# Example. Systematic program construction

#### Włodzimierz Drabent

#### LOPSTR 2021 Version 0.4 of September 7, 2021

(ロト・(型ト・ミト・ミト) そのの(や 1/3)

# Constructing correct<sup>+</sup> 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. S3. termination...

#### $\mbox{Specification } (S^0,S). \mbox{ Three kinds of elements of } S^0: \label{eq:specification}$

1.  $i(n, [], [n]) \in S^0$ .

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

< □ > < ∰ > < ≣ > < ≣ > = ■ ● ● ●

# Constructing correct<sup>+</sup> programs, example

insert/3 of insertion sort (inserting a number into a sorted list) Specification:  $(S^0,S)$ 

$$S^{0} = \left\{ i(n, l_{1}, l_{2}) \in \mathcal{HB} \mid \begin{array}{c} l_{1}, l_{2} \text{ are sorted lists of integers,} \\ elms(l_{2}) = \{n\} \cup elms(l_{1}) \end{array} \right\}$$

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

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

.

# Constructing correct<sup>+</sup> 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. $A = i(n, [h t], [n, h t]), n \le h.$
3. $A = i(n, [h t], [h t']), n > h.$

3/3

3/3

## Constructing correct<sup>+</sup> programs, example

insert/3 of insertion sort (inserting a number into a sorted list) Specification:  $(S^0, S)$ 

$$\begin{split} S^0 &= \left\{ \begin{array}{l} i(n,l_1,l_2) \in \mathcal{HB} \\ \cup \left\{ i < j \right| \dots \right\} \cup \dots \\ \text{where } elms(l_2) = \left\{ n \right\} \cup elms(l_1) \\ \text{where } elms(l) - \text{ the multiset of elements of } l \end{split} \right. \end{split}$$

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

2/3

Constructing correct<sup>+</sup> 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  $S^0$ :

 $\label{eq:clause} \mathsf{1.}\ i(n,[\,],[n])\in S^0. \ \ \text{Covered by clause}\ C_1=i(N,[\,],[N]). \ \ S\models C_1.$ 

2.  $A = i(n, [h|t], [n, h|t]), n \leq h$ . Covered by  $C = i(N, [H|T], [N, H|T]), S \neq C$ .

3/3

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

<<u>ロ><</u>/>

#### Constructing correct<sup>+</sup> programs, example

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  $C = i(N, [H|T], [N, H|T]), S \not\models C$ .  $\stackrel{\frown}{\frown}$  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.

<ロト < 四ト < 西ト < 三ト < 三ト 三三 - 今へで 3/3

#### Constructing correct<sup>+</sup> programs, example

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

 $\label{eq:constraint} \mathsf{1.}~i(n,[\,],[n])\in S^0. \ \ \mathsf{Covered} \ \mathsf{by} \ \mathsf{clause} \ C_1=i(N,[\,],[N]). \ \ S\models C_1.$ 

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

## Constructing correct<sup>+</sup> 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. S3. termination. . .

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

 $\label{eq:constraint} \text{1. } i(n,[\,],[n])\in S^0. \quad \text{Covered by clause } C_1=i(N,[\,],[N]). \quad S\models C_1.$ 

2.  $A = i(n, [h|t], [n, h|t]), n \le h$ . Covered by  $C = i(N, [H|T], [N, H|T]), S \models C$ .  $\stackrel{\frown}{\sim}$  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  $i(n, t, t') \in S^0$ .

 $\begin{array}{ll} A \text{ covered by } C' = i(N, [H|T], [H|T']) \leftarrow i(N, T, T'). & S \not\models C. & \frown \\ C_3 = C', N > H. & S \models C_3. & A \text{ covered by } C_3. \end{array}$ 

3/3

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

(ロ) (型) (言) (言) (言) (言) のへの