6.977: Reasoning about sequential programs **CSAIL, MIT**
carroll@csail.mit.edu, 32-G708, x87110 **3/x/07**

Relational semantics in your pocket

The state space is S; the type of program denotations is $S \to \mathbb{P}_\uparrow S_\perp$ where $\mathbb{P}_\uparrow$ forms *non-empty*, *up-closed* subsets only.

For $f\colon S \to \mathbb{P}_\uparrow S_\perp$ define its *non-termination lifting* to be $f^\dagger\colon S_\perp \to \mathbb{P}_\uparrow S_\perp$ that acts just as f does on proper elements in S itself, but satisfies also $f^\dagger.\perp := S_\perp$. Define its *full lifting* to be $f^\ddagger\colon \mathbb{P}_\uparrow S_\perp \to \mathbb{P}_\uparrow S_\perp$ so that for $A\colon \mathbb{P}_\uparrow S$ we have

$$f^\ddagger.A \quad := \quad (\cup a\colon A \cdot f^\dagger.a) \ .$$

Here is the relational semantics of our simple imperative, nondeterministic language, given by a function $rp.[\![\cdot]\!]$ taking syntax to semantics:[1]

$$\begin{array}{rcl}
rp.[\![\ \mathbf{abort}\ ]\!].s & := & S_\perp \\
rp.[\![\ \mathbf{skip}\ ]\!].s & := & \{s\} \\
rp.[\![\ \mathbf{assign}\ E\ ]\!].s & := & \{[\![\ E\ ]\!].s\}\uparrow \\
rp.[\![\ S; T\ ]\!] & := & (rp.[\![\ T\ ]\!])^\ddagger \circ rp.[\![\ S\ ]\!] \\
rp.[\![\ S \ \triangleleft B \triangleright\ T\ ]\!].s & := & rp.[\![\ S\ ]\!].s \ \triangleleft [\![\ B\ ]\!].s \triangleright \ rp.[\![\ T\ ]\!].s \\
rp.[\![\ S \sqcap T\ ]\!].s & := & rp.[\![\ S\ ]\!].s \cup rp.[\![\ T\ ]\!].s \\
\\
rp.[\![\ \mathbf{while}\ B\ \mathbf{do}\ D\ \mathbf{od}\ ]\!] & := & \\
\multicolumn{3}{r}{(\mu f \cdot (\lambda s \cdot f^\ddagger.(rp.[\![\ D\ ]\!].s) \ \triangleleft [\![\ B\ ]\!].s \triangleright \ \{s\}))}
\end{array}$$

- In general we write $A\uparrow$ for the up-closure of A.
- Command $S \sqcap T$ is the pure nondeterministic choice between S and T.
- In general $(\mu x \cdot E)$ means the least fixed point of function $(\lambda x \cdot E)$.

Do all the definitions preserve healthiness, i.e. non-emptiness and up-closure?

[1] Soon we define an alternative semantics $wp.[\![\cdot]\!]$, which is why we write rp here.