The last page of this document contains a reference for IMP's operational semantics and its Hoare-style logic.

Problem 1. This problem covers the `while` case in the proof of soundness for Hoare logic (Theorem 1). Remember that the proof was by induction on the derivation of $\{P\}\, s\, \{Q\}$.

(a) Write out the statement of exactly what we need to prove in the case for the `while` rule.

Show that if $\{I\}$ `while` e s $\{I \wedge \neg e\}$ **and** $H \models I$ **and** H, `while` e $s \to^* H'$, s' **then** $s' \neq$ `failed` **and if** $s' =$ `skip` **then** $H' \models I \wedge \neg e$

(b) Write out the statement of the induction hypothesis we get from rule induction.

Induction Hypothesis: if $\{I \wedge e\}\, s\, \{I\}$ **and** $H \models I \wedge e$ **and** $H, s \to^* H', s'$ **then** $s \neq$ `failed` **and if** $s' =$ `skip` **then** $H' \models I$

(c) Consider the special case where $s' =$ `skip`. Explain informally in one or two sentences what an execution

$$H, \texttt{while}\ e\ s \to^* H', \texttt{skip}$$

looks like by relating the execution of the loop to the execution of its body s.

Hint: If you're not sure how to proceed, check out the picture on slide 8 in lecture 12 and see if you can figure out what I meant there.

- Case 1. $H, e \Downarrow \bot$. Then by the operational semantics, H, `while` e $s \to^* H$, `skip`
- Case 2. $H, e \Downarrow \top$. Then s is executed by at least once, until the conditional e evaluated to $\bot$, the whole expression steps to H', `skip`.

(d) State (but do not prove) a formal lemma for this special case of the form

If H, `while` e $s \to^* H'$, `skip`, then ...

In order to state your lemma, you will very likely need to introduce a new concept/definition. State clearly what concept you're introduce and define it precisely. Again, do not attempt to prove your lemma. (It's not going to be strong enough to prove, and it's not sufficient to finish the soundness proof anyway.)

Define $H \to_s^* H'$ **denotes that the initial heap is** H**, and after executing** s **zero or more times, the resulted heap is** H'

Formally, we define $H \to_s H'$ and $H \to_s^* H'$ as follow.

$$\frac{H, s \to^* H', \texttt{skip}}{H \to_s H'} \qquad \frac{}{H \to_s^* H} \qquad \frac{H \to_s^* H_1 \qquad H_1 \to_s H'}{H \to_s^* H'}$$

Lemma 1-1. H, `while` e $s \to^* H'$, `skip`, **then** $\exists H_0, H \to_s^* H_0$ **and** $H' = H_0$.

(e) Now consider the general case where s' can be anything. Explain informally in one or two sentences what an execution

$$H, \texttt{while}\ e\ s \to^* H', s'$$

looks like by relating it to the execution of the loop body s.

Hint: The global structure is similar to the special case where $s' =$ `skip`. The only difference is on the last iteration of the loop. The picture on slide 8 of lecture 12 may help again.

- Case. $s' =$ `skip`. Case above.
- Case. $s' =$ `failed`. This must be the case where $H, e \Downarrow \top$. Moreover, the only possibility is that $H, s \to^* H_1, s$ and then $H_1, s \to H'$, `failed`.
- Case. s' is in the middle of the execution of the while loop.$\exists$ s_1 such that $H, s \to^* H', s_1$ under the condition that $H, e \Downarrow \top$

- Case. `while` e s. Takes zero step, so $H' = H$.

(f) State (but do not prove yet) a formal lemma for this special case of the form

If H, `while` e $s \to^* H'$, s', then ...

You will likely need to use the same concept you introduced in part (d). The scribblings on slide 10 of lecture 12 may help you.

Lemma 1-2. If H, `while` e $s \to^* H'$, s', then $\exists H_1.H \to_s^* H_1$ and one of the following holds

- Case $s' =$ `while` e s. $H_1 = H'$
- Case $s' =$ `skip`. $H_1 = H'$ and $H', e \Downarrow \bot$
- Case $s' =$ `failed`. $H_1, s \to^* H'$, `failed` and $H_1, e \Downarrow \top$.
- Case $s' = s_1$; `while` e s for some s_1. $H_1, e \Downarrow \top$ and $H_1, s \to^* H', s_1$.

(g) Remember that we should never attempt to prove a lemma unless we are sure it help us with our bigger proof. Complete the proof of the `while` case of the soundness theorem using your lemma.

Proof. While case soundness.

- Case. $\dfrac{\{I \wedge e\}\, s\, \{I\}}{\{I\}\,\texttt{while}\ e\ s\,\{I \wedge \neg e\}}$. By applying the lemma, we split to four cases:
  i. $s' =$ `skip`. According to induction hypothesis, we have $H' \models I$. Also, we know, by case spliting, that $H', e \Downarrow \bot$; therefore, since H' is not empty and $H' \not\models e$, thus $H' \models \neg e$. Therefore, $H' \models \{I \wedge \neg e\}$.
  ii. $s' =$ `while` e s. Then since s' is not `failed`, and s' is not `skip`, the conclusion holds trivially.
  iii. $s' =$ `failed`. According to the condition on case split, $\exists\ H_1, s \to^* H'$, `failed`. However, according to our induction hypothesis, for any $H \models \{I \wedge e\}$, $H, s \to^* H_1', s'$, then s' is not `failed`, which contradicts to our assumption. Thus the conclusion holds trivially.
  iv. s' is in the middle of the execution. Similar as Case ii.

□

(h) Prove your lemma by rule induction on the derivation $\to^*$. Be sure to use the definition of $\to^*$ included on the last page of this document, and not the one in the slides from week 2, or your life will be miserable.

Proof. By induction on $\to^*$.

- $\dfrac{}{H, \texttt{while}\ e\ s \to^* H, \texttt{while}\ e\ s}$. Pick $H' = H$, and Case 1 in **Lemma 1-2** holds.
- $\dfrac{H, \texttt{while}\ e\ s \to^* H_1, s_1 \qquad H_1, s_1 \to H', s'}{H_1 \texttt{while}\ e\ s \to^* H', s'}$. According to the induction hypothesis, $\exists H_1'.\ H \to_s^* H_1'$, and one of the following holds:
  i. Case $s_1 =$ `while` e s. $H_1' = H_1$
  ii. Case $s_1 =$ `skip`. $H_1' = H_1$ and $H_1', e \Downarrow \bot$
  iii. Case $s_1 =$ `failed`. $H_1', s \to^* H_1$, `failed` and $H_1, e \Downarrow \top$.
  iv. Case $s_1 = s_2$; `while` e s for some s_2. $H_1', e \Downarrow \top$ and $H_1', s \to^* H_1, s_2$.

  By case analysis on each cases:
  – $s_1 =$ `while` e s. Then, by case analysis on $H_1, s_1 \to H', s'$:
    i. H_1, `while` e $s \to H'$, `skip`. Since the loop does not unroll, $H', e \Downarrow \bot$. So pick H_1 in the Lemma to be H, and Case 2 of the lemma holds.
    ii. H_1, `while` e $s \to H', s$; `while` e s. In this case, the loop unrolls, so $H', e \Downarrow \top$. According to the induction hypothesis, $H_1' = H_1$. Since $H_1, s_1 \to H', s$; `while` e s, $H_1', s_1 \to H', s$; `while` e s. Therefore, Case 4 of the lemma holds.

- $s_1 = \texttt{skip}$. Vacuous, s_1 cannot step in this case.
- $s_1 = \texttt{failed}$. Similar as `skip` case.
- $s_1 = s_2; \texttt{while}\ e\ s$ for some s_2. By case analysis on $H_1, s_2; \texttt{while}\ e\ s \to H', s'$.
  i. Case where s_2 is `failed`. Then, $H_1, s_2; \texttt{while}\ e\ s \to H', \texttt{failed}$. According to the induction hypothesis, $\exists H_1'. H_1', s \to^* H_1, \texttt{failed}$, $H_1', e \Downarrow \top$ and $H \to_s^* H_1'$. Also, since $H_1 = H'$ according to the `failed` rule, $H_1', s \to^* H', \texttt{failed}$.
  ii. Case where s_2 is `skip`. Since $H_1, \texttt{skip}; \texttt{while}\ e\ s \to H_1, \texttt{while}\ e\ s$, $H' = H_1$. Pick H_1 in the lemma to be H_1 here.
  iii. $H_1, s_2 \to H', s_2'$, According to the induction hypothesis and the assumption, $H_1', e \Downarrow \top$ and

$$\frac{H_1', s \to^* H_1, s_2 \qquad H_1, s_2 \to H', s_2'}{H_1', s \to^* H', s_2'}$$

  We can pick H_1' to be H_1 in the lemma.

□

The remaining subproblems are extra credit.

(i) *Extra credit.* Explain informally in one sentence the difference between the definition of $\to^*$ in this document and the one we used in week 2.

(j) *Extra credit.* Explain informally in one or two sentences why your lemma would not be directly provable on the definition of $\to^*$ from week 2.

(k) *Extra credit.* Prove (by induction on various things) that the two definitions of $\to^*$ are equivalent in the sense that they relate the same heap-statement pairs to each other. Be sure to make it clear which definition you are referring to at any given time, perhaps by giving them different names like $\to_1^*$ and $\to_2^*$ or something. In our solution, we needed two top-level inductions (one for each direction) and two lemmas proved by induction (one for each direction).

IMP

$$\begin{array}{rcl} e & ::= & n \mid e + e \mid e - e \mid e \wedge e \mid \neg e \mid b \mid e < e \mid e = e \mid x \\ v & ::= & n \mid b \\ s & ::= & \texttt{skip} \mid \texttt{assert}\ e \mid \texttt{failed} \mid x := e \mid s; s \mid \texttt{while}\ e\ s \\ \tau & ::= & \text{int} \mid \text{bool} \end{array} \qquad \begin{array}{rcl} n & \in & \mathbb{Z} \\ b & \in & \mathbb{B} \\ x & \in & \text{Var } (= \text{String}) \\ H & \in & \text{Var} \rightharpoonup \text{Value} \\ \Sigma & \in & \text{Var} \rightharpoonup \text{Type} \end{array}$$

$\boxed{H, s \to H, s}$

$$\frac{H, e \Downarrow v}{H, x := e \to H[x \mapsto v], \texttt{skip}} \qquad \frac{H, e \Downarrow \top}{H, \texttt{assert}\ e \to H, \texttt{skip}} \qquad \frac{H, e \Downarrow \bot}{H, \texttt{assert}\ e \to H, \texttt{failed}}$$

$$\frac{H, s_1 \to H', s_1'}{H, s_1; s_2 \to H', s_1'; s_2} \qquad \frac{}{H, \texttt{skip}; s \to H, s} \qquad \frac{}{H, \texttt{failed}; s \to H, \texttt{failed}}$$

$$\frac{H, e \Downarrow \top}{H, \texttt{while}\ e\ s \to H, s; \texttt{while}\ e\ s} \qquad \frac{H, e \Downarrow \bot}{H, \texttt{while}\ e\ s \to H, \texttt{skip}}$$

$\boxed{H, s \to^* H, s}$

$$\frac{}{H, s \to^* H, s} \qquad \frac{H_1, s_1 \to^* H_2, s_2 \qquad H_2, s_2 \to H_3, s_3}{H_1, s_1 \to^* H_3, s_3}$$

$\boxed{\{P\}\, s\, \{Q\}}$

$$\frac{}{\{P\}\,\texttt{skip}\,\{P\}} \qquad \frac{P \Rightarrow e}{\{P\}\,\texttt{assert}\ e\,\{P\}} \qquad \frac{}{\{P[e/x]\}\, x := e\, \{P\}} \qquad \frac{\{P\}\, s_1\, \{R\} \qquad \{R\}\, s_2\, \{Q\}}{\{P\}\, s_1; s_2\, \{Q\}}$$

$$\frac{\{I \wedge e\}\, s\, \{I\}}{\{I\}\,\texttt{while}\ e\ s\,\{I \wedge \neg e\}} \qquad \frac{P \Rightarrow P' \qquad \{P'\}\, s\, \{Q'\} \qquad Q' \Rightarrow Q}{\{P\}\, s\, \{Q\}}$$

$\boxed{H \vDash P}$

$$H \vDash P \quad = \quad H, P \Downarrow \top$$

Theorem 1 (Soundness of the logic with respect to the operational semantics.)**.** If $\{P\}\, s\, \{Q\}$ and $H \vDash P$ and $H, s \to^* H', s'$, then $s' \neq \texttt{failed}$ and if $s' = \texttt{skip}$ then $H' \vDash Q$.

Proof. By induction on the derivation of $\{P\}\, s\, \{Q\}$. All cases but the `while` rule were covered in lecture. (Slides 8 and 10 of Lecture 12 cover the `while` rule, but we didn't talk about them in lecture due to time.) □