WEAKEST LIBERAL PRECONDITIONS

- The weakest liberal pre-condition of a statement S wrt a post-condition Q is an assertion that holds for all states such that if execution of S from this state terminates, the final state satisfies Q.

- If such a formula exists, let's denote it $wlp(S,Q)$, then: not unique ?!

$$\models_{par} \{P\}\, S\, \{Q\} \text{ whenever } P \Rightarrow wlp(S,Q) \text{ is valid}$$

So, if one can compute $wlp(S,Q)$, verification of $\{P\}S\{Q\}$ can be reduced to checking the validity of the proof obligation $P \Rightarrow wlp(S,Q)$.

- An assertion languge Assn is called <u>expressive</u> if $wlp(S,Q)$ can be expressed as an assertion, for every $S \in Stm$ and $Q \in Assn$.

- One can prove that:

$$\boxed{\begin{array}{ll} wlp(\text{skip}, Q) & \Leftrightarrow Q \\ wlp(x:=a, Q) & \Leftrightarrow Q[a/x] \\ wlp(S_1;S_2, Q) & \Leftrightarrow wlp(S_1, wlp(S_2,Q)) \\ wlp(\underline{\text{if}}\ b\ \underline{\text{then}}\ S_1\ \underline{\text{else}}\ S_2, Q) & \Leftrightarrow (b \Rightarrow wlp(S_1,Q)) \\ & \quad \wedge (\neg b \Rightarrow wlp(S_2,Q)) \end{array}}$$

Notice that these equivalences can be seen as a definition by structural induction! Call the function $wlp'(S,Q)$.

EXAMPLE Verify $\{x \leq 0\}$ if $0 \leq x$ then $x := x+1$ else $x := 1$ $\{x = 1\}$

First, we compute:

$$\begin{aligned}
& wlp'(\text{if } 0 \leq x \text{ then } x := x+1 \text{ else } x := 1,\ x = 1) \\
&= (0 \leq x \Rightarrow wlp'(x := x+1, x = 1)) \wedge ((\neg 0 \leq x \Rightarrow wlp'(x := 1, x = 1)) \\
&= (0 \leq x \Rightarrow x+1 = 1) \wedge (\neg 0 \leq x \Rightarrow 1 = 1)
\end{aligned}$$

Next, we obtain the proof obligation:

$$x \leq 0 \Rightarrow (0 \leq x \Rightarrow x+1 = 1) \wedge (\neg 0 \leq x \Rightarrow 1 = 1)$$

which is easily shown to be valid.

- In general, extending this approach to the while b do S construct is cumbersome. Two possible approaches are:
  - unfolding the loop some fixed number k of times (unsound)
  - using user-provided loop invariants

EXERCISE Extend the definition of wlp' to loops of the shape $\{I\}$ while b do S, i.e. loops annotated with candidate invariants.

Hint: it may be easier to use an accumulator argument if the definition should be by structural induction on S.

- That's how many tools work, using an automated theorem prover (SMT solver) as back-end for discharging the proof obligations.

- Canonical proof of completeness of Hoare logic based on wlp's
  $\vdash_{par} \{wlp(S, Q)\}\ S\ \{Q\}$ see Lemma 9.2? in book