Example.
Systematic program construction

Włodzimierz Drabent

LOPSTR 2021
Version 0.4 of September 7, 2021

Constructing correct$^+$ programs, example

insert/3 of insertion sort (inserting a number into a sorted list)

Specification: (S^0, S)

$$S^0 = \left\{ i(n, l_1, l_2) \in \mathcal{HB} \;\middle|\; \begin{array}{l} l_1, l_2 \text{ are sorted lists of integers,} \\ \mathit{elms}(l_2) = \{n\} \cup \mathit{elms}(l_1) \end{array} \right\}$$

where $\mathit{elms}(l)$ – the multiset of elements of l

$$S = \left\{ i(n, l_1, l_2) \in \mathcal{HB} \;\middle|\; \begin{array}{l} n \notin \mathbb{Z}, \text{ or} \\ l_1 \text{ not a sorted list} \\ \text{of integers} \end{array} \right\} \cup S^0$$

Constructing correct$^+$ programs, example

insert/3 of insertion sort (inserting a number into a sorted list)

Specification: (S^0, S)

$$S^0 = \left\{ i(n, l_1, l_2) \in \mathcal{HB} \;\middle|\; \begin{array}{l} l_1, l_2 \text{ are sorted lists of integers,} \\ \mathit{elms}(l_2) = \{n\} \cup \mathit{elms}(l_1) \end{array} \right\}$$
$$\cup \{ i < j | \ldots \} \cup \ldots$$

where $\mathit{elms}(l)$ – the multiset of elements of l

$$S = \left\{ i(n, l_1, l_2) \in \mathcal{HB} \;\middle|\; \begin{array}{l} n \notin \mathbb{Z}, \text{ or} \\ l_1 \text{ not a sorted list} \\ \text{of integers} \end{array} \right\} \cup S^0$$
$$\cup \{ i < j | \ldots \} \cup \ldots$$

Constructing correct$^+$ programs, example

Summary of the approach:
1. each atom $A \in S^0$ is covered w.r.t. S^0
2. each clause correct w.r.t. S
3. termination...

Specification (S^0, S). Three kinds of elements of S^0:

1. $i(n, [\,], [n]) \in S^0$.
2. $A = i(n, [h|t], [n, h|t])$, $n \leq h$.
3. $A = i(n, [h|t], [h|t'])$, $n > h$.

Constructing correct$^+$ programs, example

Summary of the approach:
1. each atom $A \in S^0$ is covered w.r.t. S^0
2. each clause correct w.r.t. S
3. termination...

Specification (S^0, S). Three kinds of elements of S^0:

1. $i(n, [\,], [n]) \in S^0$. Covered by clause $C_1 = i(N, [\,], [N])$. $S \models C_1$.
2. $A = i(n, [h|t], [n, h|t])$, $n \leq h$.
3. $A = i(n, [h|t], [h|t'])$, $n > h$.

Constructing correct$^+$ programs, example

Summary of the approach:
1. each atom $A \in S^0$ is covered w.r.t. S^0
2. each clause correct w.r.t. S
3. termination...

Specification (S^0, S). Three kinds of elements of S^0:

1. $i(n, [\,], [n]) \in S^0$. Covered by clause $C_1 = i(N, [\,], [N])$. $S \models C_1$.
2. $A = i(n, [h|t], [n, h|t])$, $n \leq h$. Covered by $C = i(N, [H|T], [N, H|T])$, $S \not\models C$. ☹
3. $A = i(n, [h|t], [h|t'])$, $n > h$.

Constructing correct$^+$ programs, example

Summary of the approach:
1. each atom $A \in S^0$ is covered w.r.t. S^0
2. each clause correct w.r.t. S
3. termination…

Specification (S^0, S). Three kinds of elements of S^0:

1. $i(n, [\,], [n]) \in S^0$. Covered by clause $C_1 = i(N, [\,], [N])$. $S \models C_1$.

2. $A = i(n, [h|t], [n, h|t])$, $n \le h$. Covered by $C = i(N, [H|T], [N, H|T])$, $S \not\models C$. ☹ Correct it: $C_2 = C \leftarrow N \le H$. $S \models C_2$. A Covered by C_2.

3. $A = i(n, [h|t], [h|t'])$, $n > h$.

Example Specification Construction

Constructing correct$^+$ programs, example

Summary of the approach:
1. each atom $A \in S^0$ is covered w.r.t. S^0
2. each clause correct w.r.t. S
3. termination…

Specification (S^0, S). Three kinds of elements of S^0:

1. $i(n, [\,], [n]) \in S^0$. Covered by clause $C_1 = i(N, [\,], [N])$. $S \models C_1$.

2. $A = i(n, [h|t], [n, h|t])$, $n \le h$. Covered by $C = i(N, [H|T], [N, H|T])$, $S \not\models C$. ☹ Correct it: $C_2 = C \leftarrow N \le H$. $S \models C_2$. A Covered by C_2.

3. $A = i(n, [h|t], [h|t'])$, $n > h$. Note that $i(n, t, t') \in S^0$. A covered by $C' = i(N, [H|T], [H|T']) \leftarrow i(N, T, T')$. $S \not\models C$. ☹

Example Specification Construction

Constructing correct$^+$ programs, example

Summary of the approach:
1. each atom $A \in S^0$ is covered w.r.t. S^0
2. each clause correct w.r.t. S
3. termination…

Specification (S^0, S). Three kinds of elements of S^0:

1. $i(n, [\,], [n]) \in S^0$. Covered by clause $C_1 = i(N, [\,], [N])$. $S \models C_1$.

2. $A = i(n, [h|t], [n, h|t])$, $n \le h$. Covered by $C = i(N, [H|T], [N, H|T])$, $S \not\models C$. ☹ Correct it: $C_2 = C \leftarrow N \le H$. $S \models C_2$. A Covered by C_2.

3. $A = i(n, [h|t], [h|t'])$, $n > h$. Note that $i(n, t, t') \in S^0$. A covered by $C' = i(N, [H|T], [H|T']) \leftarrow i(N, T, T')$. $S \not\models C$. ☹ Correct it: $C_3 = C', N{>}H$. $S \models C_3$. A covered by C_3.

$P = \{C_1, C_2, C_3\}$ correct & complete w.r.t. (S^0, S).