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

Exercise set 2

Bounded nondeterminism

Exercise 2.1

Consider the program Do, over a single integer-valued variable z, defined

do $z{>}0 \to z := z - 1$ [1]
$[\!]$ $z{<}0 \to z :\geq 0$ // Set z to any non-negative integer.
od .

whose first few $\mathcal{W}$-iterates (think of "unfolding" the text) are

$$\begin{array}{lcl}
\mathcal{W}^0.\bot & = & [\![\, \textbf{abort} \,]\!] \\
\mathcal{W}^1.\bot & = & [\![\, \textbf{if } z{=}0 \textbf{ then skip else abort fi} \,]\!] \\
 & = & [\![\, \textbf{if } 0{\leq}z{<}1 \textbf{ then } z := 0 \textbf{ else abort fi} \,]\!] \\
\mathcal{W}^2.\bot & = & [\![\, \textbf{if } 0{\leq}z{<}2 \textbf{ then } z := 0 \textbf{ else abort fi} \,]\!] \\
 & \vdots & \\
\mathcal{W}^k.\bot & = & [\![\, \textbf{if } 0{\leq}z{<}k \textbf{ then } z := 0 \textbf{ else abort fi} \,]\!]
\end{array}$$

— leading to the limit —

$$(\sqcup_{k=0}^{\infty} \mathcal{W}^k.\bot) \quad = \quad [\![\, \textbf{if } 0{\leq}z \textbf{ then } z := 0 \textbf{ else abort fi} \,]\!] \quad ,$$

which therefore –call it $[\![\, \mathsf{Lim} \,]\!]$– should be the denotation of program Do. That is, we should have $\mathsf{Do} = \mathsf{Lim}$.

But they are *not* the same! Program Do terminates with $z = 0$ from all initial states (is equivalent therefore to the simple $z := 0$) — but Lim is a program that aborts if begun with $z < 0$. In fact $[\![\, \mathsf{Lim} \,]\!]$ not only fails to be the least fixed point of $\mathcal{W}$, it is not a fixed point at all — because

Lim $\neq$ **do** $z{>}0 \to z := z - 1;$ Lim // Go around loop again.
$[\!]$ $z{=}0 \to$ **skip** // Terminate loop.
$[\!]$ $z{<}0 \to z :\geq 0;$ Lim // Go around loop again.
od .

Thus our question here is *why* is it not the fixed point? It's *supposed* to be. *What has gone wrong?*

[1] This is Dijkstra's elegant *GCL*-style rendering of the loop

while $z{\neq}0$ **do if** $z{>}0$ **then** $z := z - 1$ **else** $z :\geq 0$ **fi od** ,