Chapter 2 (Part 3)

Constants

The following is not satisfactory:

$$
\begin{array}{l}
[\![\\
\textbf{var}\ A, B, x : int; \\
\{A > 0 \wedge B > 0\} \\
\quad gcd \\
\{x = A\ gcd\ B\} \\
]\!]
\end{array}
$$

as $A, B, x := 1, 1, 1$ is a possible solution. Constant should not be changed.

$$
\begin{array}{l}
[\![\\
\textbf{con}\ A, B, x : int; \\
\{A > 0 \wedge B > 0\} \\
\quad gcd \\
\{x = A\ gcd\ B\} \\
]\!]
\end{array}
$$

Inner Blocks

Used to extend the state (locally) by means of new variables.

$$\{P\}[[\mathbf{var}\ y\ ; S]]\{Q\}$$

is equivalent to

$$\{P\}S\{Q\}$$

provided that y does not occur in both P and Q.

Arrays

Arrays are used to represent a set of variables.

$$f : \textbf{array } [p..q) \textbf{ of } int$$

defines a program variable f which has as value a function:

$$[p..q) \to \mathcal{Z}.$$

Chapter 3: Quantification

Uniform Computation on Sequences

For sequence $x.i$, $0 \le i < n$:

$$x.0 \oplus \cdots \oplus x.(n-1)$$

is written as

$$\underline{(\oplus i : 0 \le i < n : x.i)}$$

where $\oplus$ is commutative, associative and has e as identity. i.e.,

$$\begin{aligned} x \oplus y &= y \oplus x \\ x \oplus (y \oplus z) &= (x \oplus y) \oplus z \\ e \oplus x = x \oplus e &= x \end{aligned}$$

Note:

$$\begin{aligned} (\oplus i : 0 \le i < 0 : x.i) &= e \\ (\oplus i : 0 \le i < n+1 : x.i) &= (\oplus i : 0 \le i < n : x.i) \oplus x.n \end{aligned}$$

Quantification

Let $\oplus$ be an accumulative and associative binary operator with identity of e.

$$\underline{(\oplus x : R : F)}$$

where

- x: a list of variables
- R: a predicate denoting the *range* of the quantification
- F: a *term*.

We have

$$(\oplus x : \text{false} : F) \;=\; e.$$

$+$ and $*$

Let $+$ and $*$ be operators on $\mathcal{Z}$.

$$\begin{aligned}
(+i : 3 \le i < 5 : i^2) &= 25 \\
(+x, y : 0 \le x < 3 \wedge 0 \le y < 3 : x * y) &= 9 \\
(*k : 1 \le k < 4 : k) &= 6 \\
(+x : \text{false} : F.x) &= 0 \\
(*x : \text{false} : F.x) &= 1
\end{aligned}$$

Notation:

- $(\Sigma i : R : F)$ for $(+i : R : F)$
- $(\Pi i : R : F)$ for $(*i : R : F)$

Max and Min

The binary operators *max* and *min* are defined on $\mathcal{Z} \cup \{\infty, -\infty\}$:

$$a\ max\ b = c \ \equiv\ (a = c \vee b = c) \wedge a \leq c \wedge b \leq c$$
$$a\ min\ b = c \ \equiv\ (a = c \vee b = c) \wedge a \geq c \wedge b \geq c$$

where the identity for *max* is $-\infty$ and the identity for *min* is ∞.

- *min* and *max* distribute over each other.

$$x\ min\ (max\ i : R : F.i) \ = \ (max\ i : R : x\ min\ F.i)$$
$$x\ max\ (min\ i : R : F.i) \ = \ (min\ i : R : x\ max\ F.i)$$

- $+$ distributes over *max* and *min* for a *non-empty* range R.

$$x + (max\ i : R : F.i) \ = \ (max\ i : R : x + F.i)$$
$$x + (min\ i : R : F.i) \ = \ (min\ i : R : x + F.i)$$

$\wedge$ and $\vee$

Let $N \geq 0$ and let $X[0..N)$ be an array of integers.

$$\begin{array}{lcl} X \text{ is increasing} & \equiv & (\wedge i, j : 0 \leq i < j < N : X.i < X.j) \\ X \text{ is decreasing} & \equiv & (\wedge i, j : 0 \leq i < j < N : X.i > X.j) \\ X \text{ is ascending} & \equiv & (\wedge i, j : 0 \leq i < j < N : X.i \leq X.j) \\ X \text{ is descending} & \equiv & (\wedge i, j : 0 \leq i < j < N : X.i \geq X.j) \end{array}$$

Notation:

- $(\forall i : R : F)$ for $(\wedge i : R : F)$
- $(\exists i : R : F)$ for $(\vee i : R : F)$

General Properties

$$
\begin{aligned}
(\oplus i : \mathit{false} : F) &= e \\
(\oplus i : i = x : F) &= F(i := x) \\
(\oplus i : R : F) \oplus (\oplus i : S : F) &= (\oplus i : R \vee S : F) \oplus (\oplus i : R \wedge S : F) \\
(\oplus i : R : F) \oplus (\oplus i : R : G) &= (\oplus i : R : F \oplus G) \\
(\oplus i : R.i : (\oplus j : S.j : F.i.j)) &= (\oplus j : S.j : (\oplus i : R.i : F.i.j))
\end{aligned}
$$

When $\oplus$ is idempotent as well, i.e., $x \oplus x = x$, then

$$
\begin{aligned}
(\oplus i : R : F) \oplus (\oplus i : S : F) &= (\oplus i : R \vee S : F) \\
x \oplus (\oplus i : R : F) &= (\oplus i : R; x \oplus F)
\end{aligned}
$$

Let $\otimes$ be a binary operator on X that distributes over $\oplus$, and has e as zero. Then

$$
\begin{aligned}
x \otimes (\oplus i : R : F) &= (\oplus i : R; x \otimes F) \\
(\oplus i : R.i : F.i) \otimes (\oplus i : S.i : G.i) &= (\oplus i, j : R.j \wedge S.j : F.i \otimes G.j)
\end{aligned}
$$

Sort of Fusion.

“the number of” Quantifier

$$(\#i : R.i : F.i)$$

is defined by

$$(\Sigma i : R.i : \#.(F.i))$$

where $\#$ is a function defined by

$$\begin{aligned} \#.\mathit{false} &= 0 \\ \#.\mathit{true} &= 1 \end{aligned}$$

Notice that

$$\begin{aligned} (\exists i : R : F) &\equiv (\#i : R : F) \geq 1 \\ (\forall i : R : F) &\equiv (\#i : R : F) = (\#i : R : \mathit{true}) \end{aligned}$$

Specification using Quantifiers

Let $X[0..N)$ be an integer array.

1. r is the sum of the elements of X.

$$r = (\Sigma i : 0 \leq i < N : X.i)$$

2. m is the maximum of the array.

$$m = (max\ i : 0 \leq i < N : X.i)$$

3. All values of X are distinct.

$$(\# i, j : 0 \leq i < j < N : X.i = X.j) < 1$$

4. All values of X are equal.

$$(\forall i, j : 0 \leq i < j < N : X.i = X.j)$$

5. If X contains a 1 then X contains a 0 as well.

$$(\exists i : 0 \leq i < N : X.i = 1) \Rightarrow (\exists i : 0 \leq i < N : X.i = 0)$$

6. No two neighbors in X are equal.

$$(\forall i : 0 \leq i < N - 1 : X.i \neq X.(i + 1))$$

7. The maximum of X occurs only once in X.

$$(\#i : 0 \leq i < N : X.i = (max\ j : 0 \leq j < N : X.j)) = 1$$

8. r is the length of the longest constant segment of X.

$$r = (max\ p, q : 0 \leq p < q \leq N \land (\forall i, j : p \leq i < j < q : X.i = X.j) : q - p)$$

9. r is the length of the longest ascending segment of X.

$$r = (max\ p, q : 0 \leq p < q \leq N \land (\forall i, j : p \leq i < j < q : X.i \leq X.j) : q - p)$$

10. X is a permutation of $[0..N]$.

$$(\forall i : 0 \le i < N : (\exists j : 0 \le j < N : X[j] = i))$$

11. The number of odd elements equals the number of even elements.

$$(\# i : 0 \le i < N : X.i \ \mathit{mod}\ 2 = 1) \ = \ (\# i : 0 \le i < N : X.i \ \mathit{mod}\ 2 = 0)$$

12. r is the product of the positive elements of X.

$$r = (\Pi i : 0 \le i < N \wedge X[i] > 0 : X.i)$$

13. r is the maximum of the sums of segments of X.

$$r = (max\ i, j : 0 \leq i \leq j < N : (\Sigma k : i \leq k \leq j : X.k))$$

14. X contains a square.

$$(\exists p, q : 0 \leq p \leq q < N \wedge (\forall i, j : p \leq i < j \leq q : X.i = X.j) : q - p + 1 = X.p)$$

Exercises

Problem 3

Let $X[0..N)$ be an integer array. Express the following expressions in a natural language.

1. $b \equiv (\forall i : 0 \leq i < N : X.i \geq 0)$
2. $r = (max\ p, q : 0 \leq p \leq q \leq N \wedge (\forall i : p \leq i < q : X.i \geq 0) : q - p)$
3. $r = (\#k : 0 \leq k < N : (\forall i : 0 \leq i < k : X.i < X.k))$
4. $b \equiv (\exists i : 0 < i < N : X.(i-1) < X.i)$
5. $r = (\#p, q : 0 \leq p < q < N : X.p = 0 \wedge X.q = 0)$
6. $s = (max\ p, q : 0 \leq p < q < N : X.p + X.q)$
7. $b \equiv (\forall p, q : 0 \leq p \wedge 0 \leq q \wedge p + q = N - 1 : X.p = X.q)$
8. $b = (\exists i : 0 \leq i < N . X.i = 0)$