The general patterns for the proof obligations to discharge for showing the consistency of a simple abstract machine are given at the end of Lecture 4. We abstract away from the contextual abbreviations. Since machine `Deliveries` has no assertions, constraints and properties, proving its consistency involves:

1. proving that the initialization establishes the invariant, namely $[U]I$
2. proving that each operation preserves it, namely $I \wedge Q \Rightarrow [V]I$,

where

$$\begin{aligned} I = \mathit{items} \subseteq \mathit{ITEM} \wedge & \quad (1)\\ \mathit{deliveries} \in \mathit{items} \to \mathit{ADDRESS} \wedge & \quad (2)\\ \mathit{nogo} \subseteq \mathit{ADRESS} & \quad (3)\end{aligned}$$

1. **Initialization**

$$\begin{aligned}[U]I = {} & [\mathit{items} := \phi \mid\mid \mathit{deliveries} := \phi \mid\mid \mathit{nogo} :\in \mathbb{P}(\mathit{ADDRESS})]\ I = \\ & = [\mathit{items} := \phi \mid\mid \mathit{deliveries} := \phi \mid\mid \\ & \quad \mid\mid \mathit{ANY}\ s\ \mathit{WHERE}\ s \in \mathbb{P}(\mathit{ADDRESS})\ \ \mathit{THEN}\ \mathit{nogo} := s\ \mathit{END}]\ I = \\ & = [\ \mathit{ANY}\ s\ \mathit{WHERE}\ s \in \mathbb{P}(\mathit{ADDRESS}) \\ & \quad \mathit{THEN}\ \mathit{items} := \phi \mid\mid \mathit{deliveries} := \phi \mid\mid \mathit{nogo} := s\ \mathit{END}]\ I = \\ & = \forall\ s\ .\ (s \in \mathbb{P}(\mathit{ADDRESS}) \Rightarrow [\mathit{items} := \phi \mid\mid \mathit{deliveries} := \phi \mid\mid \mathit{nogo} := s]\ I) = \\ & = \forall\ s\ .\ (s \in \mathbb{P}(\mathit{ADDRESS}) \Rightarrow \phi \subseteq \mathit{ITEM}\ \wedge \phi : \phi \to \mathit{ADDRESS}\ \wedge s \subseteq \mathit{ADRESS}) \quad (4)\end{aligned}$$

Predicate (4) is obviously true

2. **Operations**

2.1 Operation `load`
We have

$$\begin{aligned} Q = \mathit{ii} \in \mathit{ITEM} - \mathit{items} \wedge & \quad (5)\\ \mathit{aa} \in \mathit{ADDRESS} & \quad (6)\\ V = \mathit{items} := \mathit{items} \cup \{\mathit{ii}\} \mid\mid \mathit{deliveries}(\mathit{ii}) := \mathit{aa} & \end{aligned}$$

Then

$$\begin{aligned}[V]I = {} & [\mathit{items} := \mathit{items} \cup \{\mathit{ii}\} \mid\mid \mathit{deliveries}(\mathit{ii}) := \mathit{aa}]\ I = \\ & = \mathit{items} \cup \{\mathit{ii}\} \subseteq \mathit{ITEM} \wedge \quad (7)\\ & \quad \mathit{deliveries} \mathbin{\lhd\!\!-} \{\mathit{ii} \mapsto \mathit{aa}\} \in \mathit{items} \cup \{\mathit{ii}\} \to \mathit{ADDRESS} \wedge \quad (8)\\ & \quad \mathit{nogo} \subseteq \mathit{ADDRESS} \quad (9)\end{aligned}$$

(9) is equivalent to (3), thus true
(7) follows from (1) and (5)
(8) follows from (2), (5) and (6)

2.2 Operation `drop`
We have

$$Q = items \neq \phi \tag{10}$$
$$V = ANY\ ii\ WHERE\ ii\ \in\ items\ THEN\ items := items - \{ii\} \ ||$$
$$||\ deliveries := \{ii\} \lhd deliveries \ ||\ it, ad := ii, deliveries(ii)\ END$$

Let us denote

$$V' = items := items - \{ii\} \ ||\ deliveries := \{ii\} \lhd deliveries \ ||$$
$$||\ it, ad := ii, deliveries(ii)$$

Then

$$[V]I = [ANY\ ii\ WHERE\ ii \in items\ THEN\ V'\ END]\ I =$$
$$= \forall\ ii\ .\ (ii \in items \Rightarrow [V']I)$$

$$[V']I = items - \{ii\} \subseteq ITEM \ \wedge \tag{11}$$
$$\{ii\} \lhd deliveries \in items - \{ii\} \to ADDRESS \ \wedge \tag{12}$$
$$nogo \subseteq ADDRESS \tag{13}$$

(13) is equivalent to (3), thus true for any $ii \in items$.
(11) follows from (1) for any $ii \in items$.
(12) follows from (2) for any $ii \in items$.

2.3 Operation `endofday`
We have

$$Q = true$$
$$V = CHOICE\ items, deliveries := \phi, \phi\ OR\ skip\ END$$

Then

$$[V]I = [CHOICE\ items, deliveries := \phi, \phi\ OR\ skip\ END]\ I =$$
$$= [items, deliveries := \phi, \phi]\ I \wedge [skip]\ I =$$
$$= [items, deliveries := \phi, \phi]\ I \wedge I \tag{14}$$

The first conjunct of the predicate (14) is provable by analogy to the similar part from the proof concerning the initialisation.

2.4 Operation `warning`
We have

$$Q = aa \in ADDRESS \tag{15}$$
$$V = IF\ aa \in nogo\ THEN\ V_1\ ELSE\ V_2\ END$$
$$V_1 = CHOICE\ nogo := nogo - \{aa\}\ OR$$
$$deliveries := deliveries \rhd \{aa\} \ ||\ items := items - deliveries^{-1}[\{aa\}]\ END$$
$$V_2 = IF\ aa \notin ran(deliveries)\ THEN\ nogo := nogo \cup \{aa\}\ END$$

Then

$$[V]I = (aa \in nogo \Rightarrow [V_1]I) \wedge (\neg\, aa \in nogo \Rightarrow [V_2]I) \tag{16}$$

$$[V_1]I = [nogo := nogo - \{aa\}]\ I \wedge \tag{17}$$
$$[deliveries := deliveries \rhd \{aa\} \mid\mid items := items - deliveries^{-1}[\{aa\}]]\ I \tag{18}$$

(17) reduces to $nogo - \{aa\} \subseteq ADDRESS$, which is true based on (3).

Proving (18) means proving that

$$items - deliveries^{-1}[\{aa\}] \subseteq ITEM \wedge \tag{19}$$
$$deliveries \rhd \{aa\} \in items - deliveries^{-1}[\{aa\}] \rightarrow ADDRESS \tag{20}$$

(19) follows from (1) and (15).
(20) follows from (2) and (15).

$$[V_2]I = (aa \notin ran(deliveries) \Rightarrow [nogo := nogo \cup \{aa\}]I) \wedge \tag{21}$$
$$(\neg aa \notin ran(deliveries) \Rightarrow [skip]I) \tag{22}$$

(22) is obviously true, while (21) reduces to $nogo \cup \{aa\} \subseteq ADDRESS$, which is true based on (3) and (15).