Verifikation

1 Das Programm S

$S ::=$
```
int[] a = new int[10];
int   i;
int   imin;

i = 1;
imin = 0;

while ( i < 10 ) {

   if ( a[i] < a[imin] ) {
      imin = i;
   }

   i = i+1;
}
```

Zu beweisende Pre-/Post condition: $\{PRE\}\ S\ \{POST\}$

$$PRE \ ::= \ true$$

$$POST \ ::= \ imin \in \{0..9\} \ \wedge \ \forall j \in \{0..9\} \bullet a[imin] \leq a[j]$$

2 Partielle Korrektheit

Nach dem Deklarationsteil gilt:

$$P_0 ::= i \in int \ \wedge \ imin \in int \ \wedge \ a \in \{0..9\} \rightarrow int$$

2.1 Schritt 1

Beh: Es gilt $\{P_0\}$ `i = 1;` $\{P_0 \wedge i = 1\}$
Bew: Logische Ableitung:

$$\begin{aligned} P_0 \ &\Rightarrow \ i \in int \wedge imin \in int \wedge a \in \{0..9\} \rightarrow int \wedge 1 = 1 \\ &\Rightarrow \ (i \in int \wedge imin \in int \wedge a \in \{0..9\} \rightarrow int \wedge i = 1)^1_i \\ &\Rightarrow \ (P_0 \wedge i = 1)^1_i \end{aligned}$$

Aus der Konsequenzregel folgt also, dass nach der Variablendeklaration auch $\{(P_0 \wedge i = 1)^1_i\}$ gilt. Die Anwendung der Zuweisungsregel resultiert in der Behauptung $\{P_0\}$ `i = 1`; $\{P_0 \wedge i = 1\}$.

2.2 Schritt 2

Beh: es gilt $\{P_0 \wedge i = 1\}$ `imin = 0`; $\{P_0 \wedge i = 1 \wedge imin = 0\}$
Bew: genau wie in Schritt 1

2.3 Schritt 3

Beh: es gilt $\{P_0\}$ `i = 1; imin = 0`; $\{P_0 \wedge i = 1 \wedge imin = 0\}$
Bew: Anwendung der Sequenzregel mit Schritt 1 und Schritt 2

2.4 Schritt 4

Es gelten folgende Abkürzungen:

$$\begin{aligned} P_1 \quad ::= \quad & P_0 \wedge i \in \{1..10\} \wedge imin \in \{0..9\} \wedge \\ & \forall j \in \{0..(i-1)\} \bullet a[imin] \leq a[j] \\ B \quad ::= \quad & i < 10 \end{aligned}$$

Beh: es gilt $\{P_0\}$ `i = 1; imin = 0`; $\{P_1 \wedge B\}$
Bew: es ist zu zeigen, dass $P_0 \wedge i = 1 \wedge imon = 0 \Rightarrow P_1 \wedge B$, wobei P_1 die Schleifeninvariante ist.

$$\begin{aligned} & P_0 \wedge i = 1 \wedge imin = 0 \\ \Rightarrow \quad & i \in int \wedge imin \in int \wedge a \in \{0..9\} \rightarrow int \wedge i = 1 \wedge imin = 0 \\ \Rightarrow \quad & i \in int \wedge imin \in int \wedge a \in \{0..9\} \rightarrow int \wedge i = 1 \wedge imin = 0 \wedge \\ & \forall j \in \{0..0\} \bullet a[0] \leq a[0] \wedge 1 < 10 \\ \Rightarrow \quad & i \in int \wedge imin \in int \wedge a \in \{0..9\} \rightarrow int \wedge i = 1 \wedge imin = 0 \wedge \\ & \forall j \in \{0..(i-1)\} \bullet a[imin] \leq a[j] \wedge i < 10 \\ \Rightarrow \quad & P_1 \wedge B \end{aligned}$$

Die Behauptung folgt also aus Anwendung der Konsequenzregel und Schritt 3.

2.5 Schritt 5

Beh: Es gilt $\{P_1 \wedge B\}$ `if (a[i] < a[imin]) imin = i;` $\{P_1 \wedge B \wedge a[imin] \leq a[i]\}$

Bew: Gelte $\{P_1 \wedge B\}$

Fall 1: Sei $a[i] < a[imin]$. Dann gilt $\{P_1 \wedge B \wedge a[i] < a[imin]\}$. Hieraus läßt sich ableiten:

$$\begin{array}{ll} & P_1 \wedge B \wedge a[i] < a[imin] \\ \Rightarrow & i \in int \wedge imin \in int \wedge a \in \{0..9\} \rightarrow int \wedge i < 10 \wedge \\ & \forall j \in \{0..(i-1)\} \bullet a[imin] \leq a[j] \wedge a[i] < a[imin] \\ \Rightarrow & (i \in int \wedge imin \in int \wedge a \in \{0..9\} \rightarrow int \wedge i < 10 \wedge \\ & \forall j \in \{0..i\} \bullet a[imin] \leq a[j])^i_{imin} \end{array}$$

Nach Konsequenzregel gilt also

$$\begin{array}{l} \{(i \in int \wedge imin \in int \wedge a \in \{0..9\} \rightarrow int \wedge i < 10 \wedge \\ \forall j \in \{0..i\} \bullet a[imin] \leq a[j])^i_{imin}\} \end{array}$$

also Vorbedingung zu $imin = i$. Mit Hilfe des Zuweisungsaxioms und der Konsequenzregel erhalten wir:

$$\begin{array}{l} \{P_1 \wedge B \wedge a[i] < a[imin]\} \\ \quad \texttt{imin} = \texttt{i}; \\ \{(i \in int \wedge imin \in int \wedge a \in \{0..9\} \rightarrow int \wedge i < 10 \wedge \\ \forall j \in \{0..i\} \bullet a[imin] \leq a[j])\} \end{array}$$

Die Anwendung der Konsequenzregel ergibt:

$$\begin{array}{l} \{P_1 \wedge B \wedge a[i] < a[imin]\} \\ \quad \texttt{imin} = \texttt{i}; \\ \{P_1 \wedge B \wedge a[imin] \leq a[i]\} \end{array}$$

Fall 2: gelte $\neg(a[i] < a[imin])$, also $a[imin] \leq a[i]$ Dann gilt trivialerweise (Axiom fuer die leere Anweisung)

$$\{P_1 \wedge B \wedge \neg(a[i] < a[imin])\}\ \{P_1 \wedge B \wedge a[imin] \leq a[i]\}$$

Die Behauptung von Schritt 5 folgt jetzt aus der if-Regel.

2.6 Schritt 6

Beh: Es gilt $\{P_1 \wedge B \wedge a[imin] \leq a[i]\}\ \texttt{i} = \texttt{i} + \texttt{1}; \{P_1\}$

Bew: Logische Ableitung

$$
\begin{array}{ll}
 & P_1 \wedge B \wedge a[imin] \leq a[i] \\
\Rightarrow & i \in int \wedge imin \in int \wedge a \in \{0..9\} \rightarrow int \wedge i < 10 \wedge \\
 & \forall j \in \{0..(i-1)\} \bullet a[imin] \leq a[j] \wedge a[imin] \leq a[i] \\
\Rightarrow & i \in int \wedge imin \in int \wedge a \in \{0..9\} \rightarrow int \wedge i + 1 \leq 10 \wedge \\
 & \forall j \in \{0..i\} \bullet a[imin] \leq a[j] \\
\Rightarrow & (i \in int \wedge imin \in int \wedge a \in \{0..9\} \rightarrow int \wedge i \leq 10 \wedge \\
 & \forall j \in \{0..(i-1)\} \bullet a[imin] \leq a[j])_i^{i+1} \\
\Rightarrow & P_1 \, {}_i^{i+1}
\end{array}
$$

Anwendung der Konsequenzregel ergibt also $\{P_1 \, {}_i^{i+1}\}$ als Precondition von $i = i + 1$; damit folgt die Behauptung aus der Zuweisungsregel.

2.7 Schritt 7

Beh: Es gilt

$\{P_1 \wedge B\}$
  `if (a[i] < a[imin]) {`
    `imin = i;`
  `}`
  `i = i + 1;`
$\{P_1\}$

Bew: folgt aus Anwendung der Sequenzregel auf Schritt 5 und Schritt 6.

2.8 Schritt 8

Beh: Es gilt

$\{P_1 \wedge B\}$
  `while (i < 10) {`
    `if (a[i] < a[imin]) {`
      `imin = i;`
    `}`
    `i = i + 1;`
  `}`
$\{P_1 \wedge \neg B\}$

Bew: Folgt aus Anwendung der while-Regel, Schritt 4 und Schritt 7.

2.9 Schritt 9

Beh: Es gilt $\{true\}\ S\ \{P_1 \wedge \neg B\}$
Bew: Folgt aus Schritt 4, Schritt 8 und Anwendung der Sequenzregel.

2.10 Schritt 10

Beh: Es gilt das Beweisziel $\{PRE\}\ S\ \{POST\}$
Bew: Logische Ableitung:

$$\begin{array}{ll} & P_1 \wedge \neg B \\ \Rightarrow & \forall j \in \{0..(i-1)\} \bullet a[imin] \leq a[j] \wedge i = 10 \wedge imin \in \{0..9\} \\ \Rightarrow & \forall j \in \{0..9\} \bullet a[imin] \leq a[j] \wedge imin \in \{0..9\} \\ \Rightarrow & POST \end{array}$$

Die Anwendung der Konsequenzregel und Schritt 9 ergibt das Beweisziel $\{PRE\}\ S\ \{POST\}$. □

3 Totale Korrektheit

Für die totale Korrektheit ist zusätzlich zu zeigen, dass

1. $P_1 \wedge B \Rightarrow t \geq 0$
2. $\{P_1 \wedge B \wedge t = T\}$ `if (a[i] < a[imin]) {imin = i; } i = i + 1;` $\{t < T\}$

Wähle die Terminierungsvariable t wie folgt: $t = 10 - i$.

3.1 Schritt 11

Beh: $P_1 \wedge B \Rightarrow t \geq 0$
Bew: Logische Ableitung:

$$\begin{array}{ll} & P_1 \wedge B \\ \Rightarrow & P_0 \wedge i \in \{1..10\} \wedge imin \in \{0..9\} \wedge \\ & \forall j \in \{0..(i-1)\} \bullet a[imin] \leq a[j] \wedge i < 10 \\ \Rightarrow & i \in 1..9 \end{array}$$

Eingesetzt in die Terminierungsvariable $t = 10 - i$ folgt, dass $t \geq 0$.

3.2 Schritt 12

Beh: $\{P_2\}\ i = i + 1;\ \{t < T\}$, mit $P_2 = (9 - i < T)$
Bew: Nach dem Zuweisungsaxiom gilt:

$$P_2 = (t < T)_i^{i+1} = (10 - i < T)_i^{i+1} = (10 - (i + 1) < T) = 9 - i < T$$

3.3 Schritt 13

Beh: $\{P_2\}$ `if (a[i] < a[imin]) {imin = i;}` $\{P_2\}$
Bew: Es gelte $\{P_2\}$, dann ist zu zeigen:

Fall 1: Sei $a[i] < a[imin]$, dann gilt $\{P_2 \wedge a[i] < a[imin]\}$. Hieraus läßt sich ableiten:

$$\begin{aligned} & P_2 \wedge a[i] < a[imin] \\ \Rightarrow\ & 9 - i < T \wedge a[i] < a[imin] \\ \Rightarrow\ & 9 - i < T \\ \Rightarrow\ & (9 - i < T)_{imin}^{i} \\ \Rightarrow\ & P_{2\ imin}^{\ i} \end{aligned}$$

Damit gilt das Zuweisungsaxiom:

$$\{P_2 \wedge a[i] < a[imin]\}\ imin = i;\ \{P_2\}$$

Fall 2: Sei $\neg(a[i] < a[imin])$. Für die leere Anweisung und die Konsequenzregel mit $P_2 \wedge \neg(a[i] < a[imin]) \Rightarrow P_2$ gilt:

$$\{P_2 \wedge \neg(a[i] < a[imin])\}\ \{P_2\}$$

Die Behauptung von Schritt 13 folgt jetzt aus der if-Regel.

3.4 Schritt 14

Beh: $\{P_2\}$ `if (a[i] < a[imin]) {imin = i;} i = i + 1;` $\{t < T\}$
Bew: Folgt aus Schritt 12, Schritt 13 und der Sequenzregel.

3.5 Schritt 15

Beh: es gilt $\{P_1 \wedge B \wedge t = T\}$`if (a[i] < a[imin]) {imin = i;} i = i + 1;`$\{t < T\}$

Bew: Logische Ableitung:

$$
\begin{aligned}
& P_1 \wedge B \wedge t = T \\
\Rightarrow\ & P_0 \wedge i \in \{1..10\} \wedge imin \in \{0..9\} \wedge \\
& \forall j \in \{0..(i-1)\} \bullet a[imin] \leq a[j] \wedge i < 10 \wedge 10 - i = T \\
\Rightarrow\ & i \in \{1..9\} \wedge 10 - i = T \\
\Rightarrow\ & 9 - i < T = P_2
\end{aligned}
$$

Die Behauptung folgt aus Schritt 14 und der Konsequenzregel. Damit wurde gezeigt, dass die Terminierungsvariable mit jedem Schleifendurchlauf kleiner wird.

Aus den Schritten 11 und 14 folgt, dass die while-Schleife terminiert. Zusätzlich mit Schritt 7 wurde die totale Korrektheit gezeigt. □