < k) + \Sigma(\, a[k] \cdot b[j] \mid j :\ 0 \le j \le k) \\
= & \{\text{definition } S\text{; calculus}\}
\end{array}
$$

Exercise 10.13: Examining $S(x)$

$$\boxed{S(k) = \Sigma(a[i] \cdot b[j] \mid i,j :\ 0 \leq j \leq i < k)}$$

Clearly, $0 = S(0)$.

We need to increment k. We examine $S(k+1)$, for $k < n$:

$$\begin{array}{ll}
& S(k+1) \\
= & \quad \{\text{definition } S\} \\
& \Sigma(a[i] \cdot b[j] \mid i,j :\ 0 \leq j \leq i < k+1) \\
= & \quad \{\text{split domain: } i < k \lor i = k\} \\
& \Sigma(a[i] \cdot b[j] \mid i,j :\ 0 \leq j \leq i < k) + \Sigma(a[k] \cdot b[j] \mid j :\ 0 \leq j \leq k) \\
= & \quad \{\text{definition } S\text{; calculus}\} \\
& S(k) + a[k] \cdot \Sigma(b[j] \mid j :\ 0 \leq j \leq k)
\end{array}$$

Exercise 10.13: Examining $S(x)$

$$\boxed{S(k) = \Sigma(a[i] \cdot b[j] \mid i, j :\ 0 \le j \le i < k)}$$

Clearly, $0 = S(0)$.

We need to increment k. We examine $S(k+1)$, for $k < n$:

$$
\begin{array}{ll}
 & S(k+1) \\
= & \quad \{\text{definition } S\} \\
 & \Sigma(a[i] \cdot b[j] \mid i, j :\ 0 \le j \le i < k+1) \\
= & \quad \{\text{split domain: } i < k \vee i = k\} \\
 & \Sigma(a[i] \cdot b[j] \mid i, j :\ 0 \le j \le i < k) + \Sigma(a[k] \cdot b[j] \mid j :\ 0 \le j \le k) \\
= & \quad \{\text{definition } S\text{; calculus}\} \\
 & S(k) + a[k] \cdot \Sigma(b[j] \mid j :\ 0 \le j \le k) \\
= & \quad \{\text{use half-open intervals}\}
\end{array}
$$

Exercise 10.13: Examining $S(x)$

$$\boxed{S(k) = \Sigma(a[i] \cdot b[j] \mid i, j:\ 0 \le j \le i < k)}$$

Clearly, $0 = S(0)$.

We need to increment k. We examine $S(k+1)$, for $k < n$:

$$
\begin{array}{ll}
 & S(k+1) \\
= & \quad \{\text{definition } S\} \\
 & \Sigma(a[i] \cdot b[j] \mid i, j:\ 0 \le j \le i < k+1) \\
= & \quad \{\text{split domain: } i < k \vee i = k\} \\
 & \Sigma(a[i] \cdot b[j] \mid i, j:\ 0 \le j \le i < k) + \Sigma(a[k] \cdot b[j] \mid j:\ 0 \le j \le k) \\
= & \quad \{\text{definition } S\text{; calculus}\} \\
 & S(k) + a[k] \cdot \Sigma(b[j] \mid j:\ 0 \le j \le k) \\
= & \quad \{\text{use half-open intervals}\} \\
 & S(k) + a[k] \cdot \Sigma(b[j] \mid j:\ 0 \le j < k+1)
\end{array}
$$

Exercise 10.13: Examining $S(x)$

$$\boxed{S(k) = \Sigma(a[i] \cdot b[j] \mid i, j :\ 0 \leq j \leq i < k)}$$

Clearly, $0 = S(0)$.

We need to increment k. We examine $S(k+1)$, for $k < n$:

$$
\begin{array}{ll}
& S(k+1) \\
= & \{\text{definition } S\} \\
& \Sigma(a[i] \cdot b[j] \mid i, j :\ 0 \leq j \leq i < k+1) \\
= & \{\text{split domain: } i < k \vee i = k\} \\
& \Sigma(a[i] \cdot b[j] \mid i, j :\ 0 \leq j \leq i < k) + \Sigma(a[k] \cdot b[j] \mid j :\ 0 \leq j \leq k) \\
= & \{\text{definition } S\text{; calculus}\} \\
& S(k) + a[k] \cdot \Sigma(b[j] \mid j :\ 0 \leq j \leq k) \\
= & \{\text{use half-open intervals}\} \\
& S(k) + a[k] \cdot \Sigma(b[j] \mid j :\ 0 \leq j < k+1) \\
= & \{\textbf{introduce } T(k) = \Sigma(b[j] \mid j :\ 0 \leq j < k)\ \} \\
& S(k) + a[k] \cdot T(k+1)
\end{array}
$$

Exercise 10.13: Examining $S(x)$

$$\boxed{S(k) = \Sigma(a[i] \cdot b[j] \mid i,j:\ 0 \le j \le i < k)}$$

Clearly, $0 = S(0)$.

We need to increment k. We examine $S(k+1)$, for $k < n$:

$$\begin{array}{ll}
& S(k+1) \\
= & \quad \{\text{definition } S\} \\
& \Sigma(a[i] \cdot b[j] \mid i,j:\ 0 \le j \le i < k+1) \\
= & \quad \{\text{split domain: } i < k \vee i = k\} \\
& \Sigma(a[i] \cdot b[j] \mid i,j:\ 0 \le j \le i < k) + \Sigma(a[k] \cdot b[j] \mid j:\ 0 \le j \le k) \\
= & \quad \{\text{definition } S\text{; calculus}\} \\
& S(k) + a[k] \cdot \Sigma(b[j] \mid j:\ 0 \le j \le k) \\
= & \quad \{\text{use half-open intervals}\} \\
& S(k) + a[k] \cdot \Sigma(b[j] \mid j:\ 0 \le j < k+1) \\
= & \quad \{\textbf{introduce } T(k) = \Sigma(b[j] \mid j:\ 0 \le j < k)\ \} \\
& S(k) + a[k] \cdot T(k+1)
\end{array}$$

We encountered the function $T(k)$ before, so without proof:

$$\boxed{T(0) = 0; \quad T(k+1) = b[k] + T(k)}$$

Exercise 10.13: Recurrences

For the following definitions

$$
\begin{array}{rcl}
S(k) & = & \Sigma(a[i] \cdot b[j] \mid i, j : \ 0 \leq j \leq i < k) \\
T(k) & = & \Sigma(b[j] \mid j : \ 0 \leq j < k)
\end{array}
$$

We found the recurrences:

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

Exercise 10.13: Invariant & Initialization

1. Choose an invariant J and guard B.
   Since $Q \equiv x = S(n)$, we keep $x = S(k)$ invariant while incrementing k:

   $$J : \; x = S(k) \; \wedge \; 0 \leq k \leq n \; \wedge \; y = T(k)$$

   Clearly, we choose $B : \; k \neq n$, such that $J \; \wedge \; \neg B \Rightarrow \; Q$.

Exercise 10.13: Invariant & Initialization

1 Choose an invariant J and guard B.
Since $Q \equiv x = S(n)$, we keep $x = S(k)$ invariant while incrementing k:

$$J: \; x = S(k) \; \wedge \; 0 \leq k \leq n \; \wedge \; y = T(k)$$

Clearly, we choose $B: \; k \neq n$, such that $J \; \wedge \; \neg B \Rightarrow Q$.

2 Initialization: The initialization is easy:

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

Exercise 10.13: Invariant & Initialization

1 Choose an invariant J and guard B.
Since $Q \equiv x = S(n)$, we keep $x = S(k)$ invariant while incrementing k:

$$J: \ x = S(k) \ \wedge \ 0 \leq k \leq n \ \wedge \ y = T(k)$$

Clearly, we choose $B: \ k \neq n$, such that $J \ \wedge \ \neg B \Rightarrow Q$.

2 Initialization: The initialization is easy:

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

3 Variant function: $vf = n - k \in \mathbb{Z}$. Clearly, $J \wedge B \Rightarrow vf \geq 0$.

Exercise 10.13: Body of the Loop

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

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

Exercise 10.13: Body of the Loop

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

(* $0 \leq k < n \Rightarrow T(k+1) = b[k] + T(k)$; *substitution* *)

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

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

Exercise 10.13: Body of the Loop

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

(* $0 \leq k < n \Rightarrow T(k+1) = b[k] + T(k)$; *substitution* *)

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

$y := y + b[k];$

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

$k := k + 1;$

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

Exercise 10.13: Body of the Loop

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

(* $0 \leq k < n \Rightarrow T(k+1) = b[k] + T(k)$; *substitution* *)

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

$y := y + b[k];$

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

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

$k := k + 1;$

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

Exercise 10.13: Body of the Loop

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

(* $0 \leq k < n \Rightarrow T(k+1) = b[k] + T(k)$; *substitution* *)

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

$y := y + b[k];$

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

(* $0 \leq k < n \Rightarrow S(k+1) = S(k) + a[k] \cdot T(k+1)$; *substitution* *)

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

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

$k := k + 1;$

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

Exercise 10.13: Body of the Loop

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

(* $0 \leq k < n \Rightarrow T(k+1) = b[k] + T(k)$; substitution *)

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

$y := y + b[k];$

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

(* $0 \leq k < n \Rightarrow S(k+1) = S(k) + a[k] \cdot T(k+1)$; substitution *)

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

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

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

$k := k + 1;$

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

Exercise 10.13: Body of the Loop

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

(* $0 \leq k < n \Rightarrow T(k+1) = b[k] + T(k)$; substitution *)

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

$y := y + b[k];$

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

(* $0 \leq k < n \Rightarrow S(k+1) = S(k) + a[k] \cdot T(k+1)$; substitution *)

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

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

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

(* calculus *)

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

$k := k + 1;$

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

Exercise 10.13: Body of the Loop

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

(* $0 \leq k < n \Rightarrow T(k+1) = b[k] + T(k)$; *substitution* *)

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

$y := y + b[k];$

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

(* $0 \leq k < n \Rightarrow S(k+1) = S(k) + a[k] \cdot T(k+1)$; *substitution* *)

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

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

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

(* *calculus* *)

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

$k := k + 1;$

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

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

Exercise 10.13: Body of the Loop

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

(* $0 \leq k < n \Rightarrow T(k+1) = b[k] + T(k)$; *substitution* *)

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

$y := y + b[k];$

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

(* $0 \leq k < n \Rightarrow S(k+1) = S(k) + a[k] \cdot T(k+1)$; *substitution* *)

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

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

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

(* *calculus* *)

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

$k := k + 1;$

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

(* *definitions of* J, vf *)

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

Exercise 10.13: Conclusion

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

The End